
# Mathématiques élémentaires

Julien Leroy

Département de Mathématique
Faculté des Sciences

# Ambitions

Ce cours a deux buts principaux :

1. (Re)voir certaines notions du secondaire, mais avec un point de vue universitaire.
   On va définir et démontrer certaines choses que vous connaissez déjà (parfois depuis des années).

2. Façonner une manière de réfléchir et de rédiger.

**Attention :** élémentaire ne veut pas dire facile, mais indispensable.

# Organisation

- Cours théorique :
  - pendant 2 semaines : cours commun aux mathématiciens et physiciens
  - dans 2 semaines : cours pour les mathématiciens uniquement
- Notes de cours et journal de bord sur `www.discmath.ulg.ac.be/leroy/Teaching-fr.html`
- Répétitions séparées
- Exercices en ligne : pour tous, mais prise en compte uniquement pour les mathématiciens.
  **Démo**

# Pourquoi démontrer ?

On a accepté beaucoup de propriétés dans l'enseignement secondaire, parce qu'elles étaient plausibles, raisonnables. On ne pouvait pas faire autrement.

# Pourquoi démontrer ?

On a accepté beaucoup de propriétés dans l'enseignement secondaire, parce qu'elles étaient plausibles, raisonnables. On ne pouvait pas faire autrement.

**Plausible n'est pas vérité :**

31, 331, 3331, 33331, 333331, 3333331, 33333331 sont premiers

# Pourquoi démontrer ?

On a accepté beaucoup de propriétés dans l'enseignement secondaire, parce qu'elles étaient plausibles, raisonnables. On ne pouvait pas faire autrement.

**Plausible n'est pas vérité :**

31, 331, 3331, 33331, 333331, 3333331, 33333331 sont premiers

$333333331 = 17 \times 19607843$

# Pourquoi démontrer ?

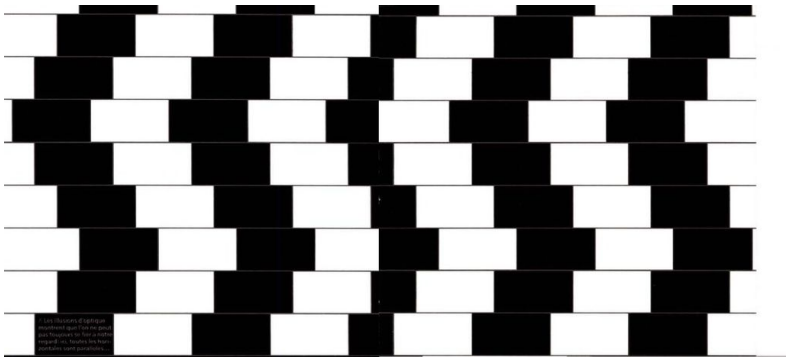
On a accepté beaucoup de propriétés dans l'enseignement secondaire, parce qu'elles étaient plausibles, raisonnables. On ne pouvait pas faire autrement.

**Plausible n'est pas vérité :**

31, 331, 3331, 33331, 333331, 3333331, 33333331 sont premiers

$333333331 = 17 \times 19607843$

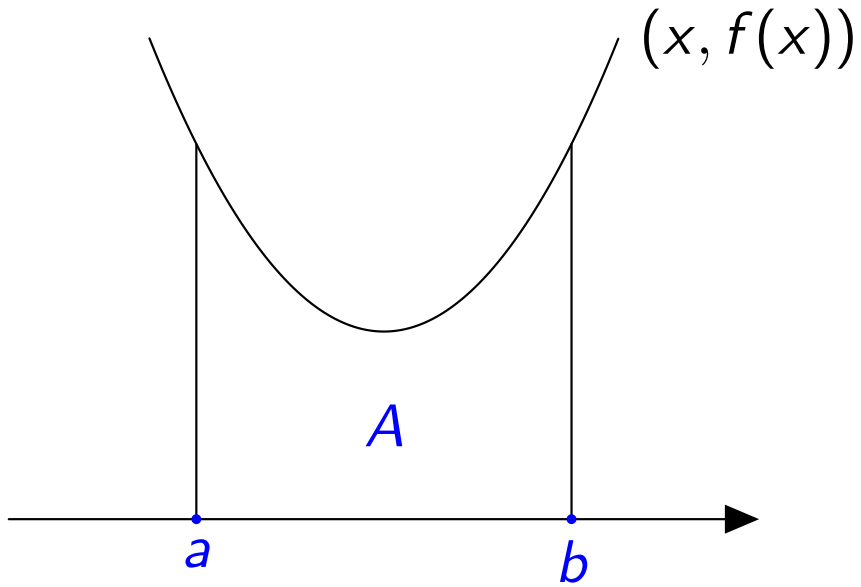
**Voir n'est pas suffisant :**



Les droites sont parallèles.

# Un exemple classique d'acceptation

Soit une fonction $f$ continue et à valeurs positives sur $[a, b]$.

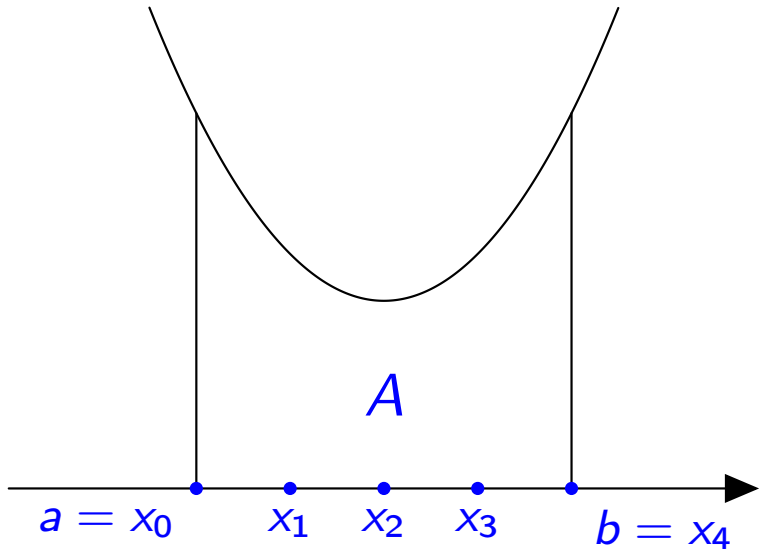



L'intégrale $\int_a^b f(x)\mathrm{d}x$ est l'aire "sous la courbe".

# Méthode de calcul par approximation

On fait un découpage de l'intervalle $[a, b]$ en se donnant des points

$$a = x_0 < x_1 < \cdots < x_{n-1} < x_n = b.$$




On a donc $n$ sous-intervalles $[x_{i-1}, x_i]$ pour $i \in \{1, \ldots, n\}$

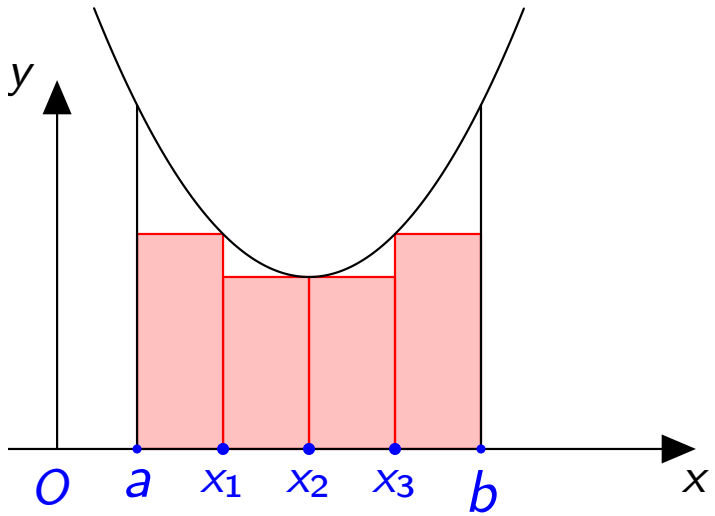
# Une approximation par défaut de l'aire

Puisque $f$ est continu, $f$ admet sur $[x_{i-1}, x_i]$ un minimum global, réalisé en un point $m_i$.

On définit la quantité

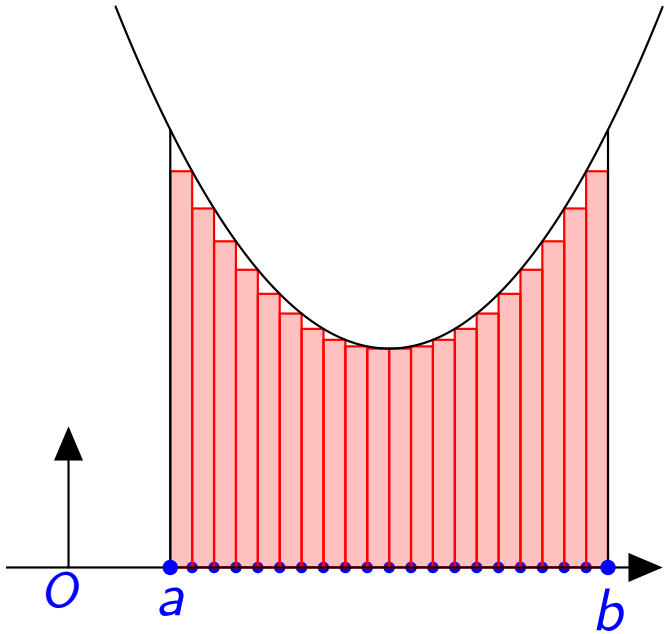
$$A_{\inf}(x_0, \ldots, x_n) = \sum_{i=1}^{n} f(m_i)(x_i - x_{i-1}) = \sum_{i=1}^{n} f(m_i)\Delta x_i.$$

C'est la somme des aires des rectangles de $[x_{i-1}, x_i]$ et de hauteur $f(m_i)$.



# En raffinant le découpage :

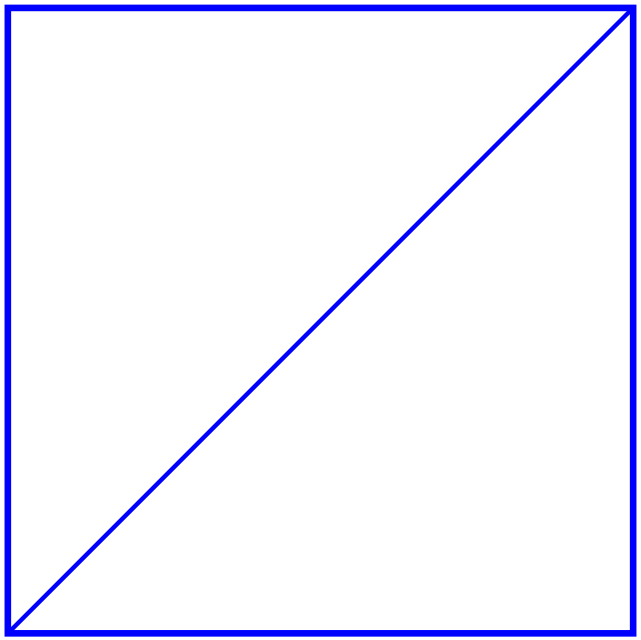
On approche l'aire par une somme d'aire de rectangles, et on passe à la limite, quand la mesure de la base des rectangles tend vers 0.




On voit bien que la somme des aires des rectangles converge vers l'aire recherchée.

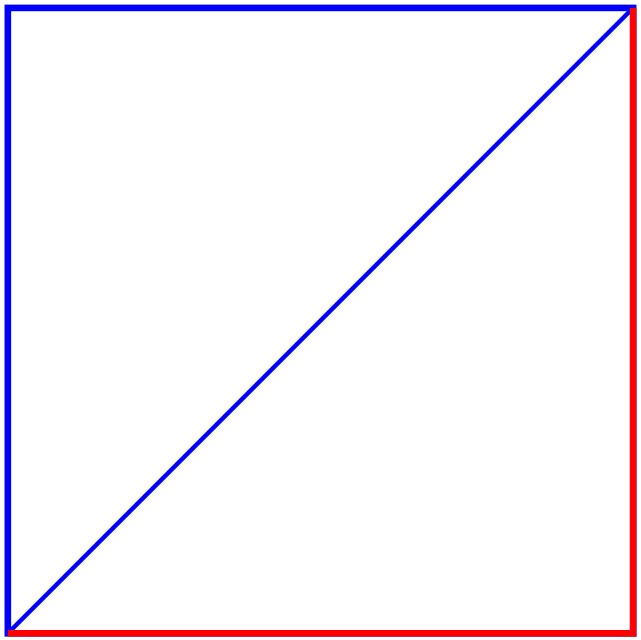
# On voit bien que $2 = \sqrt{2}$, ou la géométrie du pacman

Considérons un carré de côté 1. Quelle est la longueur de la diagonale ?



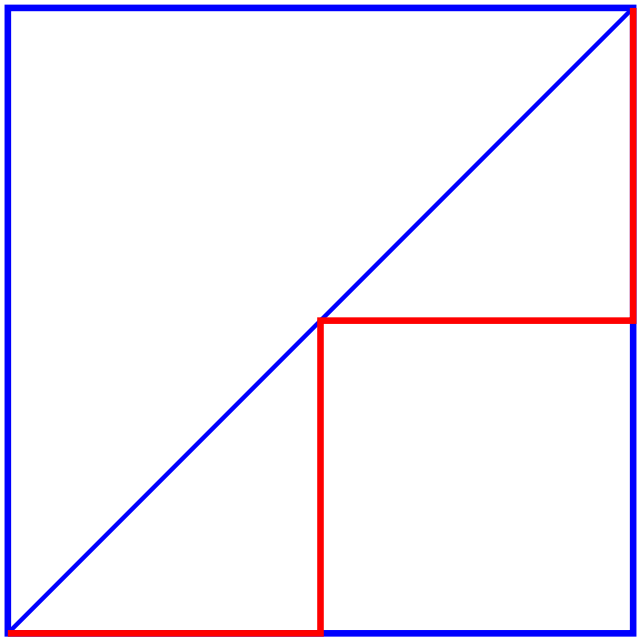
# On voit bien que $2 = \sqrt{2}$, ou la géométrie du pacman

Considérons un carré de côté 1. Quelle est la longueur de la diagonale ?



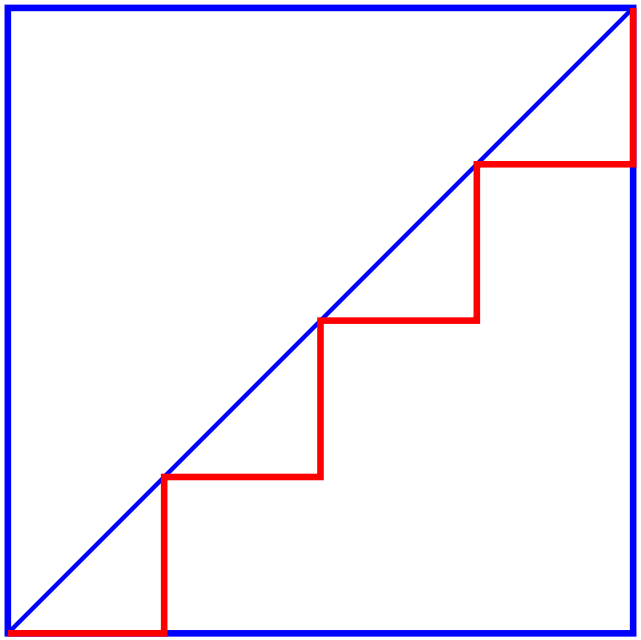
# On voit bien que $2 = \sqrt{2}$, ou la géométrie du pacman

Considérons un carré de côté 1. Quelle est la longueur de la diagonale ?



# On voit bien que $2 = \sqrt{2}$, ou la géométrie du pacman

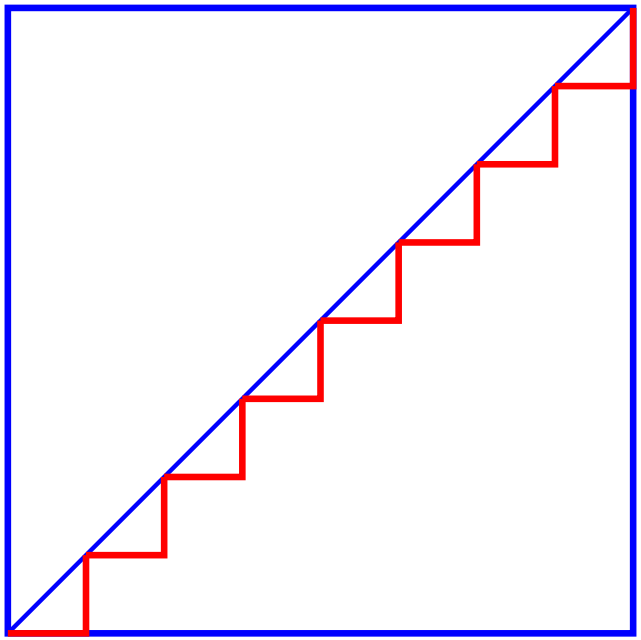
Considérons un carré de côté 1. Quelle est la longueur de la diagonale ?



À chaque étape $n$ , le pacman parcourt $d_n = 2cm$

# On voit bien que $2 = \sqrt{2}$, ou la géométrie du pacman

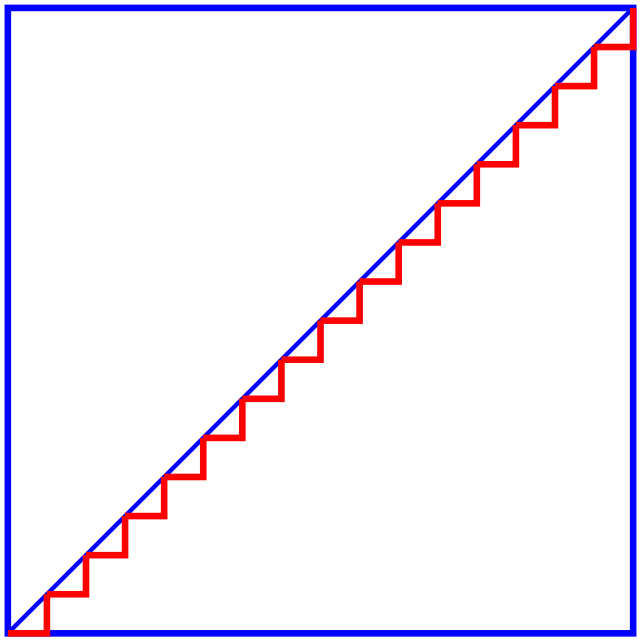
Considérons un carré de côté 1. Quelle est la longueur de la diagonale ?



À chaque étape $n$ , le pacman parcourt $d_n = 2cm$

# On voit bien que $2 = \sqrt{2}$, ou la géométrie du pacman

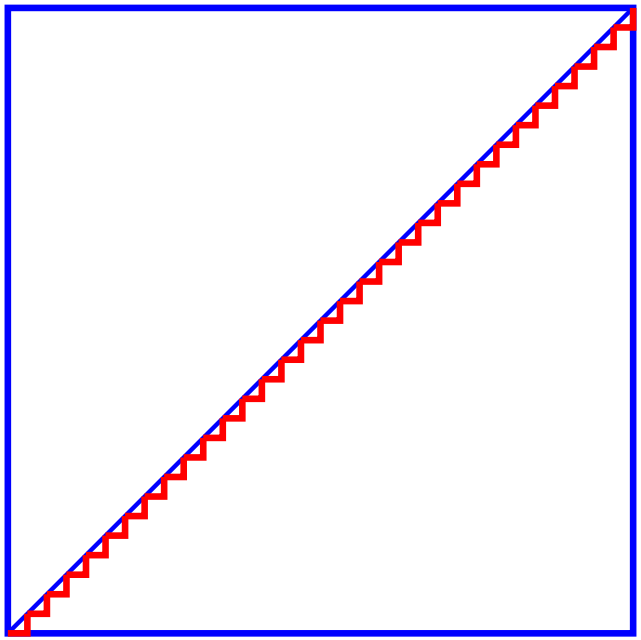
Considérons un carré de côté 1. Quelle est la longueur de la diagonale ?



À chaque étape $n$ , le pacman parcourt $d_n = 2cm$

# On voit bien que $2 = \sqrt{2}$, ou la géométrie du pacman

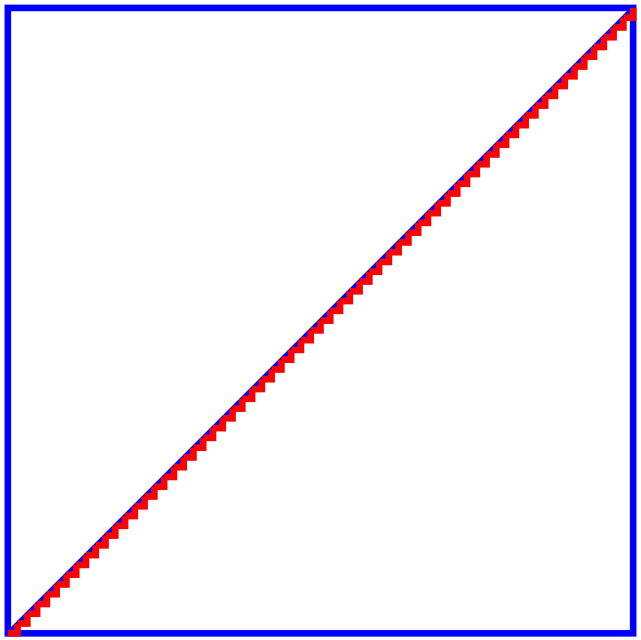
Considérons un carré de côté 1. Quelle est la longueur de la diagonale ?



À chaque étape $n$ , le pacman parcourt $d_n = 2cm$

# On voit bien que $2 = \sqrt{2}$, ou la géométrie du pacman

Considérons un carré de côté 1. Quelle est la longueur de la diagonale ?



À chaque étape $n$ , le pacman parcourt $d_n = 2cm$

# On voit bien que $2 = \sqrt{2}$, ou la géométrie du pacman

- Quand $n$ tend vers l'infini, le pacman parcourt la diagonale du carré, donc
$$\lim_{n \to +\infty} d_n = \sqrt{2} cm.$$
- Mais à chaque étape, le pacman parcourt $2cm$, donc
$$\lim_{n \to +\infty} d_n = 2cm.$$
- Donc $2 = \sqrt{2}$ (et donc $2 = 4$, $1 = 2 = 0$, ...)

# On voit bien que $2 = \sqrt{2}$, ou la géométrie du pacman

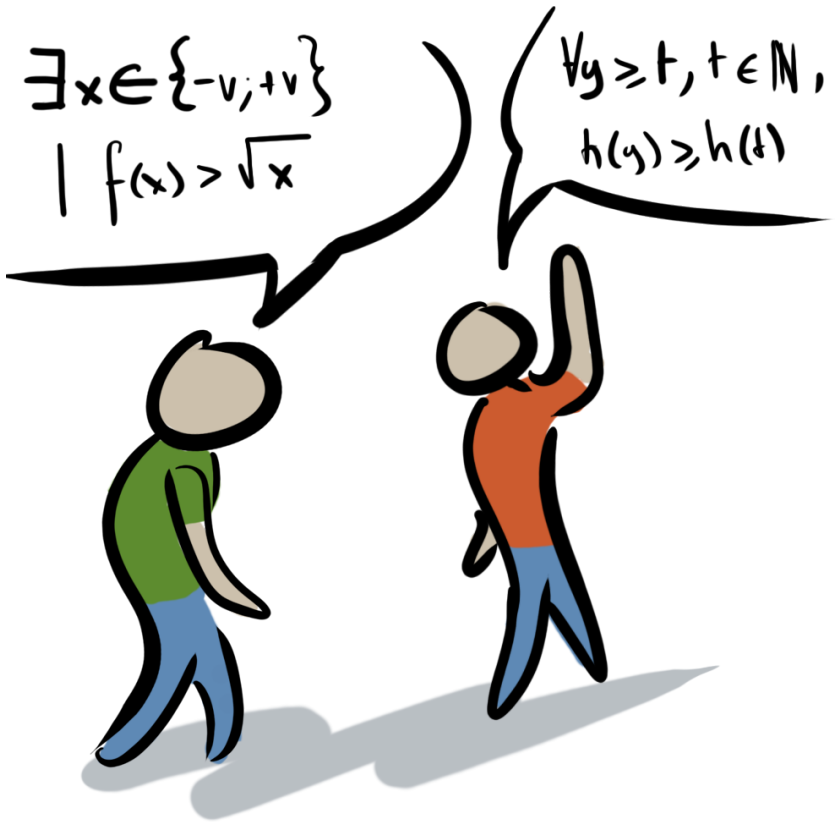
- Quand $n$ tend vers l'infini, le pacman parcourt la diagonale du carré, donc
$$\lim_{n \to +\infty} d_n = \sqrt{2} cm.$$
- Mais à chaque étape, le pacman parcourt $2cm$, donc
$$\lim_{n \to +\infty} d_n = 2cm.$$
- Donc $2 = \sqrt{2}$ (et donc $2 = 4$, $1 = 2 = 0$, ...)

Moralité : on ne peut pas toujours croire ce que l'on voit !

Il faut **démontrer**

# Première chose à faire : se comprendre

Les maths ont leur propre langage, avec ses règles et sa syntaxe.




Il s'agit de la **logique**.

# Logique propositionnelle

# Logique, assertions

On doit se mettre d'accord sur :

- un langage pour écrire des résultats ;
- la façon d'interpéter ces phrases.

## Définition 1.1.1

On appelle assertion ou proposition logique (ou proposition) toute phrase d'un langage donné dont on peut envisager sans ambiguïté le problème de sa vérité ou de sa fausseté.

**Exemples :**

1. "Aujourd'hui, je porte un pull rouge" ;
2. "3 est un nombre premier" ;
3. "3 n'est pas divisible par 2" ;
4. "tout nombre positif est pair" ;
5. "Il pleut" ;
6. "J'emporte un parapluie" ;
7. "Si Berlin est en Suisse, alors je viens de Mars" ;

# Contre-exemples, syntaxe, sémantique

Pour toutes ces phrases, on peut dire (selon le contexte) si elles sont vraies (V ou 1), ou fausses (F ou 0).

Ce n'est pas le cas des suivantes, qui ne sont donc pas des propositions :

1. "Quelle heure est-il ?"
2. "Cette phrase est fausse."
3. "Je dégrouille bien la kasibulle gauche."

# Contre-exemples, syntaxe, sémantique

Pour toutes ces phrases, on peut dire (selon le contexte) si elles sont vraies (V ou 1), ou fausses (F ou 0).

Ce n'est pas le cas des suivantes, qui ne sont donc pas des propositions :

1. "Quelle heure est-il ?"
2. "Cette phrase est fausse."
3. "Je dégrouille bien la kasibulle gauche."

**Syntaxe :** règles formatives qui permettent de construire de nouvelles propositions à partir d'anciennes.

**Sémantique :** règles pour décider de la véracité de telles propositions.

# Syntaxe de la logique propositionnelle

- On admet qu'il existe des propositions élémentaires appelées propositions atomiques ou variables propositionnelles. On les note par des variables $p$, $q$, $r$,...
- On dispose de symboles particuliers :
  - les parenthèses $(,)$
  - les connecteurs : $\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow$
- Si $p$ et $q$ sont des propositions, alors

$$\neg p, \quad (p \wedge q), \quad (p \vee q), \quad p \Rightarrow q, \quad p \Leftrightarrow q$$

sont des propositions (composées).

# Syntaxe de la logique propositionnelle

- On admet qu'il existe des propositions élémentaires appelées propositions atomiques ou variables propositionnelles. On les note par des variables $p$, $q$, $r$,...
- On dispose de symboles particuliers :
  - les parenthèses $(,)$
  - les connecteurs : $\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow$
- Si $p$ et $q$ sont des propositions, alors

$$\neg p, \quad (p \wedge q), \quad (p \vee q), \quad p \Rightarrow q, \quad p \Leftrightarrow q$$

sont des propositions (composées).

**Exemples :**

$$(p \Rightarrow (q \vee (r \wedge p))) \qquad \wedge p \Rightarrow (q \neg r)$$

## Principe du tiers exclu

Une proposition $p$ est toujours vraie (1) ou fausse (0), mais pas les deux en même temps.

La valeur de vérité d'une proposition composée (= non-atomique) dépend des valeurs de vérités des variables propositionnelles qui la composent et des connecteurs utilisés. Cette information est résumée dans la table de vérité de la proposition.

**Exemple :** La table de vérité de la proposition $P \wedge (\neg(Q \wedge P))$ est

| $P$ | $Q$ | $P \wedge (\neg(Q \wedge P))$ |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 0 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |

# La négation

## Définition 1.1.2

Si $P$ est une assertion, alors la négation de $P$ est une assertion. On la note $\neg P$. La table de vérité de l'opérateur de négation $\neg$ est :

| $P$ | $\neg P$ |
|---|---|
| 0 | 1 |
| 1 | 0 |

**Exemples :**

1. "Aujourd'hui, je ne porte pas un pull rouge" ;
2. "3 n'est pas un nombre premier" ;
3. "3 est divisible par 2" ;
4. "Il existe un nombre positif qui n'est pas pair"

**Exercice :** Ecrire la table de $P$, $\neg P$ et $\neg(\neg P)$.

# Equivalence logique

## Définition 1.1.3

Deux propositions logiques $P$ et $Q$ (composées à partir des mêmes variables propositionnelles) sont logiquement équivalentes si elles ont les mêmes tables de vérité (i.e. les mêmes valeurs de vérité, dans tous les cas). On note alors $P \equiv Q$.

On a donc $P \equiv \neg(\neg P)$.

**Remarques :** Si $P \equiv Q$, on peut les remplacer l'une par l'autre dans toute proposition composée où elles apparaissent.

Cela permet donc de simplifier des assertions comme :
"Il n'est pas impossible que ce cours ne soit pas dépourvu de concepts nouveaux. »

# La conjonction “et”

## Définition 1.1.4

Si $P$ et $Q$ sont deux assertions, alors la conjonction de $P$ et $Q$, notée $P \wedge Q$ ou “$P$ et $Q$” est une assertion qui est vraie quand $P$ est vraie et $Q$ est vraie (simultanément) et fausse sinon. La table de vérité du connecteur “et” est donc

| $P$ | $Q$ | $P \wedge Q$ |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 0 |
| 1 | 0 | 0 |
| 1 | 1 | 1 |

On peut ainsi former les assertions

1. “Il pleut et je porte un pull rouge” ;
2. “J’emporte un parapluie et 3 est un nombre premier”.

# La disjonction “ou”

## Définition

Si $P$ et $Q$ sont deux assertions, alors la disjonction de $P$ et $Q$, notée $P \vee Q$ ou “$P$ ou $Q$” est une assertion qui est vraie quand au moins l'une des deux assertions $P$, $Q$ est vraie et qui est fausse sinon. Sa table de vérité est donc la suivante.

| $P$ | $Q$ | $P \vee Q$ |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 1 |

# Négations de “et” et “ou”

## Proposition 1.1.1

On a les équivalences logiques suivantes

1. $\neg(P \vee Q) \equiv (\neg P) \wedge (\neg Q)$ ;
2. $\neg(P \wedge Q) \equiv (\neg P) \vee (\neg Q)$ ;

**Preuve :**

# Négations de “et” et “ou”

## Proposition 1.1.1

On a les équivalences logiques suivantes

1. $\neg(P \vee Q) \equiv (\neg P) \wedge (\neg Q)$ ;
2. $\neg(P \wedge Q) \equiv (\neg P) \vee (\neg Q)$ ;

**Preuve :**

**Exemples :**

- La négation de “Il pleut ou je porte un pull rouge” est “il ne pleut pas et je ne porte pas de pull rouge”.
- La négation de “Il pleut et nous sommes mardi” est “il ne pleut pas ou nous ne sommes pas mardi”.

# $\wedge$ et $\vee$ sont commutatifs et associatifs

**Exercice 1.1.2**

Soient $P, Q, R$ trois propositions. On a les équivalences logiques :

- $P \vee Q \equiv Q \vee P$
- $P \wedge Q \equiv Q \wedge P$
- $(P \vee Q) \vee R \equiv P \vee (Q \vee R)$
- $(P \wedge Q) \wedge R \equiv P \wedge (Q \wedge R)$

# Mais les parenthèses sont indispensables

Comparons $(P \wedge Q) \vee R$ et $P \wedge (Q \vee R)$.

| $P$ | $Q$ | $R$ | $P \wedge Q$ | $(P \wedge Q) \vee R$ | $Q \vee R$ | $P \wedge (Q \vee R)$ |
|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 1 | 0 | 1 | 1 | 0 |
| 0 | 1 | 0 | 0 | 0 | 1 | 0 |
| 0 | 1 | 1 | 0 | 1 | 1 | 0 |
| 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 0 | 1 | 1 | 1 |
| 1 | 1 | 0 | 1 | 1 | 1 | 1 |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 |

# Mais les parenthèses sont indispensables

Comparons $(P \wedge Q) \vee R$ et $P \wedge (Q \vee R)$.

| $P$ | $Q$ | $R$ | $P \wedge Q$ | $(P \wedge Q) \vee R$ | $Q \vee R$ | $P \wedge (Q \vee R)$ |
|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 1 | 0 | 1 | 1 | 0 |
| 0 | 1 | 0 | 0 | 0 | 1 | 0 |
| 0 | 1 | 1 | 0 | 1 | 1 | 0 |
| 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 0 | 1 | 1 | 1 |
| 1 | 1 | 0 | 1 | 1 | 1 | 1 |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 |

**Conclusion :** L'assertion $P \wedge Q \vee R$ n'a pas de sens.

# $\wedge$ et $\vee$ sont distributifs l'un sur l'autre :

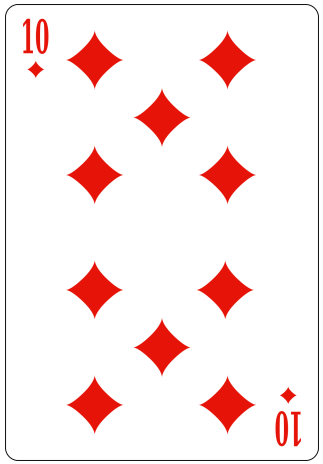
**Exercice 1.1.2**

Soient $P, Q, R$ trois propositions. On a les équivalences logiques :

- $P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$
- $P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \wedge R)$

# L'implication

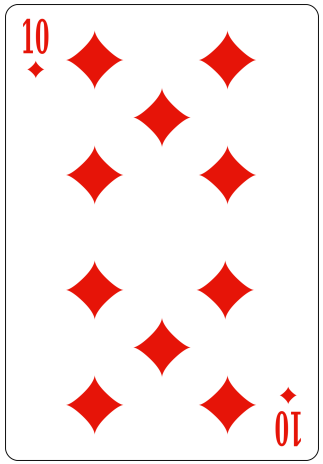
J'affirme : "Les cartes avec un dos bleu sont des dames".

Quelles sont les cartes à retourner pour vérifier la véracité de cette affirmation ?

# L'implication

J'affirme : "Les cartes avec un dos bleu sont des dames".

Quelles sont les cartes à retourner pour vérifier la véracité de cette affirmation ?
Il s'agit d'une implication :

"Si une carte a un dos bleu, alors c'est une dame."

# L'implication

## Définition 1.1.6

Si $P$ et $Q$ sont deux assertions, alors $P$ implique $Q$ est une assertion. On la note $P \Rightarrow Q$. Elle est toujours vraie sauf si $P$ est vrai et $Q$ faux. La table de vérité du connecteur $\Rightarrow$ est donc

| $P$ | $Q$ | $P \Rightarrow Q$ |
|---|---|---|
| 0 | 0 | 1 |
| 0 | 1 | 1 |
| 1 | 0 | 0 |
| 1 | 1 | 1 |

# Quelques exemples

1. "S'il pleut alors j'emporte un parapluie."[1]
2. "Si on est vendredi, je porte un pull rouge."[2]
3. "Si 3 est un nombre premier, alors je porte un pull rouge."

1. Cette implication ne donne aucune indication s'il ne pleut pas.
2. On peut aussi dire "Tous les vendredis, je porte un pull rouge."

# Quelques exemples

1. "S'il pleut alors j'emporte un parapluie."[1]
2. "Si on est vendredi, je porte un pull rouge."[2]
3. "Si 3 est un nombre premier, alors je porte un pull rouge."

**Attention :** Ne pas confondre $P \Rightarrow Q$ et $Q \Rightarrow P$.

1. Cette implication ne donne aucune indication s'il ne pleut pas.
2. On peut aussi dire "Tous les vendredis, je porte un pull rouge."

# Quelques exemples

1. "S'il pleut alors j'emporte un parapluie."[1]
2. "Si on est vendredi, je porte un pull rouge."[2]
3. "Si 3 est un nombre premier, alors je porte un pull rouge."

**Attention :** Ne pas confondre $P \Rightarrow Q$ et $Q \Rightarrow P$.
**Exercices :** Démontrer les équivalences logiques

$$P \Rightarrow Q \equiv (\neg P) \vee Q$$

$$\neg(P \Rightarrow Q) \equiv P \wedge (\neg Q)$$

1. Cette implication ne donne aucune indication s'il ne pleut pas.
2. On peut aussi dire "Tous les vendredis, je porte un pull rouge."

# La bi-implication

## Définition 1.1.7

Si $P$ et $Q$ sont deux assertions alors $P$ bi-implique $Q$ (ou $P$ est équivalent à $Q$) est une assertion. On la note $P \Leftrightarrow Q$. Elle est vraie quand $P$ implique $Q$ et $Q$ implique $P$ sont vraies. La table de vérité du connecteur $\Leftrightarrow$ est donc

| $P$ | $Q$ | $P \Leftrightarrow Q$ |
|---|---|---|
| 0 | 0 | 1 |
| 0 | 1 | 0 |
| 1 | 0 | 0 |
| 1 | 1 | 1 |

**Remarques :**

1. Par définition, on a $P \Leftrightarrow Q \equiv (P \Rightarrow Q) \wedge (Q \Rightarrow P)$
2. On dira aussi $P$ si et seulement si $Q$..

# Tautologies et contradictions

## Définition 1.1.8

Une assertion composée qui est vraie quelles que soient les valeurs de vérité des assertions qui la composent est une tautologie.
Une assertion composée qui est fausse quelles que soient les valeurs de vérité des assertions qui la composent est une contradiction.

# Tautologies et contradictions

## Définition 1.1.8

Une assertion composée qui est vraie quelles que soient les valeurs de vérité des assertions qui la composent est une tautologie.
Une assertion composée qui est fausse quelles que soient les valeurs de vérité des assertions qui la composent est une contradiction.

**Exemples :**

- $P \vee (\neg P)$ est une tautologie
- $P \wedge (\neg P)$ est une contradiction
- $((P \Rightarrow Q) \wedge P) \Rightarrow Q$ est une tautologie

**Remarque :**

1) Dire que $P$ et $Q$ sont logiquement équivalentes est donc la même chose que dire que $P \Leftrightarrow Q$ est une tautologie.
2) Toutes les tautologies sont logiquement équivalentes entre elles. De même que toutes les contradictions.

# Techniques de démonstration

# Equivalences logiques et techniques de démonstration

Les tautologies et équivalences logiques fournissent des techniques de démonstration.

La tautologie $((P \Rightarrow Q) \wedge P) \Rightarrow Q$ s'appelle le Modus ponens et fournit une technique de démonstration qui rejoint l'intuition : si $P \Rightarrow Q$ est vrai et si $P$ est vrai, alors $Q$ est vrai.

# Equivalences logiques et techniques de démonstration

Les tautologies et équivalences logiques fournissent des techniques de démonstration.

La tautologie $((P \Rightarrow Q) \wedge P) \Rightarrow Q$ s'appelle le Modus ponens et fournit une technique de démonstration qui rejoint l'intuition : si $P \Rightarrow Q$ est vrai et si $P$ est vrai, alors $Q$ est vrai.

**Exemple :** si vous savez que

1. Si il pleut à 7h alors je porte un parapluie toute la journée
2. Il pleut à 7h

Vous pouvez en déduire que je porte un parapluie.

# Preuve par contraposition

## Proposition 1.1.2

Si $P$ et $Q$ sont deux assertions, on a :

$$(P \Rightarrow Q) \equiv (\neg Q \Rightarrow \neg P).$$

**Preuve :**

# Preuve par contraposition

## Proposition 1.1.2

Si $P$ et $Q$ sont deux assertions, on a :

$$(P \Rightarrow Q) \equiv (\neg Q \Rightarrow \neg P).$$

**Preuve :**

**Deux exemples :**

## Proposition 1.1.4

Si $a, b \in \mathbb{R}$ sont tels que $a + b$ est irrationnel, alors $a$ ou $b$ est irrationnel.

## Proposition 1.1.5

Si $n$ est un nombre entier tel que $n^2$ est pair, alors $n$ est pair.

# Preuve par l'absurde

## Proposition 1.1.6

Si $P$ et $Q$ sont deux assertions, on a :

$$P \equiv (\neg P) \Rightarrow (Q \wedge (\neg Q)).$$

**Preuve :** exercice

# Preuve par l'absurde

## Proposition 1.1.6

Si $P$ et $Q$ sont deux assertions, on a :

$$P \equiv (\neg P) \Rightarrow (Q \wedge (\neg Q)).$$

**Preuve :** exercice

## Proposition 1.1.7

$\sqrt{2}$ est irrationnel.

**Preuve :**

# Contre-exemple

## Proposition 1.1.8

Si $P$ et $Q$ sont deux assertions, on a

$$\neg(P \Rightarrow Q) \equiv P \wedge (\neg Q)$$

**Preuve :** exercice

**Exemple :** Pour montrer que

$$\neg(\text{Si } f \text{ est une fonction continue en un point } x_0, \text{ alors } f \text{ est dérivable en ce point}),$$

il suffit de trouver une fonction :

- continue en $x_0$ $(P)$ ;
- non dérivable en $x_0$ $(\neg Q)$.

# Les disjonctions

## Propositions 1.1.9 et 1.1.10

Si $P$, $Q$ et $R$ sont des assertions, on a

$$P \Rightarrow (Q \vee R) \equiv (P \wedge (\neg Q)) \Rightarrow R$$
$$P \Rightarrow (Q \vee R) \equiv (P \wedge (\neg R)) \Rightarrow Q$$
$$(P \vee Q) \Rightarrow R \equiv (P \Rightarrow R) \wedge (Q \Rightarrow R)$$

**Preuve :**

**Exemple :**

## Proposition 1.1.11

Si $n$ est entier naturel, alors $n(n+1)$ est pair.

**Remarque :** Attention, faute de frappe dans les notes ($\mathbb{N}$).

# Logique du premier ordre

Un énoncé mathématique dépend souvent d'une ou plusieurs variables $x$, $y$, ... Par exemple

$$x \geqslant 3.$$

Ceci ne rentre pas dans le cadre de la définition 1.1.1 : $x \geqslant 3$ peut être vraie ou fausse selon la valeur prise par $x$ (on parlera tout de même d'assertion).

Les quantificateurs $\forall$ et $\exists$ permettent de palier à ce problème.

# Quantificateurs

$\forall$ se lit pour tout $\exists$ se lit il existe

Si $P$ est une assertion,

- $\forall x\, P =$ “Pour tout $x$, $P$ est vrai”
- $\exists x\, P =$ “Il existe au moins un $x$ pour lequel $P$ est vrai”

# Quantificateurs

$\forall$ se lit pour tout $\quad$ $\exists$ se lit il existe

Si $P$ est une assertion,

- $\forall x\, P =$ "Pour tout $x$, $P$ est vrai"
- $\exists x\, P =$ "Il existe au moins un $x$ pour lequel $P$ est vrai"

Si $P$ et $Q$ sont deux assertions, on peut écrire

$$\forall x : P, \exists y : Q$$

pour "Pour tout $x$ tel que $P$ est vrai, il existe un $y$ tel que $Q$ est vrai".

**Exemple :** $\forall x : (x \geqslant 0), \exists y : (y^2 = x)$
Attention à l'ordre des quantificateurs ! !

# Quantificateurs

$\forall$ se lit pour tout  $\exists$ se lit il existe

Si $P$ est une assertion,

- $\forall x\, P =$ "Pour tout $x$, $P$ est vrai"
- $\exists x\, P =$ "Il existe au moins un $x$ pour lequel $P$ est vrai"

Si $P$ et $Q$ sont deux assertions, on peut écrire

$$\forall x : P, \exists y : Q$$

pour "Pour tout $x$ tel que $P$ est vrai, il existe un $y$ tel que $Q$ est vrai".

**Exemple :** $\forall x : (x \geqslant 0), \exists y : (y^2 = x)$
Attention à l'ordre des quantificateurs ! !

On veut parfois une information supplémentaire sur l'existence :

- $\exists! x\, P =$ "Il existe un unique $x$ pour lequel $P$ est vraie"

# Quantificateurs et négation

Si $P$ est une assertion, alors

$$\neg(\forall x\, P) \equiv \exists x\, \neg P \qquad \neg(\exists x\, P) \equiv \forall x\, \neg P$$

**Exemples :**

1. La négation de “Tous les profs de math sont petits” est “Il existe un prof de math qui n’est pas petit”.
2. La négation de “Il existe un cheval de course bon marché” est “Tous les chevaux de course coûtent cher”.
3. Convergence d’une suite vers 0.

# Récurrence

# Une dernière technique : la récurrence

## Proposition (récurrence classique)

Soit $P(n)$ une assertion dépendant d'une variable $n$. Si les conditions suivantes sont satisfaites :

1. $P(0)$ est vrai ;
2. Pour tout $n$, si $P(n)$ est vrai alors $P(n+1)$ est vrai ;

alors $P(n)$ est vrai pour tout $n \in \mathbb{N}$.

1. Ce type de démonstration est basé sur la construction axiomatique de $\mathbb{N}$.
2. On a deux parties, un cas de base et la récurrence ou l'induction.
3. Une assertion satisfaisant la condition 2 est dite héréditaire.

**Exemple :** Pour tout $n \in \mathbb{N}$, on a

$$\sum_{k=0}^{n} k = \frac{n(n+1)}{2}.$$

# Et si on veut une propriété vraie pour $n \geqslant N$ ?

**Exemple :** Démontrer que l'on a pour tout $n \geqslant 1$ :

$$\sum_{k=1}^{n} \frac{1}{k(k+1)} = \frac{n}{n+1}.$$

## Proposition

Soit $P(n)$ une assertion dépendant d'une variable $n$ et soit $n_0 \in \mathbb{N}$.
Si les conditions suivantes sont satisfaites :

1. L'assertion $P(n_0)$ est vraie ;
2. Pour tout $n \geqslant n_0$, si $P(n)$ est vrai alors $P(n+1)$ est vrai ;

alors l'assertion $P(n)$ est vraie pour tout entier $n \geq n_0$.

**Preuve :** Définir $Q(n)$ comme "$P(n) \vee (n < n_0)$".

# La récurrence forte

## Proposition

Soit $P(n)$ une assertion dépendant d'une variable $n$. Si les conditions suivantes sont satisfaites :

1. $P(0)$ est vrai ;
2. Pour tout $k$, si $P(0), \ldots, P(k)$ sont vrais, alors $P(k+1)$ est vrai ;

alors la propriété $P(n)$ est vraie pour tout $n \in \mathbb{N}$.

**Preuve :** Considérer "$Q(n)$ : $P(k)$ est vraie pour tout $k$ t.q. $0 \leqslant k \leqslant n$."

**Remarque :** Ici aussi, on peut démontrer des propriétés vraies pour tout $n \geqslant n_0$.

# Une exemple : décomposition en nombres premiers

**Definition 2.1.2**

Un nombre naturel $p$ est premier s'il admet exactement deux diviseurs, à savoir 1 et $p$.

**Exemples :** 0, 1 ne sont pas premiers, 2,3,5 sont premiers...

**Exemple 2.1.1**

Pour tout entier $n \geqslant 2$, il existe des nombres premiers $p_1, \ldots, p_l$, $(l \geq 1)$ (éventuellement égaux), tels que $n = p_1 \cdots p_l$.

**Preuve :**

# Théorie naïve des ensembles

## Définition 1.2.1

Un ensemble est une collection d'objets possédant une ou plusieurs propriétés communes. Ces objets sont les éléments ou points de l'ensemble.

**Notation :** Généralement une lettre majuscule, mais pas obligatoirement.

Un ensemble peut être donné

1. de manière explicite, (définition en extension) comme par exemple

$$A = \{1, 2, 3, 4\} \quad \text{ou} \quad B = \{a, b, c, \ldots, z\};$$

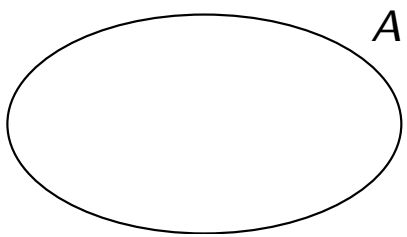
2. par une propriété caractérisant ses éléments, (définition en compréhension) comme par exemple

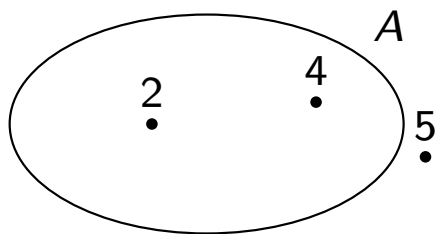
$$\begin{aligned} C &= \{n : n \text{ est entier, pair et compris entre 1 et 99}\} \\ &= \{n \mid n \text{ est entier, pair et compris entre 1 et 99}\} \end{aligned}$$

# Diagrammes de Venn

- On représente l'ensemble par un cercle ou une ellipse (appelées parfois patates).
- Si on veut marquer qu'un objet est un élément de l'ensemble, on le place dans la région correspondante.
- On représente plusieurs ensembles (généralement 2, 3 ou 4) par plusieurs patates.

**Exemple :** Soit $A$ l'ensemble des nombres entiers pairs.

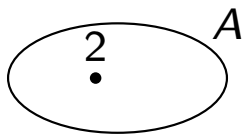


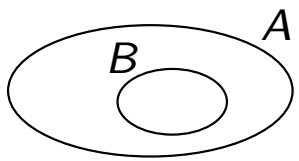
# Premières relations

**Ensemble vide** : il existe un ensemble qui ne contient pas d'éléments, l'ensemble vide, noté $\emptyset$.

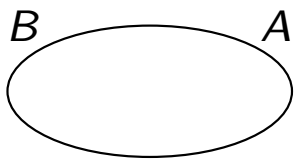
**Appartenance** : on écrit $x \in A$ ($x$ appartient à $A$) pour signifier que $x$ est un élément de l'ensemble $A$.




**Inclusion** : on écrit $B \subset A$ ($B$ est inclus dans $A$, ou $B$ est un sous-ensemble de $A$) quand tout élément de $B$ est aussi un élément de $A$.

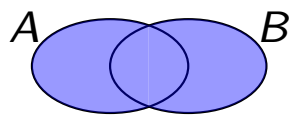



**Egalité** : on écrit $A = B$ ($A$ et $B$ sont égaux) quand les ensembles $A$ et $B$ ont les mêmes éléments. Cela se traduit aussi par le fait que $A \subset B$ et $B \subset A$.

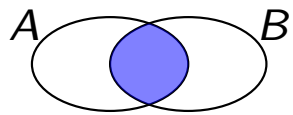


# Opérations sur les ensembles

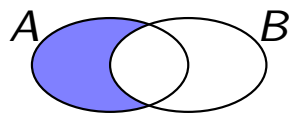
**Union** : l'ensemble $A \cup B$ est formé par les éléments qui appartiennent à $A$ ou à $B$.




**Intersection** : l'ensemble $A \cap B$ est formé par les éléments qui appartiennent à $A$ et $B$.

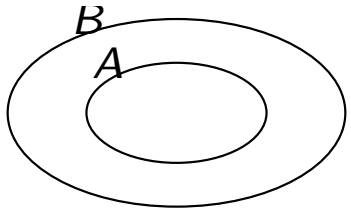



**Différence** : l'ensemble $A \setminus B$ (lisez $A$ moins $B$) est formé par les éléments qui appartiennent à $A$ et pas à $B$.

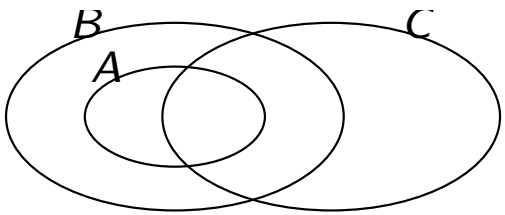


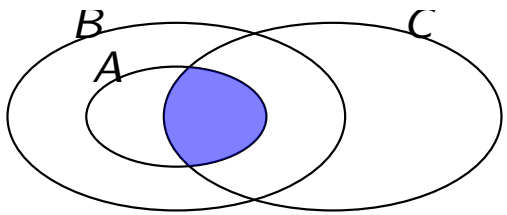
# Exemple : si $A \subset B$, alors $A \cap C \subset B \cap C$

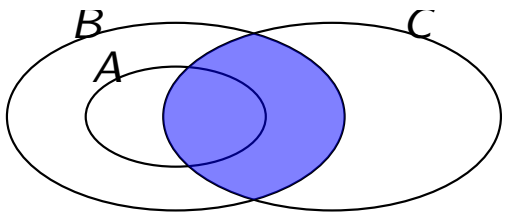
La situation où on a $A \subset B$ se représente de la manière suivante.




On représente alors l'ensemble $C$ de la manière la plus générale comme dans la figure de gauche. Au milieu, on peut colorier $A \cap C$ et à droite $B \cap C$.




On constate alors l'inclusion sur le diagramme de Venn.

**Attention :** ce n'est pas une démonstration.

# Assertions et ensembles

- Si $P$ est une assertion, on désigne par $\{x : P\}$ ou par $\{x \mid P\}$ l'ensemble des objets $x$ pour lesquels la propriété $P$ est vérifiée.
- Si $E$ est un ensemble, on peut considérer l'assertion $x \in E$.

Ces deux constructions semblent inverses l'une de l'autre, mais vont poser problème.

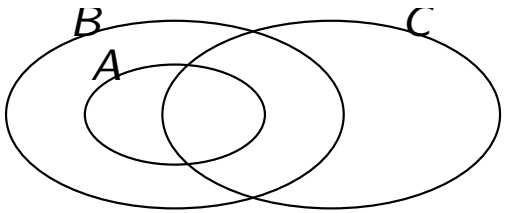
**Liens entre opérations sur les ensembles et symboles logiques :**

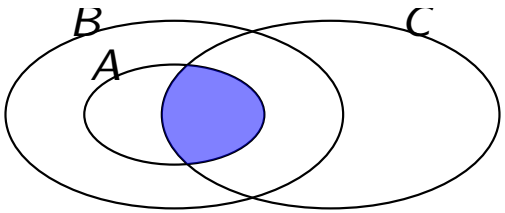
$$\begin{aligned} x \in A \cap B &\equiv (x \in A) \wedge (x \in B) \\ x \in A \cup B &\equiv (x \in A) \vee (x \in B) \\ A \subset B &\equiv (x \in A) \Rightarrow (x \in B) \\ A = B &\equiv (x \in A) \Leftrightarrow (x \in B) \end{aligned}$$

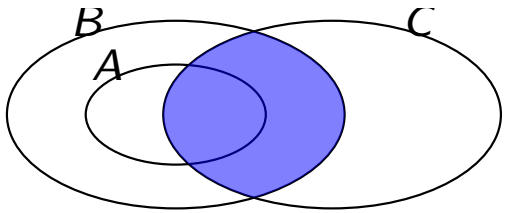
**Notations classiques :** $x \notin A$, $B \not\subset A$, $A \neq B$, $A \ni a$, $A \supset B$.

# Une “vraie” preuve

Si $A, B, C$ sont des ensembles et si $A \subset B$, alors $A \cap C \subset B \cap C$.








**Deux possibilités :**

- Traduire en assertion et vérifier qu’il s’agit d’une tautologie ;
- Preuve classique “à la main”.

# Un gros théorème

## Proposition 1.2.1

Si $X$ est un ensemble et si $A$, $B$, $C$ sont trois sous-ensembles de $X$, alors

1. $X \cup X = X$, $X \cap X = X$ ;
2. $X \setminus X = \emptyset$, $X \setminus \emptyset = X$, $\emptyset \cup X = X$, $\emptyset \cap X = \emptyset$ ;
3. $A \cup B = B \cup A$, $A \cap B = B \cap A$ ;
4. $(A \cup B) \cup C = A \cup (B \cup C)$, $(A \cap B) \cap C = A \cap (B \cap C)$ ;
5. $A \cup (X \setminus A) = X$, $A \cap (X \setminus A) = \emptyset$ ;
6. Si $A \subset B$, alors $A \cap C \subset B \cap C$ et $A \cup C \subset B \cup C$ ;
7. $A \cap B \subset A \subset A \cup B$ ;
8. si $C \subset A$ et $C \subset B$, alors $C \subset A \cap B$ ;
9. si $A \subset C$ et $B \subset C$, alors $A \cup B \subset C$ ;
10. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ ;
11. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ ;
12. $(A \cup B) \setminus C = (A \setminus C) \cup (B \setminus C)$ ;
13. $(A \cap B) \setminus C = (A \setminus C) \cap (B \setminus C)$ ;
14. $X \setminus (A \cup B) = (X \setminus A) \cap (X \setminus B)$ ;

# Une notation

Vous avez vu le symbole somme

$$\sum_{k=1}^{10} k^2 = 1^2 + 2^2 + 3^2 + \ldots + 10^2.$$

On peut utiliser cette notation avec l'union et l'intersection

$$\bigcup_{k=1}^{n} A_k = A_1 \cup \cdots \cup A_n \qquad \bigcap_{j=1}^{p} B_j = B_1 \cap \cdots \cap B_p.$$

# Le paradoxe de Russell

La théorie naïve des ensembles est contradictoire. Le problème vient de la définition des ensembles et de la correspondance "assertion-ensemble".

- Soient les ensembles $A = \{1, 2, 3, a, b, 2\}$ et $B = \{1, 2, 4, B, a, u, v\}$.
- On a $B \in B$.
- Ensembles **extraordinaires** : ceux qui se contiennent eux-mêmes (comme élément)
  Ensembles **ordinaires** : ceux qui ne sont pas extraordinaires
- Soit $R$ l'ensemble des ensembles ordinaires.
- Alors $R$ n'est ni ordinaire, ni extraordinaire.

# Relations et applications

# But du jeu

L'idée est ici de définir ce qu'est une application (fonction), ou plus généralement une relation d'un ensemble vers un autre et éviter "Une fonction de $A$ dans $B$ est une loi qui à tout $x$ associe $f(x)$".

Ceci peut être réalisé en utilisant la théorie (naïve) des ensembles.

## Définition 1.3.1

Si $A$ et $B$ sont deux ensembles, alors le produit cartésien de $A$ et $B$ est

$$A \times B = \{(a, b) : a \in A \text{ et } b \in B\}.$$

**Remarque :**
Ici aussi on peut utiliser des produits indicés (Définition 1.3.2) :

$$\prod_{i=1}^{n} A_i = A_1 \times \cdots \times A_n = \{(a_1, \ldots, a_n) : a_1 \in A_1, \ldots, a_n \in A_n\}.$$

## Définition 1.3.3

Une relation $\mathcal{R}$ de $A$ dans $B$ est une partie de $A \times B$. On appelle $A$ l'ensemble de départ et $B$ l'ensemble d'arrivée de $\mathcal{R}$.

**Autre notation :** Si $(a, b) \in \mathcal{R}$, on note aussi $a\mathcal{R}b$ et on dit que $a$ est en relation avec $b$.

**Exemple :** Si $A = \{2, 4, 6\}$ et $B = \{1, 3, 5, 7\}$, alors la relation

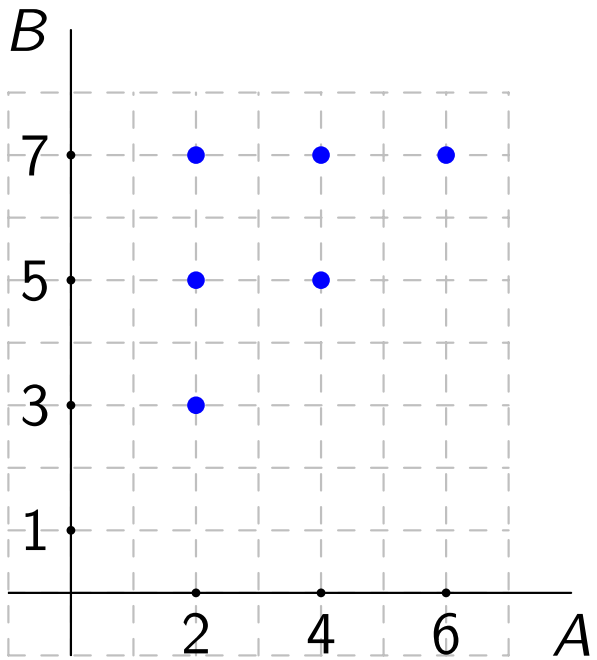
"est plus petit que",

de $A$ dans $B$ est

$$\mathcal{R} = \{(2, 3), (2, 5), (2, 7), (4, 5), (4, 7), (6, 7)\}.$$

# Représentation cartésienne

Si $A$ et $B$ sont des ensembles de nombres, on peut les représenter comme d'habitude.




**C'est une représentation parmi d'autres ! La relation n'est pas le dessin.**

Mais elle permet de se faire une idée intuitive, et nous la conserverons, même quand $A$ et $B$ ne sont pas des ensebles de nombres.

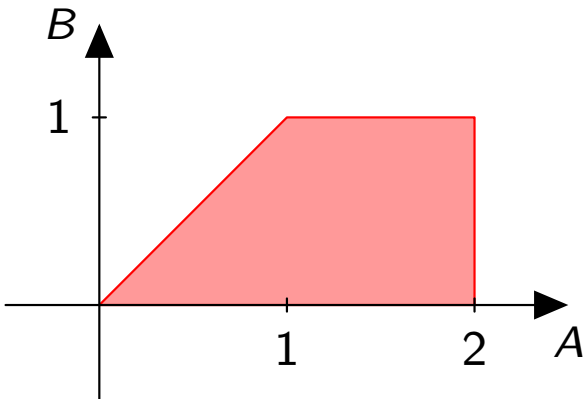
# D'autres exemples

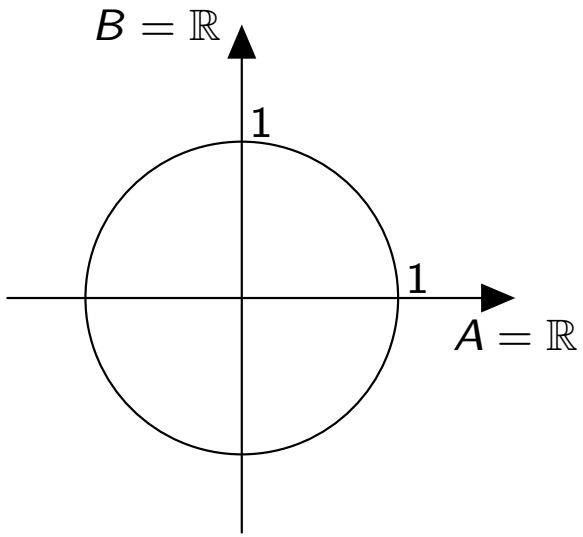
Considérons la relation $\geqslant$ de $A = [0, 2]$ dans $B = [0, 1]$ donnée par

$$\mathcal{R}_1 = \{(x, y) \in [0, 2] \times [0, 1] : x \geqslant y\}.$$

Soit $\mathcal{R}_2$ la relation de $\mathbb{R}$ dans $\mathbb{R}$ définie par

$$x\mathcal{R}_2 y \quad \text{si, et seulement si} \quad x^2 + y^2 = 1.$$



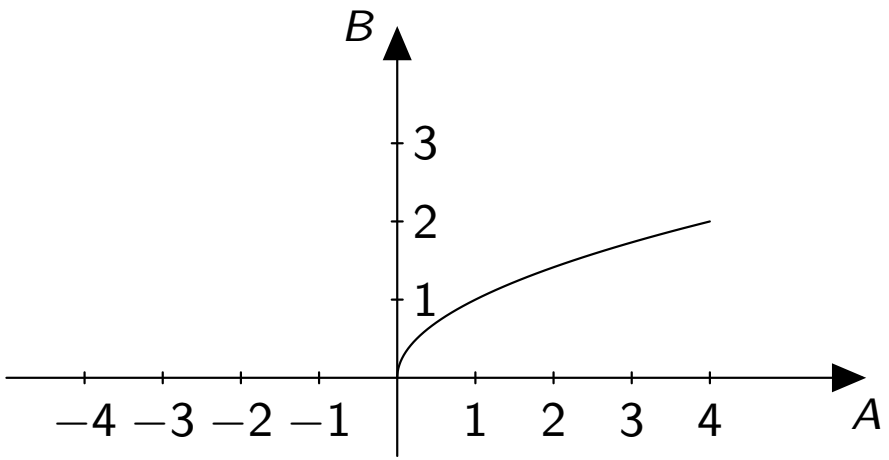



# Exemples

Terminons par la relation $\mathcal{R}_3$ définie de $A = [-4, 4]$ dans $B = [0, 3]$ par

$$x\mathcal{R}_3 y \quad \text{si, et seulement si} \quad y^2 - x = 0.$$

Elle est représentée par



# Domaine et image

## Définition 1.3.4

Soit $\mathcal{R}$ une relation de $A$ dans $B$. On appelle domaine de $\mathcal{R}$ l'ensemble des points $a$ de $A$ qui sont en relation avec au moins un élément $b$ de $B$. On le note $\mathrm{dom}_{\mathcal{R}}$ ou $\mathrm{dom}(\mathcal{R})$ ou encore $D_{\mathcal{R}}$. On a

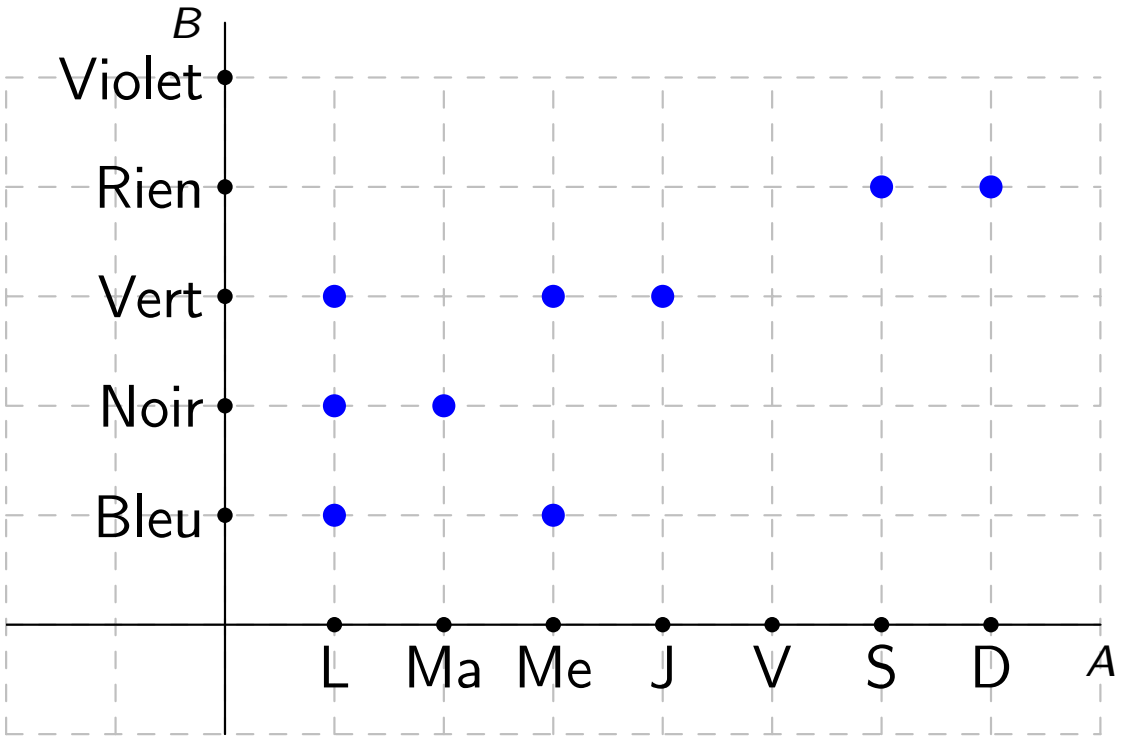
$$\mathrm{dom}_{\mathcal{R}} = \mathrm{dom}(\mathcal{R}) = D_{\mathcal{R}} = \{a \in A : \exists b \in B : a\mathcal{R}b\}.$$

On appelle codomaine ou image de $\mathcal{R}$ l'ensemble $\mathrm{Im}(\mathcal{R})$ (ou $\mathrm{Im}_{\mathcal{R}}$) des points $b$ de $B$ tels qu'il existe au moins un élément $a$ de $A$ qui soit en relation avec $b$. On a

$$\mathrm{Im}_{\mathcal{R}} = \mathrm{Im}(\mathcal{R}) = \{b \in B : \exists a \in A : a\mathcal{R}b\}.$$

# Exemple 1 Pg 16

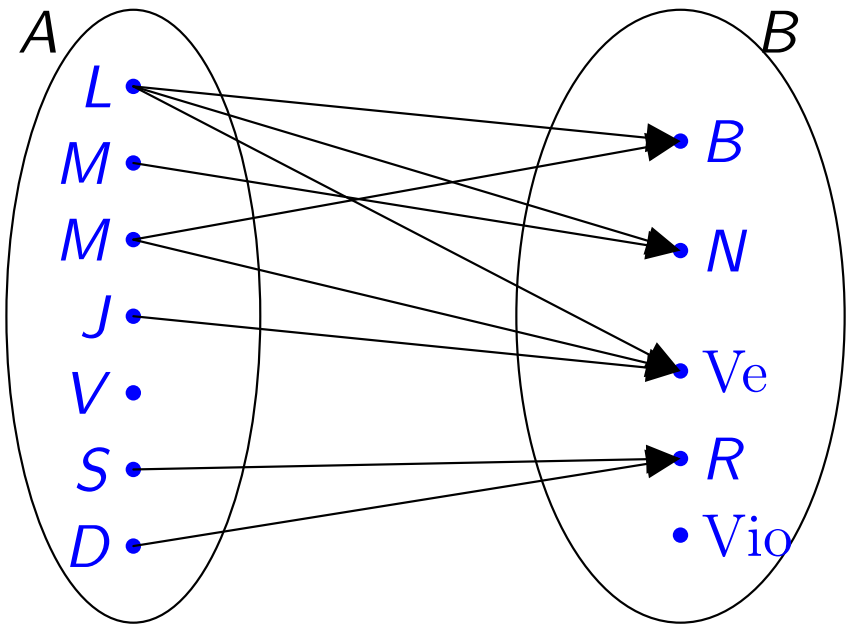
Si $A = \{\mathrm{L}, \mathrm{Ma}, \mathrm{Me}, \mathrm{J}, \mathrm{V}, \mathrm{S}, \mathrm{D}\}$ et
$B = \{\mathrm{bleu}, \mathrm{noir}, \mathrm{vert}, \mathrm{rien}, \mathrm{violet}\}$, et si $\mathcal{R}$ est représentée par



# Représentation sagitale

## Définition 1.3.5

La représentation sagittale d'une relation $\mathcal{R}$ de $A$ dans $B$ est obtenue en représentant les ensembles par des diagrammes de Venn et en indiquant une flèche de $a \in A$ vers $b \in B$ quand $a\mathcal{R}b$.



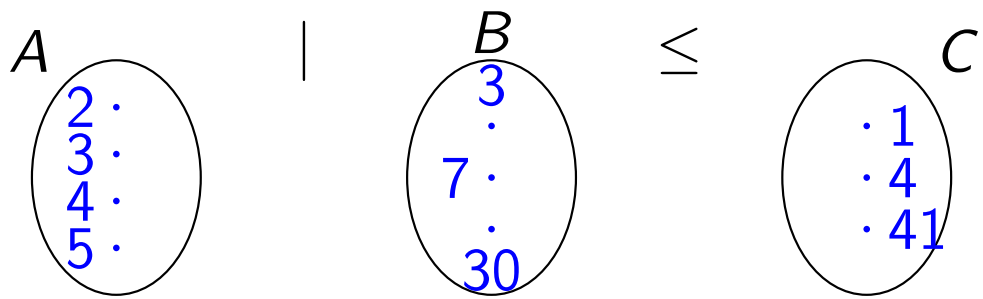
# Composée de relations

## Définition 1.3.6

Si $\mathcal{R} : A \to B$ et $\mathcal{R}' : B \to C$ sont des relations, alors la relation composée $\mathcal{R}' \circ \mathcal{R} : A \to C$ est définie par

$$\mathcal{R}' \circ \mathcal{R} = \{(a, c) \in A \times C : \exists b \in B : a\mathcal{R}b \quad \text{et} \quad b\mathcal{R}'c\}.$$

**Exemple :**



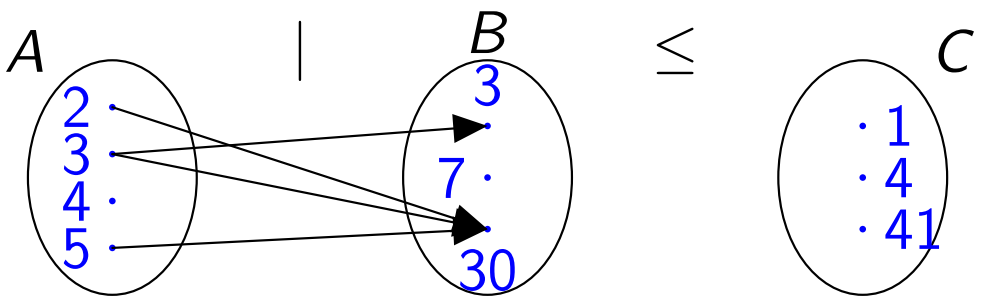
# Composée de relations

## Définition 1.3.6

Si $\mathcal{R} : A \to B$ et $\mathcal{R}' : B \to C$ sont des relations, alors la relation composée $\mathcal{R}' \circ \mathcal{R} : A \to C$ est définie par

$$\mathcal{R}' \circ \mathcal{R} = \{(a, c) \in A \times C : \exists b \in B : a\mathcal{R}b \quad \text{et} \quad b\mathcal{R}'c\}.$$

**Exemple :**



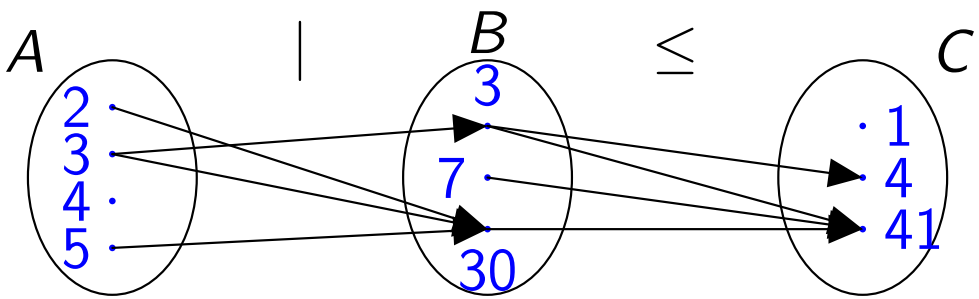
# Composée de relations

## Définition 1.3.6

Si $\mathcal{R} : A \to B$ et $\mathcal{R}' : B \to C$ sont des relations, alors la relation composée $\mathcal{R}' \circ \mathcal{R} : A \to C$ est définie par

$$\mathcal{R}' \circ \mathcal{R} = \{(a, c) \in A \times C : \exists b \in B : a\mathcal{R}b \quad \text{et} \quad b\mathcal{R}'c\}.$$

**Exemple :**



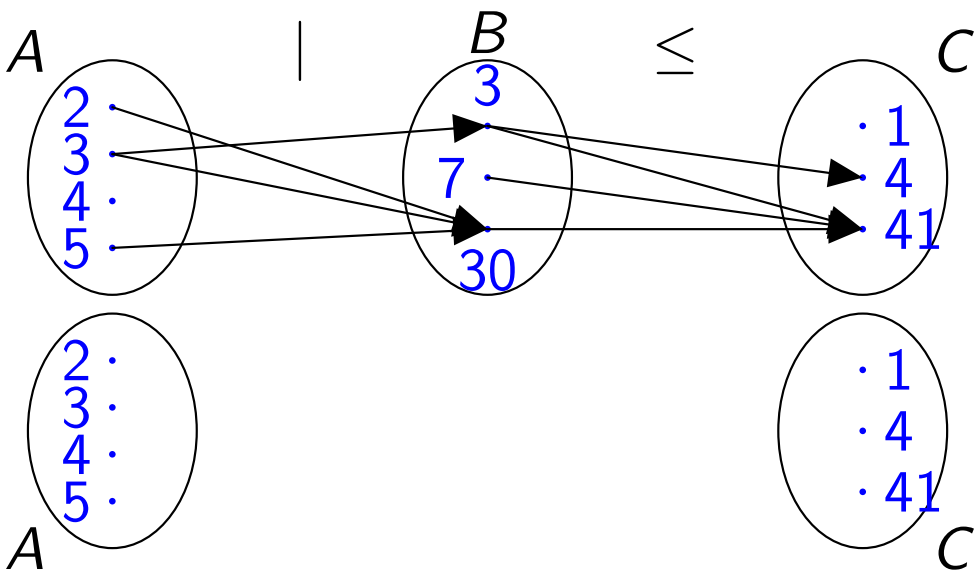
# Composée de relations

## Définition 1.3.6

Si $\mathcal{R} : A \to B$ et $\mathcal{R}' : B \to C$ sont des relations, alors la relation composée $\mathcal{R}' \circ \mathcal{R} : A \to C$ est définie par

$$\mathcal{R}' \circ \mathcal{R} = \{(a, c) \in A \times C : \exists b \in B : a\mathcal{R}b \quad \text{et} \quad b\mathcal{R}'c\}.$$

**Exemple :**



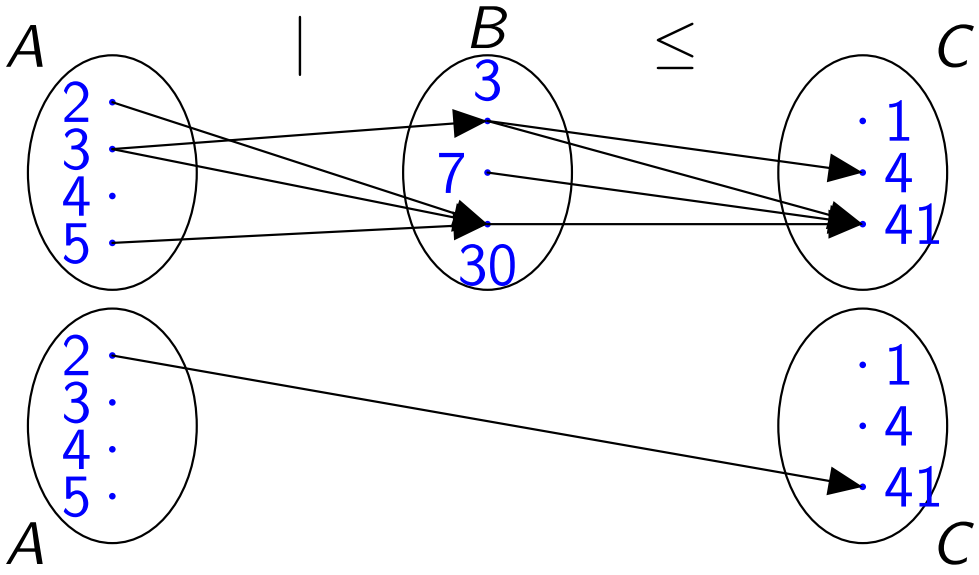
# Composée de relations

## Définition 1.3.6

Si $\mathcal{R} : A \to B$ et $\mathcal{R}' : B \to C$ sont des relations, alors la relation composée $\mathcal{R}' \circ \mathcal{R} : A \to C$ est définie par

$$\mathcal{R}' \circ \mathcal{R} = \{(a, c) \in A \times C : \exists b \in B : a\mathcal{R}b \quad \text{et} \quad b\mathcal{R}'c\}.$$

**Exemple :**



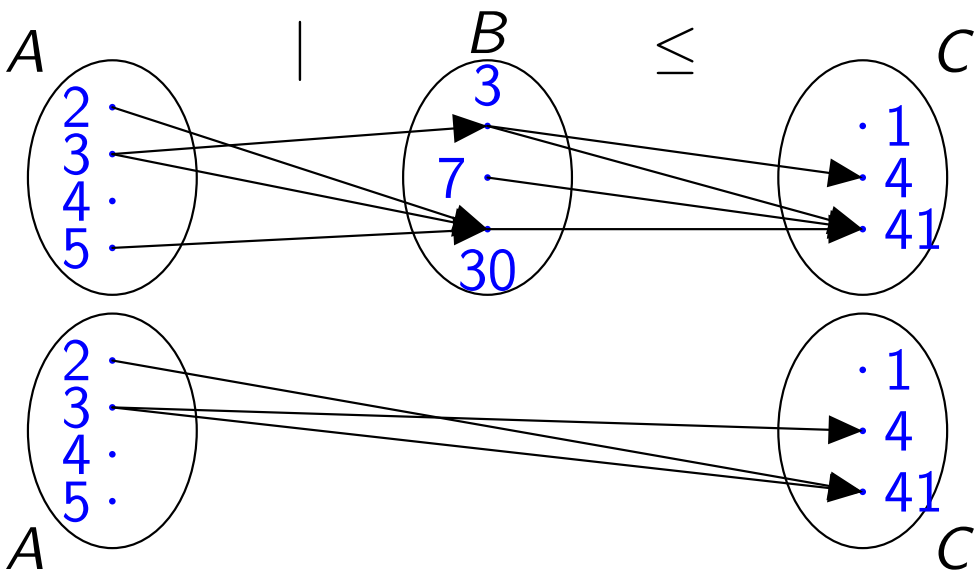
# Composée de relations

## Définition 1.3.6

Si $\mathcal{R} : A \to B$ et $\mathcal{R}' : B \to C$ sont des relations, alors la relation composée $\mathcal{R}' \circ \mathcal{R} : A \to C$ est définie par

$$\mathcal{R}' \circ \mathcal{R} = \{(a, c) \in A \times C : \exists b \in B : a\mathcal{R}b \quad \text{et} \quad b\mathcal{R}'c\}.$$

**Exemple :**



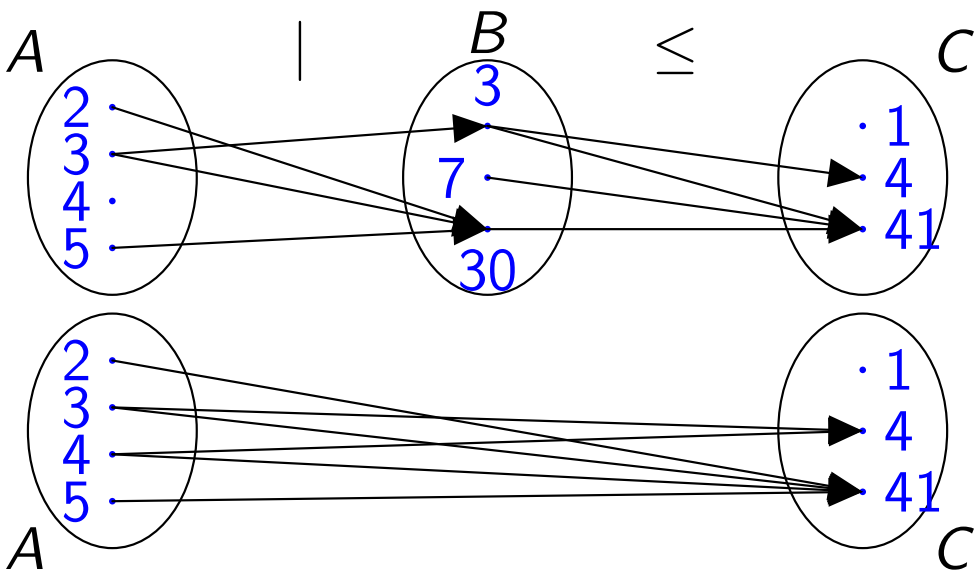
# Composée de relations

## Définition 1.3.6

Si $\mathcal{R} : A \to B$ et $\mathcal{R}' : B \to C$ sont des relations, alors la relation composée $\mathcal{R}' \circ \mathcal{R} : A \to C$ est définie par

$$\mathcal{R}' \circ \mathcal{R} = \{(a, c) \in A \times C : \exists b \in B : a\mathcal{R}b \quad \text{et} \quad b\mathcal{R}'c\}.$$

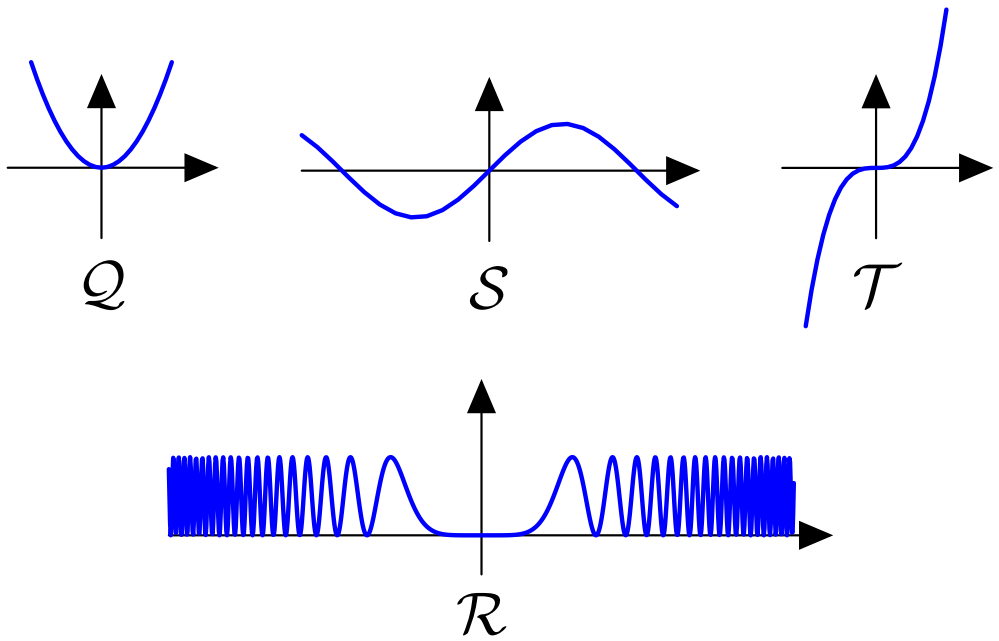
**Exemple :**



# C'est quelque chose que vous connaissez

$\mathcal{R} = \{(x, y) \in \mathbb{R}^2 : y = \sin^2(x^3)\}$ est une composée :

$$\mathcal{R} = \mathcal{Q} \circ \mathcal{S} \circ \mathcal{T}, \quad \text{où :} \quad \mathcal{Q} = \{(x, y) \in \mathbb{R}^2 : y = x^2\},$$
$$\mathcal{S} = \{(x, y) \in \mathbb{R}^2 : y = \sin(x)\},$$
$$\mathcal{T} = \{(x, y) \in \mathbb{R}^2 : y = x^3\},$$




**Remarque :** La composée de relations est associative (Exercice 1.3.1).

# Réciproques

**Définition 1.3.7**

Si $\mathcal{R} : A \to B$ est une relation, alors la relation inverse (ou réciproque) de $\mathcal{R}$ est la relation $\mathcal{R}^{-1} : B \to A$ définie par

$$\mathcal{R}^{-1} = \{(b, a) \in B \times A : a\mathcal{R}b\}.$$

**Représentation sagitale :**

# Réciproques

**Définition 1.3.7**

Si $\mathcal{R} : A \to B$ est une relation, alors la relation inverse (ou réciproque) de $\mathcal{R}$ est la relation $\mathcal{R}^{-1} : B \to A$ définie par

$$\mathcal{R}^{-1} = \{(b, a) \in B \times A : a\mathcal{R}b\}.$$

**Représentation cartésienne :**

# Réciproques

## Définition 1.3.7

Si $\mathcal{R} : A \to B$ est une relation, alors la relation inverse (ou réciproque) de $\mathcal{R}$ est la relation $\mathcal{R}^{-1} : B \to A$ définie par

$$\mathcal{R}^{-1} = \{(b, a) \in B \times A : a\mathcal{R}b\}.$$

**Propriétés :**

- $\mathrm{dom}(\mathcal{R}^{-1}) = \mathrm{Im}(\mathcal{R})$
- $\mathrm{Im}(\mathcal{R}^{-1}) = \mathrm{dom}(\mathcal{R})$
- $(\mathcal{R}^{-1})^{-1} = \mathcal{R}$
- $\mathcal{R}^{-1} \circ \mathcal{R} = \{(a, a') \in A \times A : \exists b \in B, (a, b), (a', b) \in \mathcal{R}\}$
- $\mathcal{R} \circ \mathcal{R}^{-1} = \{(b, b') \in B \times B : \exists a \in A, (a, b), (a, b') \in \mathcal{R}\}$

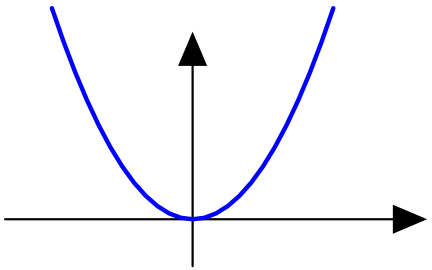
# Restriction

## Définition (Proposition 1.3.1)

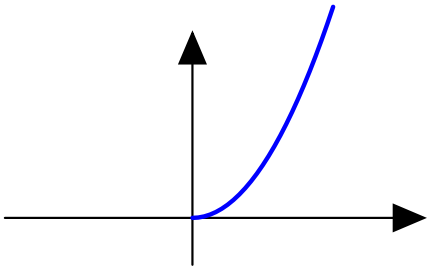
Si $\mathcal{R} : A \to B$ est une relation, et si $A'$ est un sous-ensemble de $A$, alors la restriction de $\mathcal{R}$ à $A'$ est la relation $\mathcal{R}|_{A'} : A' \to B$ définie par

$$\mathcal{R}|_{A'} = \{(a, b) \in A' \times B : a\mathcal{R}b\}.$$

**Exemple :**

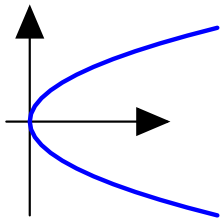


$\mathcal{R} = \{(x, y) \in \mathbb{R}^2 : y = x^2\}$



$\mathcal{R}|_{[0,+\infty[}$

# Fonction = relation particulière



Ceci n'est pas le graphe d'une fonction

## Définition 1.4.1

Une relation $\mathcal{R}$ de $A$ dans $B$ est de type fonctionnel (ou est une fonction) si tout point $a$ de $A$ est en relation avec au plus un élément de $B$, i.e.,

$$(a \in A, b_1, b_2 \in B, a\mathcal{R}b_1, a\mathcal{R}b_2) \Rightarrow b_1 = b_2.$$

**Graphiquement :** Dans la représentation cartésienne, une droite verticale intersecte au plus un point du graphe.

## Définition 1.4.2

Si $f : A \to B$ est une fonction, alors si $(a, b) \in f$, on dit que $b$ est l'image de $a$ par $\mathcal{R}$ et on note $b = f(a)$.

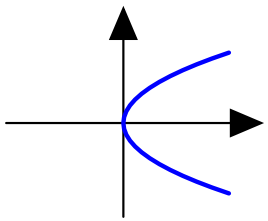
# Application = fonction particulière

## Définition 1.4.3

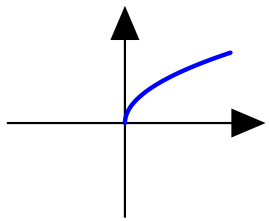
Une relation $\mathcal{R} : A \to B$ est de type application (ou est une application) si $\mathcal{R}$ est une fonction et si $\mathrm{dom}(\mathcal{R}) = A$.

**En résumé :** Une relation $\mathcal{R} : A \to B$ est une application si "Tout point $a$ de $A$ est en relation avec exactement un point de $b$ de $B$.", i.e.,

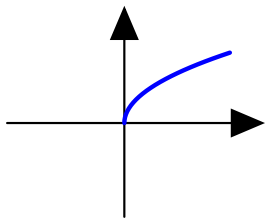
$$\forall a \in A, \exists! b \in B : a\mathcal{R}b.$$



$\{(x, y) \in \mathbb{R} \times \mathbb{R} : x = y^2\}$
~~fonction~~
~~application~~



$\{(x, y) \in \mathbb{R} \times \mathbb{R}_{\geq 0} : x = y^2\}$
fonction
~~application~~



$\{(x, y) \in \mathbb{R}_{\geq 0} \times \mathbb{R}_{\geq 0} : x = y^2\}$
fonction
application

# Restriction - Loi de transformation

## Proposition 1.4.1

Si $f : A \to B$ est une fonction, alors $f|_{\mathrm{dom}(f)}$ est une application.

**Attention :** Erreur dans les notes : $\mathcal{R}_4$ est une fonction, mais pas une application.

**Une notation :**

$$f : A \to B : a \mapsto f(a).$$

Elle indique que $f$ est une application de $A$ dans $B$ qui à chaque point $a$ de $A$ **associe** son image $f(a)$.

Toute application de $A$ dans $B$ définit donc bien une **loi de transformation** de $A$ dans $B$

# Connection avec le point de vue du secondaire.

## Définition (Intuitive mais incomplète)

Une application $f$ de $A$ dans $B$ est une "loi de transformation" qui associe à tout point $x$ de $A$, associe un point $f(x)$ de $B$.

Nous avons **reconstruit** cette définition :

1. Toute application donne lieu à une "loi de tranformation".
2. Toute "loi de transformation" $f : A \to B$ qui transforme chaque élément $x$ de $A$ en un élément $f(x)$ de $B$ donne lieu à une relation
$$G_f = \{(x, f(x)) : x \in A\}.$$
C'est une relation de type application (appelée graphe de $f$).

**Les deux points de vue coexistent, même si un seul est parfaitement défini.**

# Ce qu'on peut dire ou pas

- La fonction $f(x)$... Non
- La fonction $y = f(x)$... Non plus
- La fonction $f$... oui

Alors,

- Qu'est-ce que $f(x)$ ? Un élément de $B$
- Qu'est ce que $y = f(x)$ ?
  C'est l'équation cartésienne du graphe de $f$ :

$$G_f = \{(x, y) \in A \times B : y = f(x)\}.$$

Dans ce cadre, $x$ représente un élément de $A$.

# Injections, surjections

# Composée d'applications = application

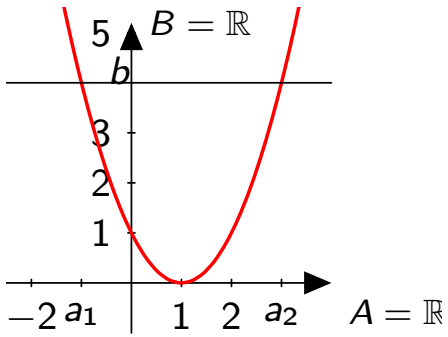
## Proposition 1.4.3

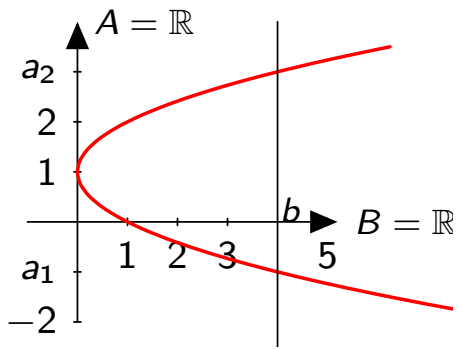
Si $f : A \to B$, $g : B \to C$ sont deux applications, alors $g \circ f : A \to C$ est une application. En particulier, pour tout $a \in A$, $g \circ f(a) = g(f(a))$.

**Question :** Et la réciproque d'une application ?

1. C'est une relation (comme réciproque d'une relation).
2. Il n'y a aucune raison que ce soit une application.

**Exemple :** La réciproque de $f : \mathbb{R} \to \mathbb{R} : x \mapsto (x-1)^2$ n'est pas une application :



# Bijections

## Proposition 1.5.1

Soit $f : A \to B$ une application. Alors $f^{-1}$ est une application si et seulement si pour tout $b \in B$ il existe un unique $a \in A$ tel que $f(a) = b$, i.e.,

$$\forall b \in B, \exists! a \in A : f(a) = b.$$

## Définition 1.5.1

Une application $f : A \to B$ est une bijection si pour tout $b \in B$ il existe un unique $a \in A$ tel que $f(a) = b$.

**Attention :**

- une relation $\mathcal{R} : A \to B$ est une application si

$$\forall a \in A, \exists! b \in B : (a, b) \in \mathcal{R}.$$

- une application $f : A \to B$ est une bijection si

$$\forall b \in B, \exists! a \in A : (a, b) \in f.$$

# Ce n'est pas ça qu'on vous a dit

**Définition classique :** une application $f$ est une bijection si elle est injective et surjective.

On va voir que ces définitions sont équivalentes et faire le lien avec les propriétés de la relation réciproque.

# Injections

## Définition 1.5.2

Une application $f : A \to B$ est injective (est une injection) si il n'existe pas $a_1, a_2 \in A$ tels que $a_1 \neq a_2$ et $f(a_1) = f(a_2)$, i.e.,

$$\forall a_1, a_2 \in A, \quad a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2)$$

## Proposition 1.5.2

Une application $f : A \to B$ est injective si, et seulement si, pour tous $a_1, a_2 \in A$, si $f(a_1) = f(a_2)$, alors $a_1 = a_2$, i.e.,

$$\forall a_1, a_2 \in A, \quad f(a_1) = f(a_2) \Rightarrow a_1 = a_2$$

**Attention :** Erreur fréquente avec la définition d'une fonction

# Exemples

1. L'application $f : \mathbb{R} \to \mathbb{R} : x \mapsto x^3$ est injective.
2. L'application $f : \mathbb{R} \to \mathbb{R} : x \mapsto x^2$ n'est pas injective.
3. L'application $f : [0, +\infty[ \to \mathbb{R} : x \mapsto x^2$ est injective.

# Injectivité et relation réciproque

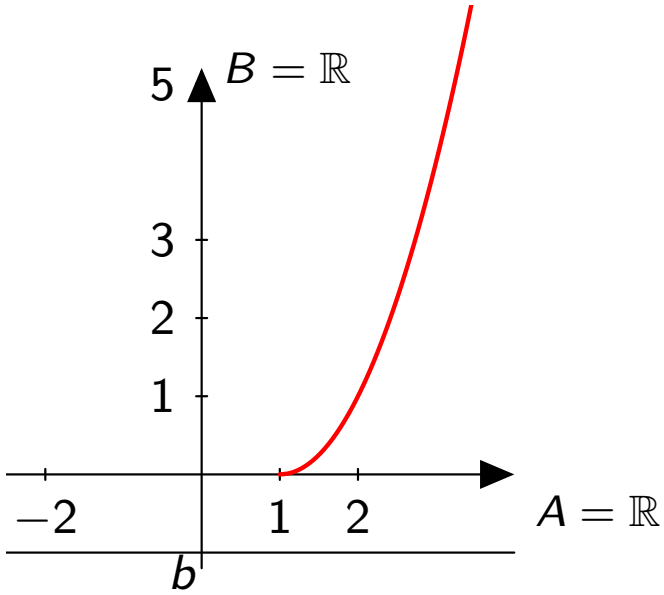
L'injectivité garanti le caractère fonctionnel de la relation réciproque :

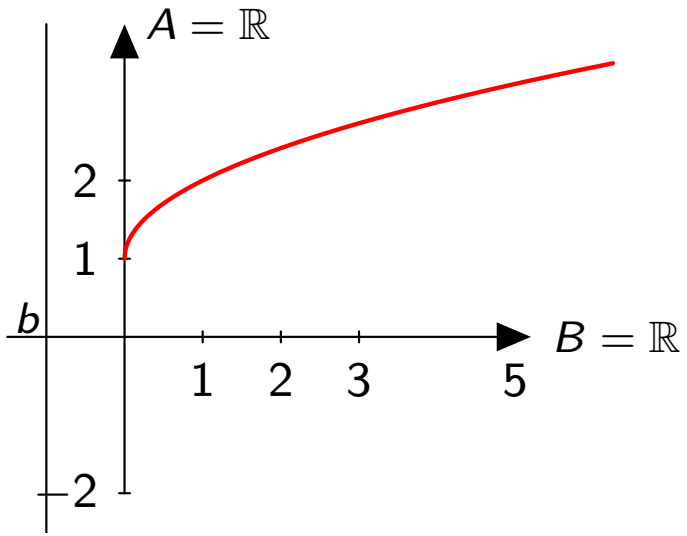
**Proposition 1.5.3**

Si $f : A \to B$ est une injection, alors $f^{-1} : B \to A$ est une fonction.

# Surjections

L'application $f : [1, +\infty[ \to \mathbb{R} : x \mapsto (x-1)^2$ admet une relation réciproque qui n'est pas une application :




## Définition 1.5.3

Une application $f : A \to B$ est surjective (est une surjection) si $\mathrm{Im}(f) = B$.

**Notation :** $f(A) = \mathrm{Im}(f)$.

# Exemples

1. L'application $f : \mathbb{R} \to \mathbb{R} : x \mapsto x^3$ est surjective.
2. L'application $f : \mathbb{R} \to \mathbb{R} : x \mapsto x^2$ n'est pas surjective.
3. L'application $f : \mathbb{R} \to [0, +\infty[ : x \mapsto x^2$ est surjective.

**Proposition 1.5.7**

Pour toute application $f : A \to B$, l'application $f : A \to f(A)$ est surjective.

# Surjectivité et relation réciproque

**Proposition 1.5.5**

Une application $f : A \to B$ est surjective si et seulement si $\mathrm{dom}(f^{-1}) = B$.

**Attention :** $f^{-1}$ est la notation pour la relation réciproque de $f$, ce n'est pas forcément une fonction !

# Réunification

## Proposition

Soit $f : A \to B$ une application. Les assertions suivantes sont équivalentes :

1. $f$ est une bijection ;
2. $f$ est injective et surjective ;
3. $f^{-1}$ est une application.

En particulier, sous ces conditions on a

$$f^{-1} \circ f = \mathrm{id}_A, \quad f \circ f^{-1} = \mathrm{id}_B \quad \text{et} \quad (f^{-1})^{-1} = f$$

## Proposition 1.5.11

Soient $f : A \to B$ et $g : B \to C$ deux applications.

1. Si $f$ et $g$ sont injectives, alors $g \circ f$ aussi ;
2. Si $f$ et $g$ sont surjectives, alors $g \circ f$ aussi ;
3. Si $f$ et $g$ sont bijectives, alors $g \circ f$ aussi. De plus, on a

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}.$$

# Images et pré-images de sous-ensembles

## Définition 1.6.1

Soient $f : A \to B$ une application, $X \subset A$ et $Y \subset B$.

1. L'image de $X$ par $f$ est l'ensemble

$$f(X) = \{f(x) : x \in X\}.$$

2. La pré-image (ou image inverse) de $Y$ par $f$ est l'ensemble

$$f^{-1}(Y) = \{x \in A : f(x) \in Y\}.$$

**Remarque :** si $f$ est une bijection, $f^{-1}(Y)$ a deux significations différentes, qui donnent le même résultat.

# Exemples : $f : \mathbb{R} \to \mathbb{R} : x \mapsto \sin(x)$

$$f([0, \frac{\pi}{2}]) =$$

$$f^{-1}([0, 1]) =$$

$$f^{-1}([\frac{1}{2}, \frac{3}{2}]) =$$

# Propriétés

## Proposition 1.6.1

Soit $f : A \to B$ une application. On a alors

1. $f^{-1}(Y \cup Z) = f^{-1}(Y) \cup f^{-1}(Z)$, pour tous $Y, Z \subset B$ ;
2. $f^{-1}(Y \cap Z) = f^{-1}(Y) \cap f^{-1}(Z)$, pour tous $Y, Z \subset B$
3. $f(Y \cup Z) = f(Y) \cup f(Z)$, pour tous $Y, Z \subset A$ ;
4. $f(Y \cap Z) \subset f(Y) \cap f(Z)$, pour tous $Y, Z \subset A$.

En général, la dernière inclusion est stricte.

## Proposition 1.6.2

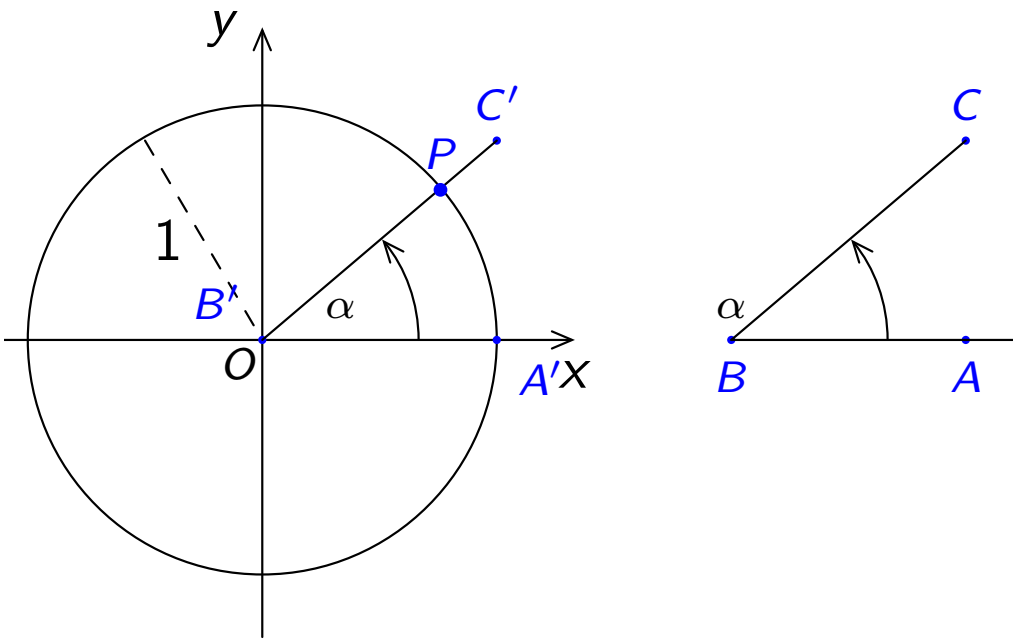
Soit $f : A \to B$ une application. Pour tout $X \subset A$ et tout $Y \subset B$,

1. On a $X \subset f^{-1}(f(X))$, l'égalité ayant lieu notamment si $f$ est injectif ;
2. On a $f(f^{-1}(Y)) \subset Y$, l'égalité ayant lieu notamment si $f$ est surjectif.

# Bijections et trigonométrie

# Degrés et radians

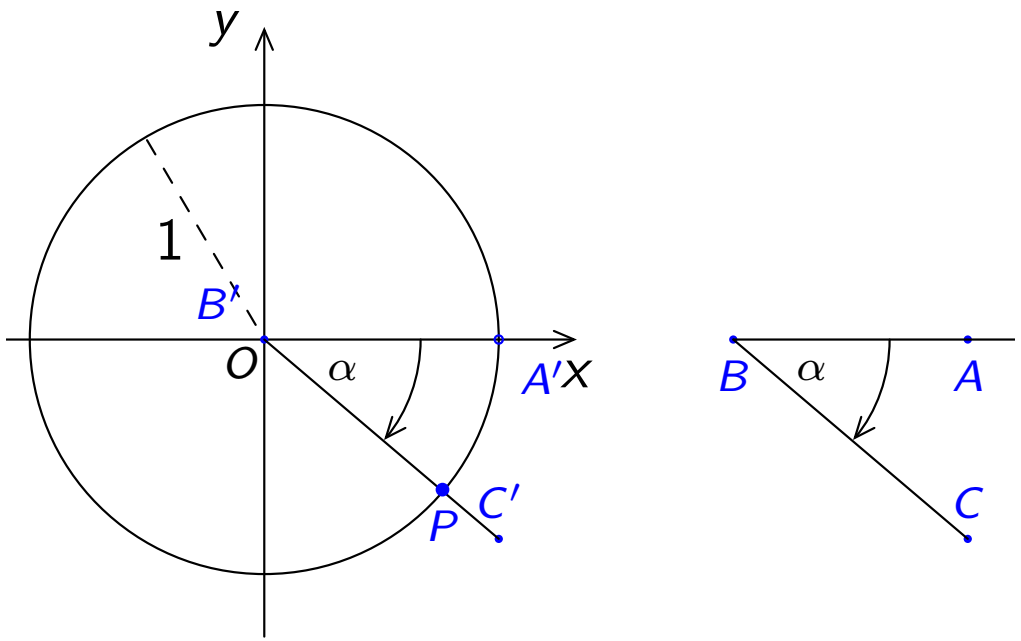
- On se donne un système d'axes orthonormés du plan, d'origine $O$ et d'axes (gradués) $x$ et $y$ ;
- Le cercle trigonométrique est le cercle **de rayon 1**, centré à l'origine $O$ ;




Tout angle orienté $\widehat{ABC}$ permet de définir un point $P$ sur le cercle trigonométrique, et vice versa.

# Degrés et radians

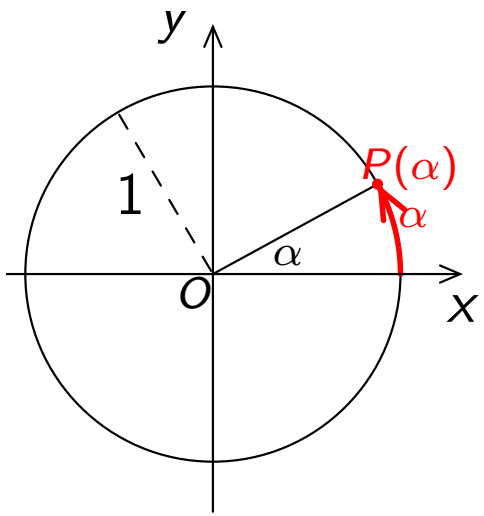
Attention, les angles sont orientés : voyez la situation suivante.

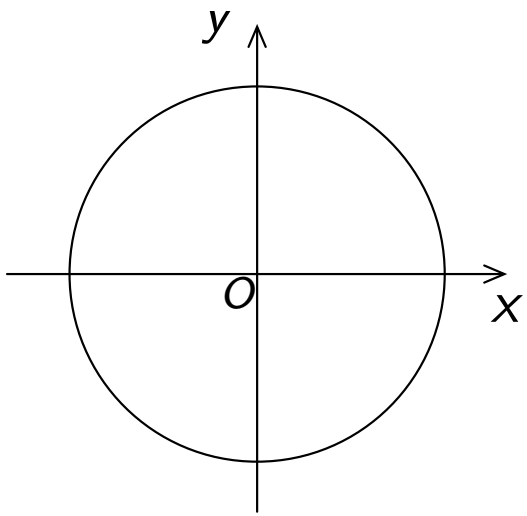



Ici, l'angle orienté $\alpha = \widehat{ABC}$ a une amplitude négative.

# Degrés et radians

- Nous avons associé à chaque amplitude $\alpha$ (en degrés) un point $P$ sur le cercle trigonométrique.
- Ce point peut aussi être repéré par la longueur d'arc parcourue (également notée $\alpha$), entre le point de coordonnées $(1, 0)$ et $P$ ;
- Cette longueur d'arc est comptée positivement si on suit le sens trigonométrique positif et négativement sinon.
- $2\pi$ correspond à 360 degrés et "longueur d'arc" (en radians) et "amplitude" (en degrés) sont directement proportionnelles.



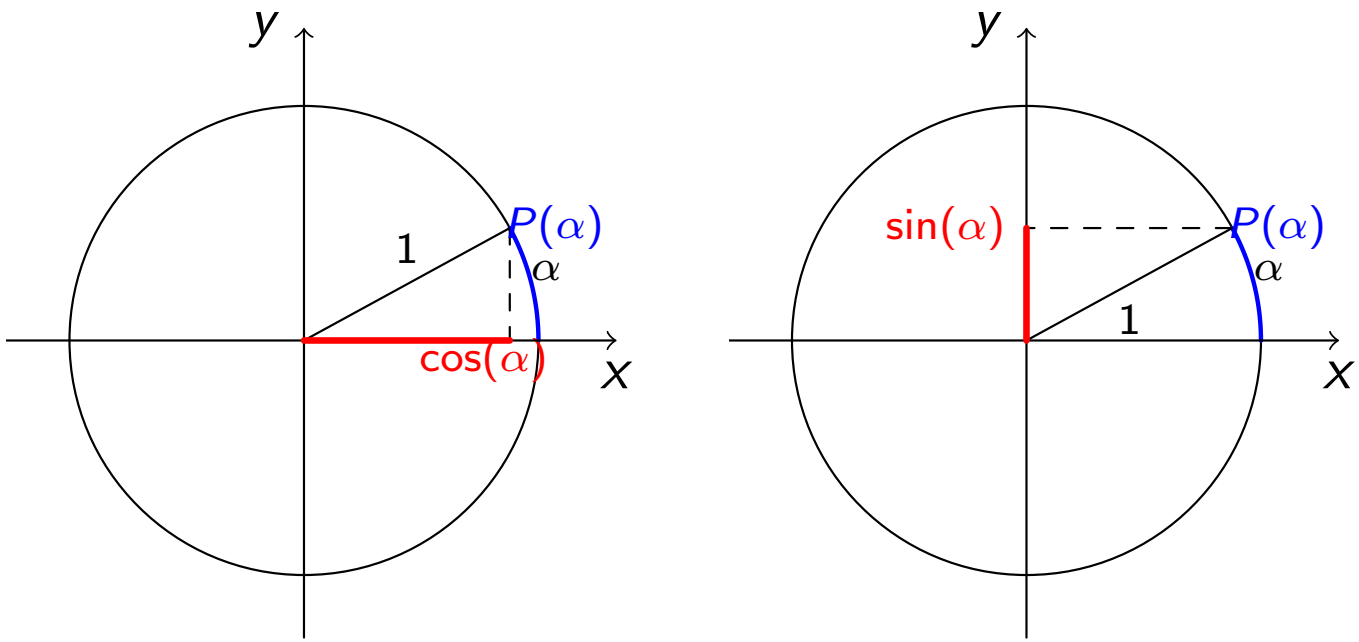



# Cosinus et sinus

Soit $\alpha$ l'amplitude d'un angle exprimée en radians ou en degrés. Par définition, les coordonnées du point $P$ correspondant du cercle trigonométrique sont

$$(\cos(\alpha), \sin(\alpha)).$$

On a donc




**Attention** : $\cos(\alpha)$ et $\sin(\alpha)$ sont des coordonnées et non des longueurs : ce sont des nombres éventuellement négatifs, compris entre $-1$ et $1$.

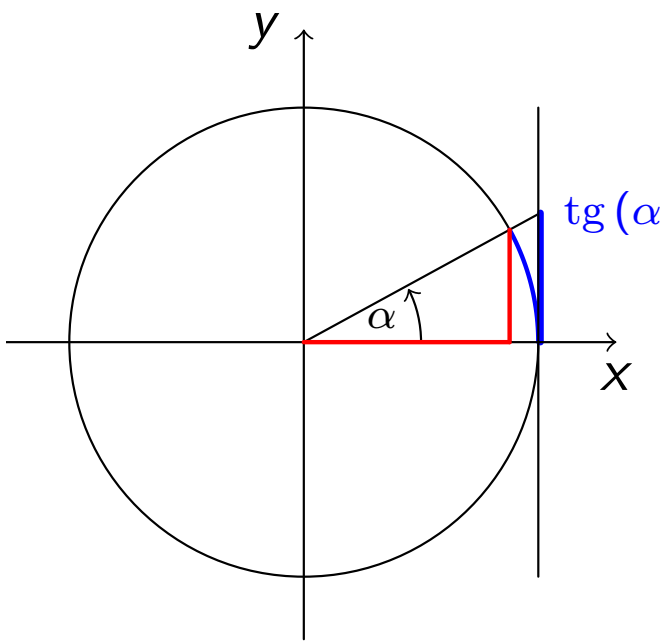
# Tangente et cotangente

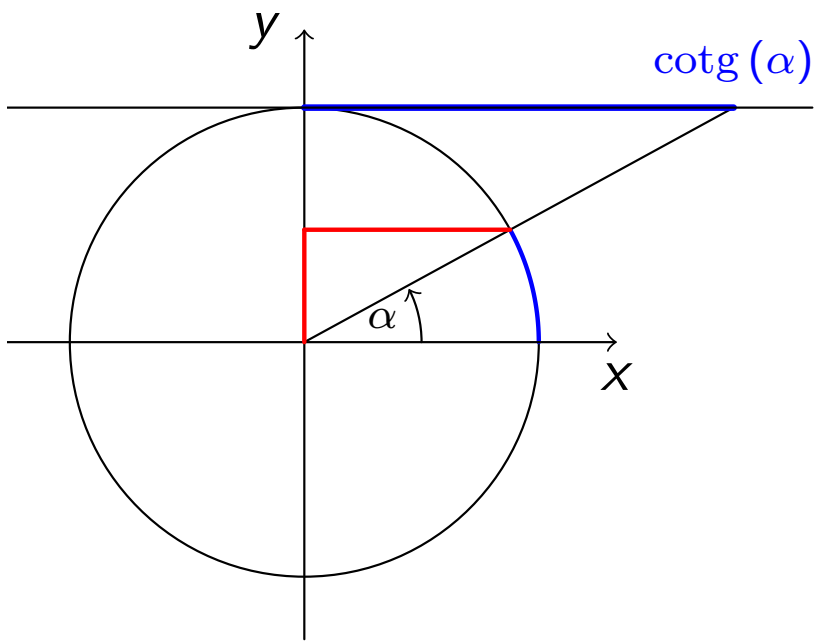
On définit la tangente et cotangente de $\alpha$ par

$$\boxed{\operatorname{tg}(\alpha) = \frac{\sin(\alpha)}{\cos(\alpha)}, \quad \text{et} \quad \operatorname{cotg}(\alpha) = \frac{\cos(\alpha)}{\sin(\alpha)}.}$$

Bien sûr, ces nombres ne sont définis que si le dénominateur est non nul.

On peut les représenter de manière géométrique.



# Premières propriétés

## Proposition : Relation fondamentale

Pour tout $\alpha \in \mathbb{R}$, on a la relation fondamentale :

$$\boxed{\cos^2(\alpha) + \sin^2(\alpha) = 1.}$$

## Proposition : $2\pi$-Périodicité

Pour tout $\alpha \in \mathbb{R}$ et tout $k \in \mathbb{Z}$, on a

$$\begin{aligned}
\cos(\alpha + 2k\pi) &= \cos(\alpha) \\
\sin(\alpha + 2k\pi) &= \sin(\alpha) \\
\operatorname{tg}(\alpha + 2k\pi) &= \operatorname{tg}(\alpha) \\
\operatorname{cotg}(\alpha + 2k\pi) &= \operatorname{cotg}(\alpha)
\end{aligned}$$

# Angles associés

## Proposition : Angles opposés

Pour tout $\alpha \in \mathbb{R}$, on a

$$\cos(2\pi-\alpha) = \cos(-\alpha) = \cos(\alpha) \quad \text{et} \quad \sin(2\pi-\alpha) = \sin(-\alpha) = -\sin(\alpha).$$

## Proposition : Angles supplémentaires

Pour tout $\alpha \in \mathbb{R}$, on a

$$\cos(\pi - \alpha) = -\cos(\alpha) \quad \text{et} \quad \sin(\pi - \alpha) = \sin(\alpha).$$

## Proposition : Angles antisupplémentaires

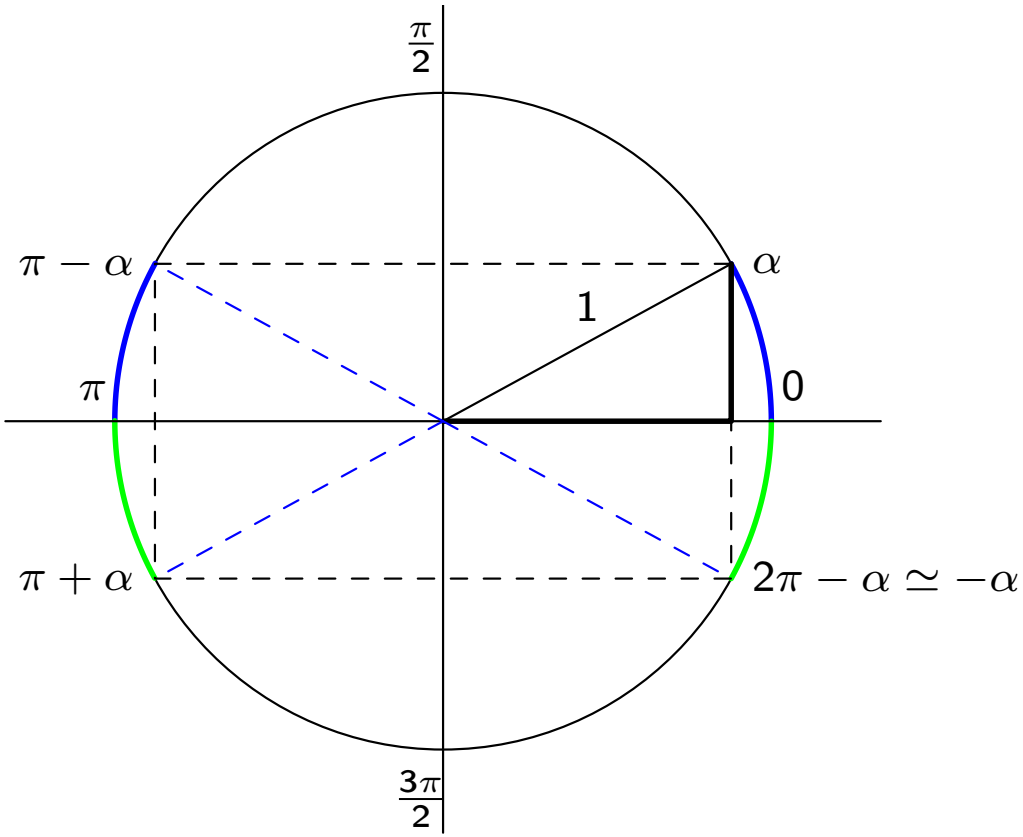
Pour tout $\alpha \in \mathbb{R}$, on a

$$\cos(\pi + \alpha) = -\cos(\alpha) \quad \text{et} \quad \sin(\pi + \alpha) = -\sin(\alpha),$$

et donc $\operatorname{tg}(\alpha + k\pi) = \operatorname{tg}(\alpha)$ et $\operatorname{cotg}(\alpha + k\pi) = \operatorname{cotg}(\alpha)$, pour tout $k \in \mathbb{Z}$.

# Une bonne nouvelle : cela se voit

Ces résultats sont dus aux symétries de la figure suivantes, qui préservent les longueurs.



# Valeurs particulières

À l'aide des identités que nous venons de montrer, on peut toujours se ramener à un angle compris entre 0 et $\frac{\pi}{2}$.

## Proposition : valeurs remarquables

On a le tableau de valeurs suivant.

| $\alpha$ | 0 | $\frac{\pi}{6}$ | $\frac{\pi}{4}$ | $\frac{\pi}{3}$ | $\frac{\pi}{2}$ |
|---|---|---|---|---|---|
| $\sin(\alpha)$ | 0 | $\frac{1}{2}$ | $\frac{\sqrt{2}}{2}$ | $\frac{\sqrt{3}}{2}$ | 1 |
| $\cos(\alpha)$ | 1 | $\frac{\sqrt{3}}{2}$ | $\frac{\sqrt{2}}{2}$ | $\frac{1}{2}$ | 0 |
| $\mathrm{tg}(\alpha)$ | 0 | $\frac{\sqrt{3}}{3}$ | 1 | $\sqrt{3}$ | – |
| $\mathrm{cotg}(\alpha)$ | – | $\sqrt{3}$ | 1 | $\frac{\sqrt{3}}{3}$ | 0 |

- Il est utile de les retenir par coeur. Les valeurs sont $\frac{\sqrt{0}}{2}, \frac{\sqrt{1}}{2}, \frac{\sqrt{2}}{2}, \frac{\sqrt{3}}{2}, \frac{\sqrt{4}}{2}$ ;
- On peut toujours les retrouver en traçant le cercle trigonométrique et en repérant les triangles particuliers.

# Formules d'addition

## Proposition

Pour tous nombres réels $\alpha$ et $\beta$, on a

1. $\cos(\alpha+\beta) = \cos(\alpha)\cos(\beta) - \sin(\alpha)\sin(\beta)$ ;
2. $\cos(\alpha-\beta) = \cos(\alpha)\cos(\beta) + \sin(\alpha)\sin(\beta)$ ;
3. $\sin(\alpha+\beta) = \sin(\alpha)\cos(\beta) + \cos(\alpha)\sin(\beta)$ ;
4. $\sin(\alpha-\beta) = \sin(\alpha)\cos(\beta) - \cos(\alpha)\sin(\beta)$.

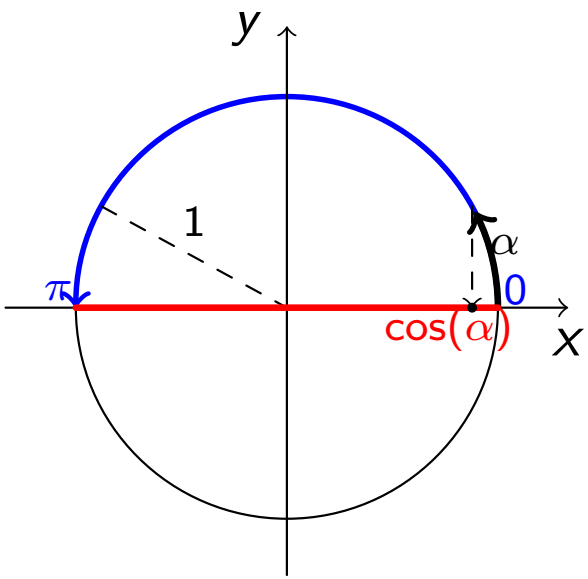
Formules revues en analyse.
On en déduit les formules de duplication (et de Carnot), ainsi que les formules de Simpson.

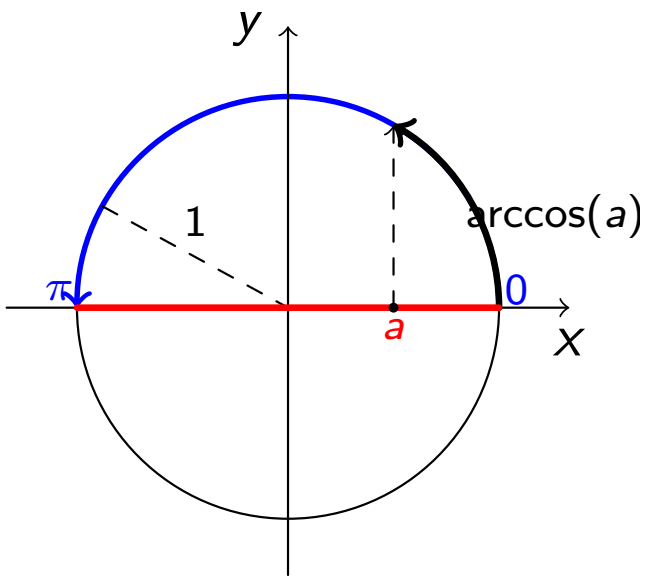
# L'arc cosinus

La fonction $\cos : \mathbb{R} \to \mathbb{R} : x \mapsto \cos(x)$ n'est pas une bijection. Mais sa restriction $\cos : [0, \pi] \to [-1, 1] : x \mapsto \cos(x)$ en est une.

## Définition

Pour tout nombre $a \in [-1, 1]$, il existe un unique nombre $\alpha \in [0, \pi]$ tel que $\cos(\alpha) = a$. Ce nombre est appelé $\arccos(a)$.




L'arc cosinus jouit des propriétés suivantes.

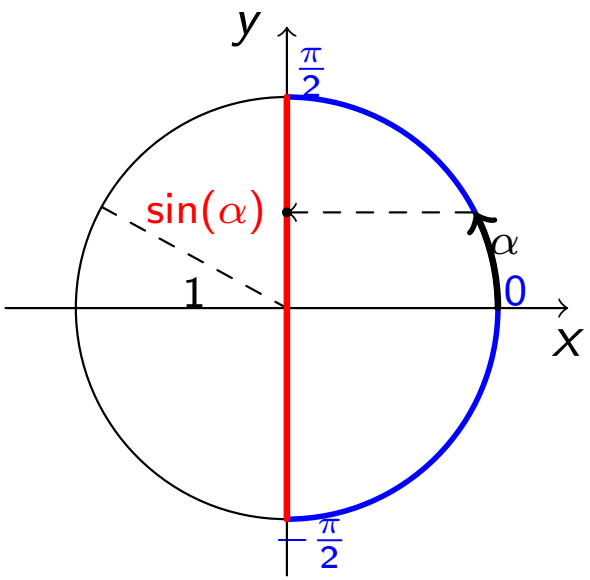
- $\cos(\arccos x) = x, \quad \forall x \in [-1, 1]$ ;
- $\arccos(\cos x) = x, \quad \forall x \in [0, \pi]$ ;

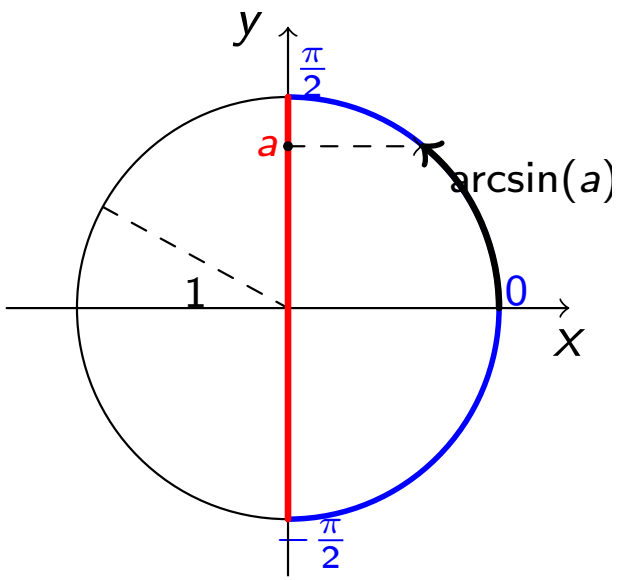
# L'arc sinus

La fonction $\sin : \mathbb{R} \to \mathbb{R} : x \mapsto \sin(x)$ n'est pas une bijection. Mais sa restriction $\sin : [-\frac{\pi}{2}, \frac{\pi}{2}] \to [-1, 1] : x \mapsto \sin(x)$ en est une.

## Définition

Pour tout nombre $a \in [-1, 1]$, il existe un unique nombre $\alpha \in [-\frac{\pi}{2}, \frac{\pi}{2}]$ tel que $\sin(\alpha) = a$. Ce nombre est appelé $\arcsin(a)$.




La fonction arc sinus a les propriétés suivantes.

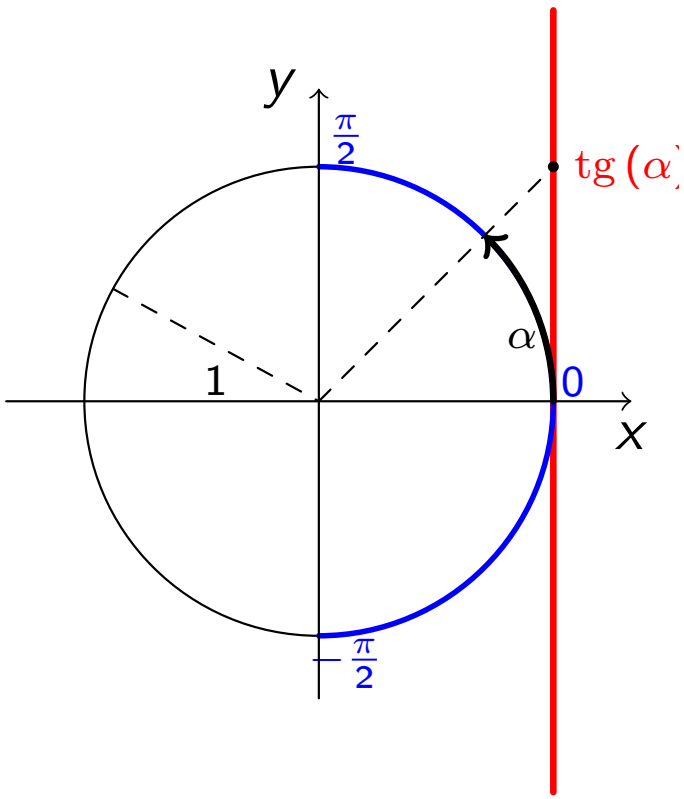
- On a $\sin(\arcsin x) = x, \quad \forall x \in [-1, 1]$ ;
- On a $\arcsin(\sin x) = x, \quad \forall x \in [-\frac{\pi}{2}, \frac{\pi}{2}]$ ;

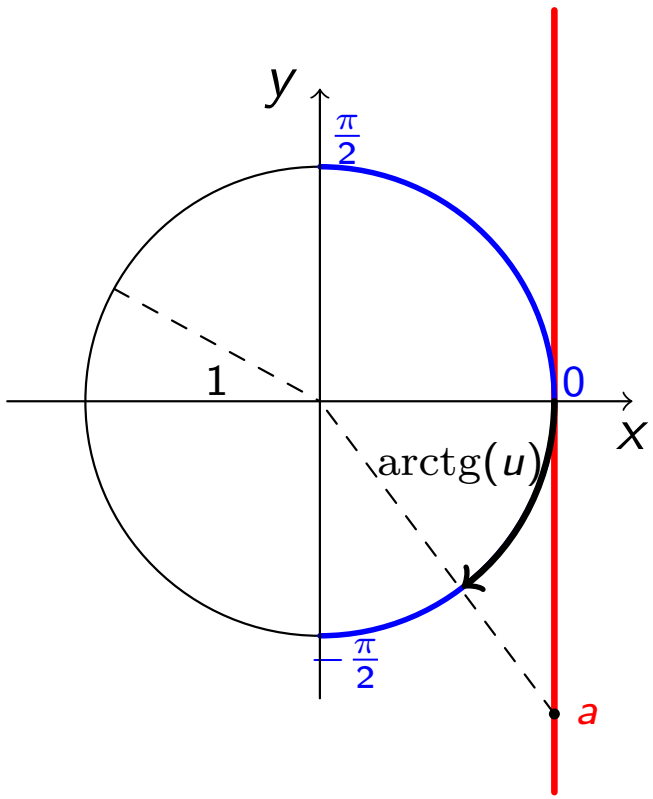
# L'arc tangente

L'application $\mathrm{tg} : ]-\frac{\pi}{2}, \frac{\pi}{2}[ \to \mathbb{R} : x \mapsto \mathrm{tg}(x)$ est une bijection.

## Définition

Pour tout nombre $a \in \mathbb{R}$, il existe un unique nombre $\alpha \in ]-\frac{\pi}{2}, \frac{\pi}{2}[$ tel que $\mathrm{tg}(\alpha) = a$. Ce nombre est appelé $\mathrm{arctg}(a)$.



# Equations trigonométriques

## Equations en cosinus

L'équation $\cos(\alpha) = a$ admet les solutions suivantes :
Si $a \notin [-1, 1]$, il n'y a pas de solution. Si $a \in [-1, 1]$, on a les solutions :

$$\alpha = \arccos(a) + 2k\pi, (k \in \mathbb{Z}), \quad \text{ou} \quad \alpha = -\arccos(a) + 2k\pi, (k \in \mathbb{Z}).$$

## Equations en sinus

L'équation $\sin(\alpha) = a$ admet les solutions suivantes :
Si $a \notin [-1, 1]$, il n'y a pas de solution. Si $a \in [-1, 1]$, on a les solutions :

$$\alpha = \arcsin(a) + 2k\pi, (k \in \mathbb{Z}), \quad \text{ou} \quad \alpha = \pi - \arcsin(a) + 2k\pi, (k \in \mathbb{Z}).$$

## Equations en tangente

L'équation $\mathrm{tg}\,(\alpha) = a$ admet les solutions suivantes :

$$\alpha = \mathrm{arctg}(a) + 2k\pi, (k \in \mathbb{Z}), \quad \text{ou} \quad \alpha = \pi + \mathrm{arctg}(a) + 2k\pi, (k \in \mathbb{Z}).$$

# Nombres complexes (version light)

# Équations du second degré

On veut résoudre $ax^2 + bx + c = 0$, pour $a \neq 0$ et $x \in \mathbb{R}$.

## Proposition

*Notons $\Delta = b^2 - 4ac$ (le discriminant).*

1. *si $\Delta > 0$ : l'équation admet deux solutions distinctes : on a*
$$S = \{\frac{-b - \sqrt{\Delta}}{2a}, \frac{-b + \sqrt{\Delta}}{2a}\}.$$
2. *si $\Delta = 0$ : l'équation admet une seule solution : $S = \{\frac{-b}{2a}\}$. On dit que la solution $\frac{-b}{2a}$ est double.*
3. *Si $\Delta < 0$ : l'équation n'admet pas de solution. On note $S = \emptyset$ ;*

# Factorisation, somme et produit

## Proposition

*Si $a \neq 0$ et $\Delta \geqslant 0$, l'équation $ax^2 + bx + c = 0$ admet les solutions $x_1$ et $x_2$ (éventuellement égales), et le trinôme correspondant se factorise :*

$$ax^2 + bx + c = a(x - x_1)(x - x_2) \quad \forall x \in \mathbb{R}.$$

*De plus, la somme des solutions vaut $\frac{-b}{a}$ et leur produit vaut $\frac{c}{a}$.*

## Proposition (Réciproque)

*Si $n_1$ et $n_2$ sont deux nombres dont la somme est $s$ et le produit $p$, alors ces nombres sont solutions de l'équation*

$$x^2 - sx + p = 0.$$

**Preuve :** Il suffit d'exprimer les conditions.

# Nombres complexes

## Définition

On définit l'ensemble des nombres complexes par

$$\mathbb{C} = \{(x, y) : x, y \in \mathbb{R}\}.$$

## Définition

On définit l'addition des nombres complexes par

$$+ : \mathbb{C} \times \mathbb{C} \to \mathbb{C} : ((x, y), (x', y')) \mapsto (x + x', y + y'),$$

et on définit la multiplication par

$$\cdot : \mathbb{C} \times \mathbb{C} \to \mathbb{C} : ((x, y), (x', y')) \mapsto (xx' - yy', xy' + x'y)$$

# Structure de champ de $\mathbb{C}$

On note $0$ l'élément $(0,0)$ de $\mathbb{C}$ et on note $1$ l'élément $(1,0)$ de $\mathbb{C}$.

**Proposition**

$(\mathbb{C}, +, \cdot, 0, 1)$ *est un champ.*

**Preuve :** Avec les matheux uniquement.

# Plongement de $\mathbb{R}$ dans $\mathbb{C}$

## Proposition

*L'application* $j : \mathbb{R} \to \mathbb{C}, x \mapsto (x, 0)$ *est une injection ayant les propriétés suivantes :*

1. $j(x + x') = j(x) + j(x')$ *pour tous* $x, x' \in \mathbb{R}$ ;
2. $j(x.x') = j(x).j(x')$ *pour tous* $x, x' \in \mathbb{R}$ ;

- Conséquence : en identifiant $x$ à $j(x)$, on peut considérer que $\mathbb{R} \subset \mathbb{C}$.
- Si $a \in \mathbb{R}$, et $z = (x, y) \in \mathbb{C}$, on définit $a.z = j(a).z = (ax, ay)$.

## Proposition

*Tout nombre complexe* $z$ *s'écrit de manière unique*

$$z = x(1, 0) + y(0, 1) = x.1 + y.(0, 1), \quad x, y \in \mathbb{R}.$$

# Le nombre $i$

## Définition

Nous notons $i$ le nombre complexe $(0, 1)$.

## Proposition

*Tout nombre complexe* $(x, y)$ $(x, y \in \mathbb{R})$ *s'écrit de manière unique* $x + iy$, $x, y \in \mathbb{R}$. *On a* $i^2 = -1$.

## Définition

Si $x, y$ sont réels, l'écriture $x + iy$ est l'écriture sous forme algébrique du nombre complexe $(x, y)$.

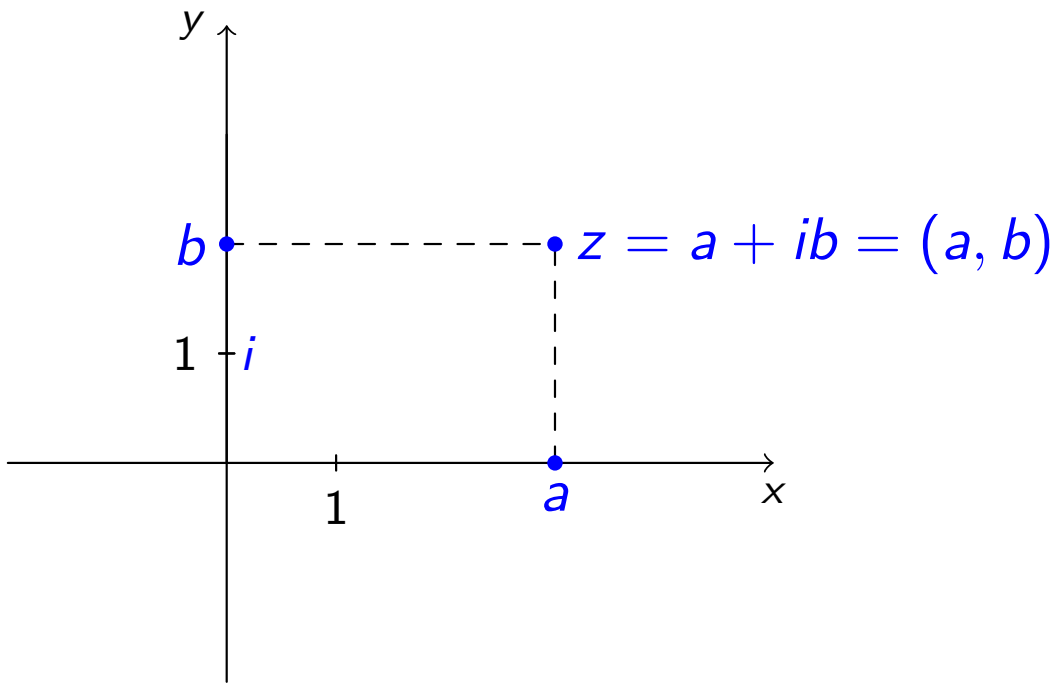
## Proposition

*On a, pour tous réels* $x, x', y, y'$ *:*

- $(x + iy) + (x' + iy') = x + x' + i(y + y')$ ;
- $(x + iy)(x' + iy') = xx' - yy' + i(xy' + x'y)$.

# Représentation cartésienne des nombres complexes

**L'idée** : on a $\mathbb{C} = \mathbb{R}^2$. On utilise la **représentation** de $\mathbb{R}^2$ au moyen d'un repère orthonormé. On parle de plan complexe.



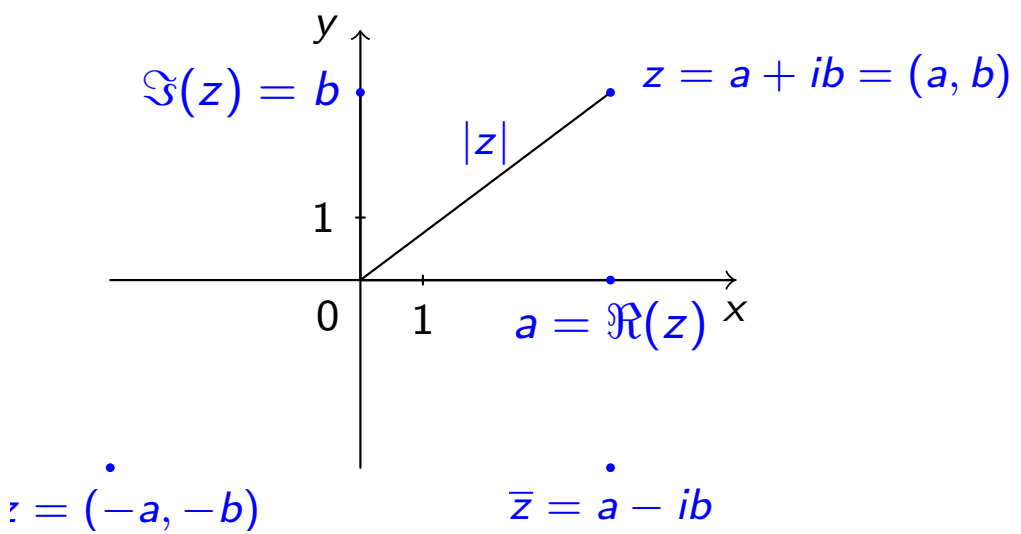

- Attention, les nombres portés sur le deuxième axe ne sont pas réels, mais imaginaires purs : si on reporte $b$ sur l'axe des ordonnées, on représente le coupe $(0, b)$ et donc le nombre complexe $ib = (0, b)$.

# Nombres associés

## Définition

Pour tout nombre complexe $z = a + ib$ $(a, b \in \mathbb{R})$, on définit

1. la partie réelle de $z$ par $\Re(z) = a$ ;
2. la partie imaginaire de $z$ par $\Im(z) = b$ ; Attention : pas $ib$
3. Le nombre complexe conjugué de $z$ par $\overline{z} = a - ib$ ;
4. le module de $z$ : $|z| = \sqrt{a^2 + b^2} = \sqrt{z \cdot \overline{z}}$ ;




**Exemple :** Pour $z = 1 + \sqrt{3}i$, calculer $\Re(z), \Im(z), \overline{z}$ et $|z|$.

# Propriétés

## Proposition (Conjugué)

*Pour tous nombres complexes $z_1$ et $z_2$, on a*

1. $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$, $\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$ *et* $\overline{\overline{z_1}} = z_1$ ;
2. *Si* $z_2 \neq 0$, *alors* $\overline{\left(\frac{z_1}{z_2}\right)} = \frac{\overline{z_1}}{\overline{z_2}}$ ;
3. *Si* $z_1 \neq 0$, *on a* $\frac{1}{z_1} = \frac{\overline{z_1}}{|z_1|^2}$.

## Proposition (Parties réelles et imaginaires)

*Pour tout nombre complexe $z$,*

1. *On a* $\Re(z) = \frac{z+\overline{z}}{2}$ *et* $\Im(z) = \frac{z-\overline{z}}{2i}$ ;
2. $z$ *est réel ssi* $\Im(z) = 0$ *ssi* $z = \overline{z}$ ;
3. $z$ *est imaginaire pur ssi* $\Re(z) = 0$ *ssi* $z = -\overline{z}$.

**Exemple :** Mettre $\frac{3+i}{4-i}$ sous forme algébrique.

# Propriétés - suite

## Proposition (Module)

*Pour tous nombres complexes $z$, $z_1$, $z_2$*

1. $|z|^2 = z\overline{z}$, $|\overline{z}| = |z|$ ;
2. $|z_1 z_2| = |z_1||z_2|$ *et si* $z_2 \neq 0$, $|\frac{z_1}{z_2}| = \frac{|z_1|}{|z_2|}$ ;
3. $|z_1 + z_2|^2 = |z_1|^2 + |z_2|^2 + 2\Re(z_1\overline{z_2})$

## Proposition (Inégalités)

*Pour tous nombres complexes $z$, $z_1$, $z_2$*

1. $|\Re(z)| \leqslant |z|$, $|\Im(z)| \leqslant |z|$ ;
2. *On a l'inégalité triangulaire* $|z_1 + z_2| \leqslant |z_1| + |z_2|$.
3. *De plus* $|z_1 - z_2| \geqslant ||z_1| - |z_2||$

# Exponentielle complexe

## Définition (Exponentielle complexe)

Si $z = a + ib$, où $a, b \in \mathbb{R}$, on définit

$$e^z = e^a(\cos(b) + i\sin(b)).$$

**Remarques importantes :**

1. Ici $e^z$ est défini à partir des fonctions réelles exp, cos et sin. Dans le cours d'analyse, on fera le chemin en sens inverse.
2. Si $a, b \in \mathbb{R}$, $e^a = e^a$ et $e^{ib} = \cos(b) + i\sin(b) =$ "$cis(b)$".

## Proposition

*Pour tous nombres complexes $z, z_1, z_2$, on a*

1. $e^{z_1}e^{z_2} = e^{z_1+z_2}$ ;
2. $\frac{1}{e^z} = e^{-z}$ ;
3. $(e^z)^n = e^{nz}, \forall z \in \mathbb{N}$.
4. *Pour tout $x \in \mathbb{R}$, on a $|e^{ix}| = 1$.*

# Formules pour le cosinus et le sinus

**Proposition**

*On a*

$$\cos(x) = \Re(e^{ix}) = \frac{e^{ix} + e^{-ix}}{2}, \quad \textit{et} \quad \sin(x) = \Im(e^{ix}) = \frac{e^{ix} - e^{-ix}}{2i}$$

*pour tout* $x \in \mathbb{R}$.

**Utilisation :**

1. Récupérer les formules de Carnot.
2. Exprimer $\cos^3(x)$ en fonction de $\cos(3x)$ et $\cos(x)$.
3. Faire de même avec $\sin^3(x)$.
4. Se souvenir des formules d'addition : $\cos(x+y) = \Re(e^{i(x+y)})$, de même avec le sinus.

# Forme trigonométrique/exponentielle

## Proposition

*Si $z = a + ib$ est un nombre complexe non nul, alors il existe un unique $\theta \in [0, 2\pi[$ et un unique $\rho \in ]0, +\infty[$ tels que $z = \rho e^{i\theta}$.*

Cette écriture du nombre complexe $z$ est appelée forme exponentielle ou forme trigonométrique de $z$.

**Preuve :** Pour l'existence, on constate que si $\rho = |z|$, alors $\frac{z}{\rho}$ est de module 1. L'unicité est classique.

## Définition

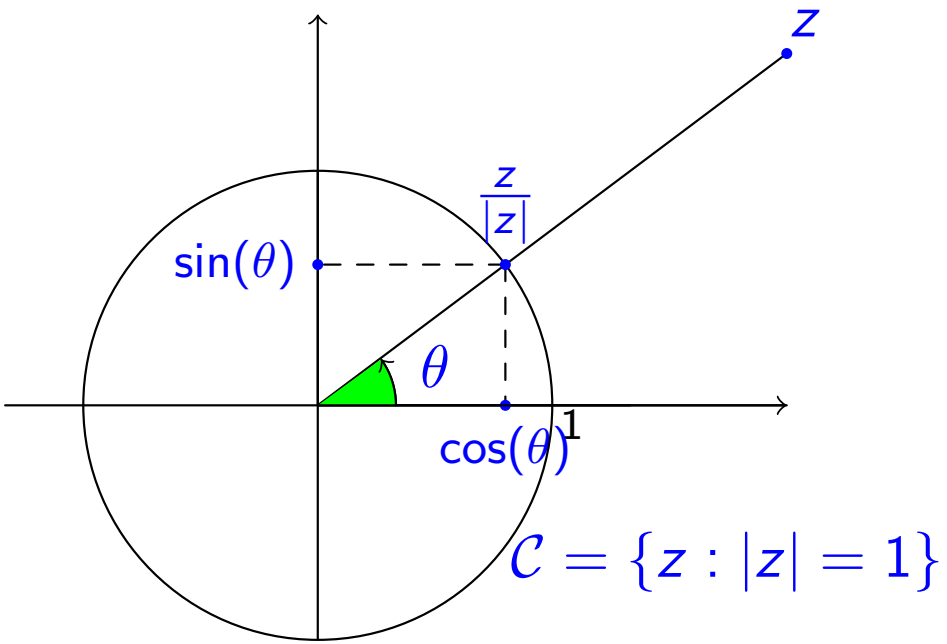
L'angle $\theta$ de la proposition précédente est appelé l'argument de $z$. Par extension, on appellera aussi argument de $z$ tout angle $\theta'$ tel que $\theta' - \theta = 2k\pi$, $k \in \mathbb{Z}$.

**Exemple :**

Trouver la forme trigonométrique de $z = 1 + \sqrt{3}i$

Calculer $z^6$.

# Une représentation




## Proposition

*L'application qui à tout* $z = (a, b) \in \mathbb{C} \setminus \{0\}$ *associe le couple* $(\rho, \theta)$ *est une bijection de* $\mathbb{C} \setminus \{0\}$ *sur son image* $]0; +\infty[\times[0; 2\pi[$.

**Remarque :** En géométrie, il s'agit du passage en coordonnées polaires.

# Multiplication, et formule de Moivre

## Proposition

*On a, pour tous* $z_1 = \rho_1 e^{i\theta_1}$ *et* $z_2 = \rho_2 e^{i\theta_2}$

1. $z_1 z_2 = \rho_1 \rho_2 e^{i(\theta_1+\theta_2)}$ ;
2. $z_1^{-1} = \frac{1}{\rho_1} e^{-i\theta_1}$ ;
3. $z_1^n = \rho_1^n e^{in\theta_1}$, *pour tout* $n \in \mathbb{Z}$.

## Corollaire (Formule de Abraham de Moivre (1667-1754))

*On a, pour tout* $\theta \in \mathbb{R}$ *et tout* $n \in \mathbb{Z}$ *:*

$$(\cos(\theta) + i\sin(\theta))^n = \cos(n\theta) + i\sin(n\theta)$$

**Application :** Utiliser cette formule pour obtenir des expressions de $\cos(3\theta)$ et $\sin(3\theta)$.

# Racines carrées

## Définition

Pour tout nombre complexe $z$, on appelle **une** racine carrée de $z$ tout nombre $w$ tel que $w^2 = z$.

## Proposition

*Tout nombre complexe non nul admet exactement deux racines carrées opposées. Le nombre complexe* 0 *admet une seule racine carrée, qu'on dira racine double.*

**Preuve :** 1) Le cas de 0 est trivial. 2) Prendre la forme trigonométrique.

**Remarque :**

Il est moins facile de privilégier une de ces racines que dans le cas des nombres réels. On évitera donc la notation $\sqrt{z}$, qui fait penser à une application.

# Les racines carrées, via la forme algébrique

- Soit $z = a + ib$ $(a, b \in \mathbb{R})$. On cherche $w = x + iy$ $(x, y \in \mathbb{R})$ tel que $w^2 = z$.
- Si $b = 0$, c'est facile. Donc considérons $b \neq 0$.
- En utilisant $w^2 = z$ et $|w|^2 = |z|$, on obtient le système

$$\begin{cases} x^2 - y^2 &= a \\ 2xy &= b \\ x^2 + y^2 &= \sqrt{a^2 + b^2} \end{cases}$$

- Les équations 1 et 3 donnent

$$x^2 = \frac{\sqrt{a^2 + b^2} + a}{2} = \tilde{x} \quad \text{et} \quad y^2 = \frac{\sqrt{a^2 + b^2} - a}{2} = \tilde{y}$$

et on doit choisir 2 solutions parmi

$$(\sqrt{\tilde{x}}, \sqrt{\tilde{y}}),\ (-\sqrt{\tilde{x}}, -\sqrt{\tilde{y}}),\ (\sqrt{\tilde{x}}, -\sqrt{\tilde{y}}),\ (-\sqrt{\tilde{x}}, \sqrt{\tilde{y}}).$$

- Ce choix est donné par le signe de $b$.

# Retour aux équations du deuxième degré

On considère l'équation

$$az^2 + bz + c = 0,$$

où l'inconnue $z$ est complexe, et $a, b, c$ aussi, et où $a \neq 0$.

## Proposition

*Cette équation admet toujours exactement deux solutions, éventuellement confondues (on dira "comptées avec leur multiplicité"). Elles sont données par la formule* $\frac{-b \pm \delta}{2a}$ *où* $\delta^2 = \Delta = b^2 - 4ac$.

**Preuve :** On reprend la décomposition

$$az^2 + bz + c = a[(z + \frac{b}{2a})^2 - \frac{\Delta}{4a^2}]$$

Mais $\Delta = \delta^2$ (toujours), donc $\frac{\Delta}{4a^2} = (\frac{\delta}{2a})^2$. On factorise :

$$az^2 + bz + c = a(z + \frac{b}{2a} + \frac{\delta}{2a})(z + \frac{b}{2a} - \frac{\delta}{2a}).$$

# Factorisation, somme et produit

## Proposition

*Le trinôme du deuxième degré* $az^2 + bz + c$ *se factorise* ***toujours*** *: on a*

$$az^2 + bz + c = a(z - z_1)(z - z_2), \quad \forall z \in \mathbb{C},$$

*où* $z_1, z_2$ *sont les solutions de l'équation* $az^2 + bz + c = 0$.
*De plus, on a* $z_1 + z_2 = \frac{-b}{a}$ *et* $z_1 z_2 = \frac{c}{a}$.

**Remarque :**
Ça se généralise aux polynômes de degré $n$, pour tout $n \geqslant 1$.

**Exemples :** Déterminer les racines (dans $\mathbb{C}$) et factoriser

- $x^2 + 4x + 8$
- $(1 + i)z^2 + iz - 1$.

# Le cas des équations à coefficients réels

**Proposition**

*Si $a, b, c \in \mathbb{R}$, l'ensemble des solutions dans $\mathbb{C}$ de $ax^2 + bx + c = 0$ est stable par conjugaison.*

**Preuve :**

- Si $\Delta \geqslant 0$, les solutions sont réelles.
- Sinon, elles s'écrivent $\frac{-b \pm i\sqrt{-\Delta}}{2a}$ et sont conjuguées l'une de l'autre.

**Généralisation :**

- Si $P$ est une fonction polynomiale à coefficients réels, alors le résultat reste vrai.
- En fait, dans ce cas, on a $P(\overline{z}) = \overline{P(z)}$, pour tout $z \in \mathbb{C}$.

# Puissances $n$-èmes et binôme de Newton

Si on veut calculer une puissance $n$-ème d'un nombre complexe, soit on utilise la forme trigonométrique, soit la forme algébrique. Dans ce cas, on est amené à calculer $(a+ib)^n$. C'est la $n$-ème puissance d'un binôme.

## Définition

Pour tous $k, n \in \mathbb{N}$ tels que $0 \leqslant k \leqslant n$, on définit le coefficient binomial

$$C_n^k = \frac{n!}{k!(n-k)!}.$$

**Remarques :**

- On pose $0! = 1$, donc $C_n^0 = C_n^n = 1$.
- Le nombre $C_n^k$ est le nombre de façons de choisir $k$ objets parmi $n$ objets distincts, l'ordre n'ayant pas d'importance.

# Triangle de Pascal et binôme de Newton

## Proposition

*Pour tout $n \geqslant 1$ et tout $k$ tel que $0 \leqslant k \leqslant n$,*

$$C_n^k + C_n^{k+1} = C_{n+1}^{k+1}$$

**Preuve :** Calculer.

## Proposition (Formule du binôme de Newton)

*Pour tous nombres complexes $w$ et $z$, et tout $n \in \mathbb{N}$, on a*

$$(w+z)^n = \sum_{k=0}^{n} C_n^k w^k z^{n-k}.$$

**Preuve :** Par récurrence, ou développer

$$(w+z)^n = (w+z)\cdots(w+z).$$

# Racines $n$-èmes

## Definition

Une racine $n$-ème d'un nombre complexe $z$ est un nombre complexe $w$ tel que $w^n = z$.

## Proposition

*Tout nombre complexe non nul admet n racines n-èmes distinctes.*

**Preuve :** Il suffit de considérer l'équation, sous forme exponentielle. Les racines $n$-èmes de $\rho e^{i\theta}$ sont alors

$$\sqrt[n]{\rho} e^{i\frac{\theta+2k\pi}{n}}, k \in \{0, \ldots, n-1\}.$$

## Definition

Les racines $n$-èmes de l'unité sont les nombres $z$ tels que $z^n = 1$. Elles sont données par

$$e^{i\frac{2k\pi}{n}}, k \in \{0, \ldots, n-1\}.$$

# Quelques propriétés

## Proposition

- *Les racines n-èmes de l'unité sont les puissances successives de* $\omega_n = e^{i\frac{2\pi}{n}}$.
- *Les raines n-èmes de l'unité ont un module égal à 1.*
- *Les racines n-èmes de l'unité sont les sommets d'un polygone régulier à n côtés.*
- *Si* $n \geqslant 2$, *la somme des racines n-èmes de l'unité est nulle.*
- *L'ensemble des racines n-èmes de* $w \in \mathbb{C}$ *s'écrit* $\{w_0\omega_n^k : k \in \{0, \ldots, n-1\}\}$, *si* $w_0$ *est une racine n-ème de* $w$.

# Racines $n$-èmes primitives

## Définition

Une racine $n$-ème de l'unité $\omega$ est primitive si $n$ est le plus petit $t \in \mathbb{N}_0$ tel que $\omega^t = 1$.

**Exemple :** $-1$ n'est pas une racine quatrième primitive de l'unité. Mais $i$ et $-i$ le sont.

## Proposition

*Si $\omega$ est une racine n-ème primitive de l'unité, alors les racines n-èmes de l'unité sont $\{\omega, \omega^2, \ldots, \omega^n = 1\}$.*

## Proposition

*Si $e^{\frac{i2k\pi}{n}}$ est une racine primitive, alors $k$ et $n$ sont premiers entre eux.*

**Remarque :** La réciproque est vraie.

# Cardinalité des ensembles finis

# Qui est le plus gros ?

La cardinalité d'un ensemble est une mesure de sa taille.

On peut facilement dire qui de

$$\{1, 2, 3\} \qquad \text{et} \qquad \mathbb{N}$$

est le plus "gros", i.e., contient le plus d'éléments.

Mais qu'en est-il entre

$$\mathbb{N}, \quad \mathbb{Z}, \quad \mathbb{Q}, \quad \mathbb{R}, \quad \mathbb{C}, \quad [0, 1], \quad \{2n \mid n \in \mathbb{N}\}, \ldots ?$$

L'intuition dirait que $\mathbb{R}$ est plus gros que $\mathbb{N}$, mais

- comment le formaliser ?
- que dit l'intuition pour $\mathbb{Q}$ et $\mathbb{R}$ ?

# Une première tentative de classement

Une idée naturelle est de classer les ensembles par inclusion :

"$A$ est plus gros que $B$ si $B \subset A$"

Si $X$ est un ensemble, l'inclusion $\subset$ définit sur $\mathcal{P}(X)$ une *relation d'ordre*.

## Définition 3.3.1

Une relation $\mathcal{R}$ de $A$ dans $A$ est une relation d'ordre si elle est :

1. réflexive : pour tout $a \in A$, $a\mathcal{R}a$ ;
2. antisymétrique : pour tous $a, b \in A$, si $a\mathcal{R}b$ et $b\mathcal{R}a$, alors $a = b$ ;
3. transitive : pour tous $a, b, c \in A$, si $a\mathcal{R}b$ et $b\mathcal{R}c$, alors $a\mathcal{R}c$.

On dit alors que $(A, \mathcal{R})$ est un ensemble ordonné.

**Interpréter** ces propriétés dans la représentation cartésienne de $\mathcal{R}$.

## Exemple

$(\mathbb{N}, \leq)$ et $(\mathcal{P}(X), \subset)$ sont des ensembles ordonnés.

# $\subset$ n'est pas satisfaisant

On ne peut pas tout comparer :

$$\{2n \mid n \in \mathbb{Z}\} \not\subset \mathbb{N} \quad \text{et} \quad \{2n \mid n \in \mathbb{Z}\} \not\supset \mathbb{N}$$
$$\{2n \mid n \in \mathbb{Z}\} \not\subset \{1,2,3\} \quad \text{et} \quad \{2n \mid n \in \mathbb{Z}\} \not\supset \{1,2,3\}$$

**Definition**

Un ordre $\mathcal{R}$ sur $A$ est total si pour tous $a, b \in A$, on a $a\mathcal{R}b$ ou $b\mathcal{R}a$.
On dit alors que $(A, \mathcal{R})$ est un ensemble totalement ordonné.

**Exemple**

$(\mathbb{N}, \leq)$ est totalement ordonné ; $(\mathcal{P}(X), \subset)$ ne l'est pas.

# Ce qu'on veut, c'est pouvoir "compter"

## Définition 4.1.2

Un ensemble $A$ est fini s'il est vide ou s'il existe $n \in \mathbb{N}_0$, tel que $A$ soit en bijection avec $\{0, \ldots, n-1\}$. Sinon, il est infini.
Le cardinal d'un ensemble fini $A$ est

$$|A| = \#A = \begin{cases} 0, & \text{si } A = \varnothing; \\ n, & \text{si } A \text{ est en bijection avec } \{0, \ldots, n-1\}. \end{cases}$$

**Remarques :**

1. On a une bijection évidente entre $\{0, \ldots, n-1\}$ et $\{1, \ldots, n\}$ ;
2. C'est ce que l'on fait quand on compte des objets ;
3. Il faut cependant que si $\{0, \ldots, n-1\}$ et $\{0, \ldots, m-1\}$ sont en bijection, alors $m = n$.

# Le cardinal des ensembles finis est bien défini

## Lemme 4.1.2

L'ensemble vide n'est en bijection avec aucun ensemble non vide.

## Lemme 4.1.1

Si $f : A \to B$ est une bijection, pour tout $A' \subset A$, $f|_{A'} : A' \to f(A')$ est une bijection.

## Lemme 4.1.3

Pour tout $n \geqslant 2$, et pour tout $i \in \{0, \ldots, n-1\}$, l'ensemble $\{0, \ldots, n-1\} \setminus \{i\}$ est en bijection avec $\{0, \ldots, n-2\}$.

## Proposition 4.1.4

Si $m, n \in \mathbb{N}_0$ sont tels que $\{0, \ldots, n-1\}$ et $\{0, \ldots, m-1\}$ soient en bijection, alors on a $m = n$.

**Définition 4.2.3**

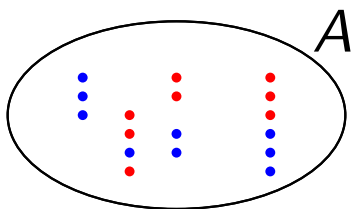
Soit $A$ un ensemble. Une partition de $A$ est une famille de sous-ensembles de $A$ deux à deux disjoints et dont l'union est égale à $A$.

**Exemples :**

1. Soit $A = \{1, 2, 3, 4, 5\}$. Alors $\{\{1, 2\}, \{3, 4\}, \{5\}\}$ est une partition de $A$.
2. Soit $A = \mathbb{N}$. Posons $A_0 = 2\mathbb{N}$, l'ensemble des nombres pairs et $A_1 = I$, l'ensemble des nombres impairs. Alors $\{A_0, A_1\}$ est une partition de $\mathbb{N}$.
3. Soit $A = \mathbb{R}^2$. Pour tout $x \in \mathbb{R}$, définissons $E_x = \{(x, y) : y \in \mathbb{R}\}$. Alors $\{E_x : x \in \mathbb{R}\}$ est une partition de $\mathbb{R}^2$.

# Partitions d'un ensemble fini et comptages

On s'intéresse au cardinal d'un ensemble fini $A$ :




On regroupe les éléments selon un "critère" (couleur, paquets verticaux, ...). À chaque fois, on réalise une partition de l'ensemble $A$ (en sous-ensembles non vides).

**Proposition**

Si $\{A_1, \ldots, A_m\}$ est une partition d'un ensemble fini $A$, alors $|A| = \sum_{i=1}^{m} |A_i|$.

# Cardinalité et applications

## Proposition

Soient $A$ et $B$ deux ensembles finis.

1. $\#A = \#B$ si et seulement s'il existe une bijection $f : A \to B$
2. $\#A \leq \#B$ si et seulement s'il existe une injection $f : A \to B$
3. $\#A \geq \#B$ si et seulement s'il existe une surjection $f : A \to B$

## Proposition

Soient $A$ et $B$ deux ensembles finis et $f : A \to B$ une application.

1. Si $\#A \geq \#B$ et $f$ est injective, alors $f$ est bijective ;
2. Si $\#A \leq \#B$ et $f$ est surjective, alors $f$ est bijective ;

# Cardinalité des ensembles infinis

# Rappels

Le cardinal d'un ensemble fini $A$ est

$$\#A = n \in \mathbb{N}, \quad \text{si } A \text{ est en bijection avec } \{0, 1, \ldots, n-1\}.$$

## Proposition

Soient $A$ et $B$ deux ensembles finis.

1. $\#A = \#B$ si et seulement s'il existe une bijection $f : A \to B$
2. $\#A \leq \#B$ si et seulement s'il existe une injection $f : A \to B$
3. $\#A \geq \#B$ si et seulement s'il existe une surjection $f : A \to B$

## Proposition

Soient $A$ et $B$ deux ensembles finis de même cardinalité.

Toute $\left\{ \begin{array}{l} \text{injection} \\ \text{surjection} \end{array} \right\}$ de $A$ dans $B$ est une bijection.

# Et pour les ensembles infinis alors ?

On étend $\#A = \#B$, mais sans définir $\#A$ (on le fera en master).

**Definition**

Deux ensembles (finis ou infinis) sont équipotents s'il existe une bijection $f : A \to B$.

**Exemple :** $\mathbb{N}$ et $-\mathbb{N} = \{-n \mid n \in \mathbb{N}\}$ sont équipotents.

## Définition 4.1.3 (Ensembles dénombrables)

Un ensemble $A$ est infini dénombrable s'il est équipotent à $\mathbb{N}$.
Par extension, un ensemble $A$ est dénombrable s'il est fini ou infini dénombrable.
Sinon, il est indénombrable.

Intuitivement, les ensembles infinis dénombrables sont les ensembles infinis "les plus petits possible".

## Proposition

Les ensembles

$$2\mathbb{N} = \{2n \mid n \in \mathbb{N}\}, \quad 2\mathbb{N}+1 = \{2n+1 \mid n \in \mathbb{N}\}, \quad \mathbb{Z}, \quad \mathbb{N} \times \mathbb{N}$$

sont infinis dénombrables.

# Simplifions-nous la vie !

Il est parfois plus facile de montrer qu'un ensemble infini est en bijection avec une partie de $\mathbb{N}$ qu'avec $\mathbb{N}$.

## Définition

Une relation d'ordre $\mathcal{R}$ sur $A$ est un bon ordre si toute partie non-vide $B \subset A$ possède un minimum $b$, i.e.

$$b \in B \wedge \forall c \in B, b\mathcal{R}c.$$

## Lemme

$\leq$ est un bon ordre sur $\mathbb{N}$.

**Mais :** $\leq$ n'est pas un bon ordre sur $\mathbb{Z}$, ni sur $\mathbb{R}$.

## Corollaire

Toute partie de $\mathbb{N}$ est dénombrable.

# Caractérisation de la dénombrabilité

## Théorème

Soit $A$ un ensemble. Les conditions suivantes sont équivalentes.

1. $A$ est dénombrable ;
2. il existe une injection $f : A \to \mathbb{N}$ ;
3. il existe une surjection $g : \mathbb{N} \to B$.

## Corollaire

Soient $A$ et $B$ deux ensembles et $f : A \to B$ une application.

1. Si $f$ est injective et $B$ dénombrable, alors $A$ est dénombrable ;
2. Si $f$ est surjective et $A$ dénombrable, alors $B$ est dénombrable ;

# Dénombrabilité et opérations

## Proposition 4.1.3

Si $A$ et $B$ sont dénombrables, alors $A \cup B$ et $A \cap B$ sont dénombrables.

## Definition

Une union $\bigcup_{i \in I} A_I = \{x \mid \exists i \in I : x \in A_i\}$ est une union dénombrable si $I$ est dénombrable.

## Proposition

Toute union dénombrable d'ensembles dénombrables est dénombrable.

## Proposition

Tout produit fini d'ensembles dénombrables est dénombrable.

# Tout n'est pas dénombrable

**Definition**

Une suite à termes dans un ensemble $A$ est une application de $\mathbb{N}$ dans $A$.

**Théorème 4.1.1 (Cantor)**

L'ensemble $E$ des suites à termes dans $\{0,1\}$ est indénombrable.

**Corollaire**

$\mathcal{P}(\mathbb{N})$ est indénombrable.

**Ce résultat se généralise :** $A$ et $\mathcal{P}(A)$ ne sont jamais équipotents.

**proposition**

$[0,1[$ est indénombrable.

**Corollaire**

$\mathbb{R}$ et $\mathbb{C}$ sont indénombrables.

# Indénombrabilité et opérations

## Proposition

Soient $A$ un ensemble dénombrable et $B$ un ensemble indénombrable.
Les ensembles $A \cup B$ et $B \setminus A$ sont indénombrables.

## Corollaire

$[0,1] \setminus \mathbb{Q}$ est indénombrable.

**Remarque :** l'intersection d'ensembles indénombrables n'est pas forcément indénombrable (ça peut par exemple être vide !)

# Relations d'équivalence

# Retour sur les partitions

## Définition 4.2.3

Soit $A$ un ensemble. Une partition de $A$ est une famille de sous-ensembles de $A$ deux à deux disjoints et dont l'union est égale à $A$.

## Proposition

Si $\{A_1, \ldots, A_m\}$ est une partition d'un ensemble fini $A$, alors $|A| = \sum_{i=1}^{m} |A_i|$.

Un manière de partitionner un ensemble est de sélectionner les éléments selon un critère.

**Exemples :**

- $\mathbb{N} = 2\mathbb{N} \cup (2\mathbb{N} + 1)$ ;
- $\mathbb{R} \times \mathbb{R} = \bigcup_{x \in \mathbb{R}} \{(x, y) \mid y \in \mathbb{R}\}$ ;

# Qu'est-ce que ce "critère" ?

On a en fait défini des relations :

- $\mathbb{N} = 2\mathbb{N} \cup (2\mathbb{N}+1)$ : avoir la même "parité"
- $\mathbb{R} \times \mathbb{R} = \bigcup_{x \in \mathbb{R}} \{(x, y) \mid y \in \mathbb{R}\}$ : avoir la même "abscisse"

1. Ces relations sont appelées relations d'équivalence : les points sont équivalents pour ce critère.
2. Ces relations permettent de partitionner/diviser l'ensemble.
   $\rightarrow$ Quel est le quotient, puisqu'on divise ?
3. C'est ce qui reste quand on identifie les points équivalents pour le critère ; il reste les sous ensembles de la partition.

A-t-on vraiment le droit d'identifier des éléments différents ?
C'est ce qu'on fait quand on dit que $\frac{1}{2} = \frac{2}{4}$.

Attention, on ne peut pas le faire pour toutes les relations. Les points en relation seront considéré comme égaux. Il faut donc que la relation se « comporte » comme l'égalité.

# La définition I

## Définition 4.2.1

Soit $A$ un ensemble. Une relation $\mathcal{R} : A \to A$ est une relation d'équivalence si les trois conditions suivantes sont satisfaites :

1. Elle est réflexive : on a $a\mathcal{R}a$ pour tout $a \in A$ ;
2. Elle est symétrique : pour tous $a, b \in A$, si $a\mathcal{R}b$, alors $b\mathcal{R}a$ ;
3. Elle est transitive : pour tous $a, b, c \in A$, si $a\mathcal{R}b$ et $b\mathcal{R}c$, alors $a\mathcal{R}c$.

**Exemples :**

1. Si $A$ est un ensemble, l'égalité est une relation d'équivalence.
2. Sur $\mathbb{R}$, la relation définie par $x\mathcal{R}y \Leftrightarrow \exists k \in \mathbb{Z} : y - x = 2k\pi$ est une relation d'équivalence ;
3. La relation « avoir la même parité » dans $\mathbb{Z}$ est une relation d'équivalence ;

# La définition II

## Définition 4.2.2

Soit $\mathcal{R}$ une relation d'équivalence sur un ensemble $A$.

- Pour tout $a \in A$, la classe d'équivalence de $a$, notée $[a]_{\mathcal{R}}$ ou $[a]$ est l'ensemble des éléments équivalents à $a$ :

$$[a]_{\mathcal{R}} = \{b \in A : b\mathcal{R}a\}$$

- Le quotient de $A$ par $\mathcal{R}$, noté $A/\mathcal{R}$ est l'ensemble formé par les classes d'équivalence :

$$A/\mathcal{R} = \{[a] : a \in A\}.$$

  Ici, $[a]$ est un point du quotient $A/\mathcal{R}$.
- L'élément $a \in A$ est appelé un représentant de $[a]$.
- L'application $\pi_{\mathcal{R}} : A \to A/\mathcal{R} : a \mapsto [a]$ est appelée projection canonique.

# Correspondance « partition $\leftrightarrow$ relation d'équivalence »

## Proposition 4.2.2

Soit $A$ un ensemble et $\{A_i : i \in I\}$ une partition ($I$ fini ou infini) de $A$ par des sous-ensembles non vides. Il existe une unique relation d'équivalence $\mathcal{R}$ dont les classes sont les sous-ensembles $A_i$.

## Lemme 4.2.1

Soit $A$ un ensemble et $\mathcal{R}$ une relation d'équivalence sur $A$. Alors pour tous $a, a' \in A$, on a $[a] = [a']$ si, et seulement si $a\mathcal{R}a'$.

## Proposition 4.2.1

Soit $A$ un ensemble et $\mathcal{R}$ une relation d'équivalence sur $A$. Les classes d'équivalence de $\mathcal{R}$ forment une partition de $A$ (par des sous-ensembles non vides).

# Retour à un problème connu

**Problème :** Comment rendre l'application $f : \mathbb{R} \to \mathbb{R} : x \to x^2$ bijective ?

- on restreint l'ensemble d'arrivée à $[0; +\infty[$
- on restreint l'ensemble de départ à $[0; +\infty[$

L'ensemble d'arrivée est naturel : c'est $f(\mathbb{R})$.
Mais comment choisir « naturellement » l'ensemble de départ ?

$$[0, +\infty[, ]-\infty, 0], (\mathbb{Q} \cap [0, +\infty[) \cup ((\mathbb{R} \setminus \mathbb{Q}) \cap ]-\infty, 0[), \ldots ?$$

Tout ensemble $A \subset \mathbb{R}$ tel que $\forall x \in \mathbb{R}$, $\#(A \cap \{-x, x\}) = 1$ convient.

**Idée :**

- Identifier $x$ et $-x$ dans un nouvel ensemble quotient $\mathbb{R}/\mathcal{R}$ ; on notera $[x]$ le point unique correspondant.
- Définir une nouvelle application $\widetilde{f} : \mathbb{R}/\mathcal{R} \to \mathbb{R} : [x] \mapsto x^2$.

**Intuitivement,** on colle plutôt que de couper.

# Rendons bijective l'application $f : \mathbb{R} \to \mathbb{R} : x \to x^2$

1. On prend $f(\mathbb{R}) = [0, +\infty[$ comme ensemble d'arrivée ; elle devient surjective.

2. On définit la relation $\mathcal{R} : \mathbb{R} \to \mathbb{R}$ par

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

   C'est une relation d'équivalence.
   La classe de $x$ est $[x] = \{x, -x\}$.

3. On passe au quotient $\mathbb{R}/\mathcal{R}$, et on définit une application sur le quotient

$$\widetilde{f} : \mathbb{R}/\mathcal{R} \to \mathbb{R} : [x] \mapsto x^2.$$

**Remarque :** Toutes les solutions proposées « en coupant » sont en bijection avec le quotient $\mathbb{R}/\mathcal{R}$.

# On ne peut pas faire n'importe quoi

$$\widetilde{f} : \mathbb{R}/\mathcal{R} \to \mathbb{R} : [x] \mapsto x^2.$$

est bien définie car si $x, x' \in \mathbb{R}$ sont tels que $[x] = [x']$, alors

$$\widetilde{f}([x]) = \widetilde{f}([x']).$$

On dit que $\widetilde{f}([x])$ est indépendant du représentant.

Mais avec

$$g : \mathbb{R} \to \mathbb{R} : x \mapsto x^3$$
$$\widetilde{g} : \mathbb{R}/\mathcal{R} \to \mathbb{R} : [x] \mapsto x^3$$

l'application $\widetilde{g}$ n'est pas bien définie :

$$[x] = [-x], \quad \text{mais} \quad \widetilde{g}([x]) \neq \widetilde{g}([-x]).$$

# Toute application définie sur un quotient est une « $\widetilde{f}$ »

1. Soit $g : A/\mathcal{R} \to B$ est une application.
2. Alors $f : A \to B : a \mapsto g \circ \pi_{\mathcal{R}}(a)$ est une application.
3. On a $g([x]) = f(x)$. Donc "$g = \widetilde{f}$".
4. L'application $f$ est constante sur les classes (d'équivalence).

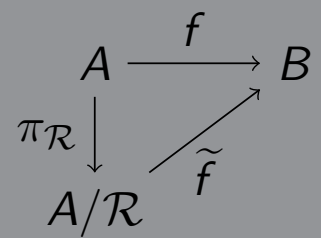
**Conclusion :** Toute application $g$ définie sur le quotient $A/\mathcal{R}$ est définie à partir d'une application $f$ définie sur $A$. Cette application $f$ doit être constante sur les classes.

# Caractérisations des $f$ pour lesquelles $\widetilde{f}$ est définie

## Définition 4.2.4

Soient $A, B$ deux ensembles, $\mathcal{R}$ une relation d'équivalence sur $A$ et $f : A \to B$ une application. On dit que :

1. $f$ passe au quotient $A/\mathcal{R}$ s'il existe une application (alors unique) $\widetilde{f} : A/\mathcal{R} \to B$ telle que pour tout $a \in A$, $\widetilde{f}([a]) = f(a)$.




2. $f$ est constante sur les classes de $\mathcal{R}$ si pour tous $a, a' \in A$,

$$a\mathcal{R}a' \Rightarrow f(a) = f(a').$$

## Proposition 4.2.3

Avec les mêmes notations, $f$ passe au quotient $A/\mathcal{R}$ si et seulement si elle est constante sur les classes de $\mathcal{R}$.

# À tout $f$, on peut associer une bijection $\widetilde{f}$

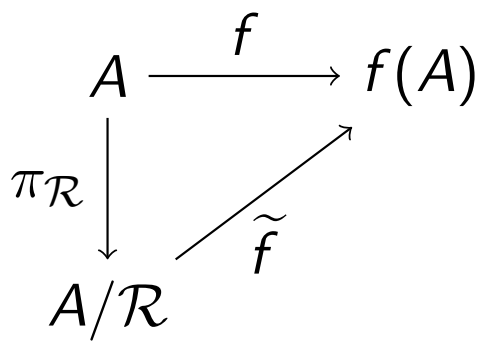
## Théorème 4.2.1

Soient $A$ et $B$ deux ensembles et $f : A \to B$ une application. On définit la relation $\mathcal{R}$ sur $A$ par

$$a\mathcal{R}a' \Leftrightarrow f(a) = f(a').$$

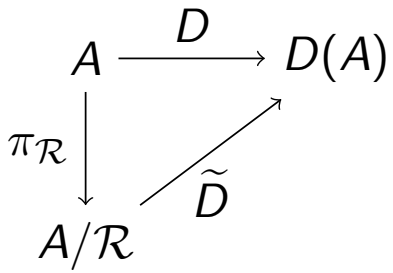
Alors $f$ passe au quotient en une application bijective

$$\widetilde{f} : A/\mathcal{R} \to f(A) : [a] \mapsto f(a).$$



# Application : l'opérateur de dérivation

Soient $\Omega$ un intervalle ouvert de $\mathbb{R}$
$A$ l'ensemble des applications $f : \Omega \to \mathbb{R}$ dérivables
$D : A \to D(A)$ l'opérateur de dérivation
$f \mathcal{R} g \Leftrightarrow Df = Dg$




$\widetilde{D}$ est une bijection et son application réciproque est la primitivation.

**Théorème d'analyse (TOC)**

Pour $f, g \in A$, $Df = Dg \Leftrightarrow \exists c \in \mathbb{R} : f = g + c$.

Autrement dit, $\mathcal{R}$ est défini par

$$f \mathcal{R} g \Leftrightarrow \exists c \in \mathbb{R} : f = g + c$$

# Nombres et structures algébriques

# But du jeu

On sait que $\mathbb{R}$ et $\mathbb{C}$ sont des champs. Qu'en est-il des autres ensembles de nombres classiques comme $\mathbb{N}$, $\mathbb{Z}$ ou $\mathbb{Q}$ ?

1. Définir l'ensemble $\mathbb{Z}$ : c'est un quotient de $\mathbb{N} \times \mathbb{N}$ ;
2. Définir l'addition dans $\mathbb{Z}$ : $(\mathbb{Z}, +, 0)$ est un groupe commutatif ;
3. Définir le produit : il n'y a qu'une bonne façon de faire ;
4. En déduire le classique « moins par moins donne plus » ;
5. Montrer que $(\mathbb{Z}, +, 0, \cdot, 1)$ est un anneau commutatif ;
6. Faire la même chose pour $\mathbb{Q}$, et montrer que c'est un champ.

# On suppose connaître $\mathbb{N}$ (on pourrait tout démontrer)

1. $(\mathbb{N}, +, 0, \cdot, 1)$ est un semi-anneau commutatif :
   i. $(\mathbb{N}, +, 0)$ est un monoïde commutatif, i.e. l'opération

   $$+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$$

   satisfait les propriétés suivantes :
   - $+$ est associatif : $\forall a, b, c \in \mathbb{N},\ a + (b + c) = (a + b) + c$ ;
   - 0 est le neutre (il est unique) : $\forall a \in \mathbb{N},\ a + 0 = a = 0 + a$ ;
   - $+$ est commutatif : $\forall a, b \in \mathbb{N},\ a + b = b + a$.

   ii. $(\mathbb{N}, \cdot, 1)$ est un monoïde commutatif ;

   iii. $\cdot$ distribue $+$ : $\forall a, b, c \in \mathbb{N},\quad a \cdot (b + c) = a \cdot b + a \cdot c$
   $(b + c) \cdot a = b \cdot a + c \cdot a$
2. 0 n'a pas de diviseur : $a \cdot b = 0 \Rightarrow a = 0 \vee b = 0$.
3. $\forall a, b, c \in \mathbb{N},\ a + b = a + c \Rightarrow b = c$.
4. $\mathbb{N}$ est bien ordonné par $a \leq b \equiv \exists c \in \mathbb{N} : b = a + c$

# Sans "$-$", comment définir $\mathbb{Z}$ ?

On fait comme les comptables : une colonne pour les recettes, une pour les dépenses, puis on compare.

## Définition 5.1.1

On définit la relation $\mathcal{R}$ sur $\mathbb{N} \times \mathbb{N}$ par

$$(a, b)\mathcal{R}(a', b') \Leftrightarrow a + b' = a' + b.$$

L'idée est que $(a, b)$ va correspondre à $a - b$, et donc que $a - b = a' - b'$, mais on ne veut/peut pas l'écrire comme cela.

## Proposition 5.1.1

La relation $\mathcal{R}$ est une relation d'équivalence. De plus, on a

$$(a, b)\mathcal{R}(a', b') \Leftrightarrow \exists k \in \mathbb{N} : \begin{cases} a' = a + k \\ b' = b + k \end{cases} \quad \text{ou} \quad \begin{cases} a = a' + k \\ b = b' + k \end{cases}$$

# $\mathbb{Z}$ et l'addition

## Définition 5.1.2

L'ensemble $\mathbb{Z}$ est le quotient $(\mathbb{N} \times \mathbb{N})/\mathcal{R}$.
L'addition sur $\mathbb{Z}$ est l'application

$$+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} : ([(a, b)], [(c, d)]) \mapsto [(a + c, b + d)].$$

L'addition est indépendante des représentants :

## Proposition 5.1.2

Pour tout $a, a', b, b', c, c', d, d' \in \mathbb{N}$,

$$\text{si } \begin{cases} (a, b)\mathcal{R}(a', b') \\ (c, d)\mathcal{R}(c', d') \end{cases} \text{, alors } (a + c, b + d)\mathcal{R}(a' + c', b' + d').$$

# $+$ dans $\mathbb{Z}$ hérite des propriétés de $+$ dans $\mathbb{N}$

**Corollaire**

$(\mathbb{Z}, +, 0)$, où $0 = [(0,0)]$, est un monoïde commutatif.

**Mais on a mieux :**

**Définition 5.1.3**

Un groupe est un monoïde $(G, \circ, e)$ dans lequel tout élément admet un inverse, i.e.,

$$\forall g \in G,\ \exists g' \in G : \quad g \circ g' = e = g' \circ g.$$

Un groupe est commutatif si $g \circ g' = g' \circ g$ pour tous $g, g' \in G$.

**Remarque :** lorsque l'opération du groupe est $+$, on parle plutôt d'opposé à la place d'inverse.

**Proposition 5.1.5**

$(\mathbb{Z}, +, 0)$, où $0 = [(0,0)]$, est un groupe commutatif.

# $\mathbb{N} \subset \mathbb{Z}$

Les éléments de $\mathbb{Z}$ sont des parties de $\mathbb{N} \times \mathbb{N}$
Donc on n'a pas $\mathbb{N} \subset \mathbb{Z}$.

## Proposition 5.1.6

L'application

$$\varphi : \mathbb{N} \to \mathbb{Z} : n \mapsto [(n, 0)]$$

est injective. De plus elle satisfait

$$\begin{cases} \varphi(0) = 0 \\ \varphi(n + n') = \varphi(n) + \varphi(n'), \quad \forall n, n' \in \mathbb{N} \end{cases}.$$

On identifie $\mathbb{N}$ à $\varphi(\mathbb{N})$, et on écrit $\mathbb{N} \subset \mathbb{Z}$.

# Nombres négatifs

- Via le plongement $\varphi$, on note $n$ le nombre $[(n, 0)]$.
- Son opposé dans $\mathbb{Z}$ est $[(0, n)]$ ; on le note $-n$.
- On note alors $-\mathbb{N}$ l'ensemble $\{-n : n \in \mathbb{N}\}$.

**Proposition 5.1.7**

On a $\mathbb{Z} = \mathbb{N} \cup -\mathbb{N}$ et $\mathbb{N} \cap -\mathbb{N} = \{0\}$.

# Soustraction

## Proposition 5.1.8

Pour tous $x, y \in \mathbb{Z}$, $y + (-x)$ est l'unique $z \in \mathbb{Z}$ tel que $x + z = y$.
On le note $y - x$.

**Remarque :** pour tout $[(a, b)] \in \mathbb{Z}$, on a

$$[(b, 0)] + [(a, b)] = [(a + b, b)] = [(a, 0)]$$

donc $[(a, b)] = a - b$.

## Proposition 5.1.9

Pour tous $x, y \in \mathbb{Z}$, on a $-(x + y) = (-x) + (-y) = -x - y$.
En particulier, $-(y - x) = x - y$.

# Multiplication

Comment multiplier $[(a, b)]$ et $[(c, d)]$ ?

- On se souvient que $[(a, b)] = a - b$ et $[(c, d)] = c - d$.
- On veut que $\cdot$ ait des propriétés "raisonnables" (associativité, distributivité,...), donc

$$\begin{aligned}[(a, b)] \cdot [(c, d)] &= (a - b) \cdot (c - d) \\ &= a \cdot c - b \cdot c - a \cdot d + b \cdot d \\ &= [(ac + bd, ad + bc)]\end{aligned}$$

- On retrouve le "moins par moins donne plus" :

$$[(0, b)] \cdot [(0, d)] = [(bd, 0)].$$

# La multiplication est bien définie

**Définition 5.2.1**

La multiplication des nombres entiers est l'application

$$\cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} : ([(a, b)], [(c, d)]) \mapsto [(ac + bd, ad + bc)].$$

La multiplication est indépendante des représentants :

**Proposition 5.2.5**

Pour tout $a, a', b, b', c, c', d, d' \in \mathbb{N}$,

si $\begin{cases} (a, b)\mathcal{R}(a', b') \\ (c, d)\mathcal{R}(c', d') \end{cases}$, alors

$(ac + bd, ad + bc)\mathcal{R}(a'c' + b'd', a'd' + b'c')$.

# L'anneau $(\mathbb{Z}, +, 0, \cdot, 1)$

$$\cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} : ([(a, b)], [(c, d)]) \mapsto [(ac + bd, ad + bc)].$$

## Définition 5.2.2

Un anneau est un quintuplet $(A, +, 0, \cdot, 1)$, où $A$ est un ensemble, $0, 1 \in A$ et qui satisfait les propriétés suivantes

- $(A, +, 0)$ est un groupe commutatif ;
- $(A, \cdot, 1)$ est un monoïde ;
- La multiplication distribue l'addition : pour tous $a, b, c \in A$,

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{et} \quad (b + c) \cdot a = b \cdot a + c \cdot a$$

Un anneaux est commutatif si $a \cdot b = b \cdot a$ pour tous $a, b \in A$.

## Proposition 5.2.6

$(\mathbb{Z}, +, 0, \cdot, 1)$ est un anneau commutatif.

# On fait pareil pour construire $\mathbb{Q}$

- On considère $(a, b) \in \mathbb{Z} \times \mathbb{Z}_0$ (ou $\mathbb{Z} \times \mathbb{N}_0$), et on écrit

$$(a, b)\mathcal{E}(c, d) \Leftrightarrow ad = bc.$$

- C'est une relation d'équivalence.
- $\mathbb{Q}$ est le quotient $(\mathbb{Z} \times \mathbb{Z}_0)/\mathcal{E}$.
- On définit les opérations pour que cela fasse ce qu'on veut :

$$+ : \mathbb{Q} \times \mathbb{Q} : ([(a, b)], [(c, d)]) \mapsto [(a, b)] + [(c, d)] = [(ad + bc, bd)].$$
$$\cdot : \mathbb{Q} \times \mathbb{Q} : ([(a, b)], [(c, d)]) \mapsto [(a, b)] \cdot [(c, d)] = [(ac, bd)].$$

- On montre que $+$ et $\cdot$ sont bien définis et font de $\mathbb{Q}$ un champ.

# Arithmétique

# Divisibilité

## Définition 5.2.6

Soient $a \in \mathbb{Z}$ et $d \in \mathbb{Z}_0$. On dit que $d$ divise $a$ (ou que $d$ est un diviseur de $a$) si il existe $c \in \mathbb{Z}$ tel que $a = d \cdot c$. On écrit alors $d|a$ et $c = \frac{a}{d}$.

## Proposition 5.2.9

Soient $a \in \mathbb{Z}$, $d \in \mathbb{Z}_0$, tels que $d|a$. Alors $-d|a$, $d|-a$ et $-d|-a$. On a de plus $\frac{a}{-d} = \frac{-a}{d} = -\frac{a}{d}$ et $\frac{-a}{-d} = \frac{a}{d}$.

# Et quand $d \nmid a$ ?

## Proposition 6.1.2 (Division Euclidienne)

Soient $a \in \mathbb{Z}$ et $d \in \mathbb{Z}_0$. Il existe un unique couple d'entiers $(q, r)$ tels que

$$a = qd + r, \qquad 0 \leq r < |d|.$$

$d$ est le diviseur, $q$ le quotient et $r$ le reste de la division.

## Définition

Soit $(G, \circ, e)$ un groupe et soit $H \subset G$. On dit que $H$ est un sous-groupe de $G$ si $(H, \circ_{|H \times H}, e)$ est un groupe.

## Corollaire

Tout sous-groupe de $(\mathbb{Z}, +, 0)$ est de la forme $(n\mathbb{Z}, +, 0)$ pour un $n \in \mathbb{N}$.

# pgcd

## Définition

Soient $a, b \in \mathbb{Z}_0$. Le plus grand commun diviseur (pgcd) de $a$ et de $b$ est l'unique entier $d$, noté $\mathrm{pgcd}(a, b)$ qui satisfait

- $d \mid a$ et $d \mid b$ ;
- pour tout $c$, si $c \mid a$ et $c \mid b$, alors $c \leq d$.

## Proposition 6.2.7

Pour tous $a, b \in \mathbb{Z}_0$, on a

$$\mathrm{pgcd}(a, b) = \mathrm{pgcd}(-a, b) = \mathrm{pgcd}(a, -b) = \mathrm{pgcd}(-a, -b).$$

## Proposition 6.2.8

Pour tous $a, b \in \mathbb{Z}_0$ tout $m \in \mathbb{Z}$, on a

$$\mathrm{pgcd}(a, b) = \mathrm{pgcd}(a, b + ma).$$

# Algorithme d'Euclide

## Proposition 6.2.9 (Algorithme d'Euclide)

Soient $a, b \in \mathbb{Z}_0$ avec $|b| \geq |a|$,. On pose $r_0 = |a|$ et on effectue les divisions euclidiennes suivantes :

$$\begin{aligned}
a &= bq_1 + r_1, \quad 0 < r_1 < |b|; \\
b &= r_1 q_2 + r_2, \quad 0 < r_2 < r_1; \\
r_1 &= r_2 q_3 + r_3, \quad 0 < r_3 < r_2; \\
&\vdots \\
r_{n-2} &= r_{n-1} q_n + r_n, \quad 0 < r_n < r_{n-1}; \\
r_{n-1} &= r_n q_{n+1}.
\end{aligned}$$

Alors $\mathrm{pgcd}(a, b)$ est le dernier reste non nul $r_n$.

# Théorème de Bezout

## Théorème 6.2.1 (Théorème de Bezout)

Soient $a, b \in \mathbb{Z}_0$. Il existe $x, y \in \mathbb{Z}$ tels que

$$ax + by = \mathrm{pgcd}(a, b).$$

# Nombres premiers entre eux

## Définition 6.2.4

Deux entiers $a, b \in \mathbb{Z}_0$ sont premiers entre eux si $\mathrm{pgcd}(a, b) = 1$.

## Proposition 6.2.10

Deux entiers $a, b \in \mathbb{Z}_0$ sont premiers entre eux si et seulement s'il existe $x, y \in \mathbb{Z}$ tels que

$$ax + by = 1.$$

## Corollaire (Lemme de Gauss)

Soient $a, b, c \in \mathbb{Z}_0$. Si $a \mid bc$ et $\mathrm{pgcd}(a, b) = 1$, alors $a \mid c$.

# Equations diophantiennes linéaires

## Proposition

On considère l'équation

$$ax + by = c, \quad a, b \in \mathbb{Z}_0, c \in \mathbb{Z}.$$

1. Celle-ci admet des solutions $(x, y) \in \mathbb{Z}^2$ si et seulement si $\mathrm{pgcd}(a, b) \mid c$ ;
2. Si $(x_0, y_0) \in \mathbb{Z}^2$ est une solution, alors il en existe une infinité qui sont exactement les

$$(x, y) \in \left\{ \left( x_0 + k\frac{b}{\mathrm{pgcd}(a, b)}, y_0 - k\frac{a}{\mathrm{pgcd}(a, b)} \right) \mid k \in \mathbb{Z} \right\}.$$

# Théorème fondamental de l'arithmétique

## Lemme 3.4.1 (Lemme d'Euclide)

Soit $p$ un nombre premier et soient $a, b \in \mathbb{N}$. Si $p \mid ab$, alors $p \mid a$ ou $p \mid b$.

## Théorème 3.4.1 (Théorème fondamental de l'arithmétique)

Tout nombre naturel $n \geq 2$ se décompose en un produit de nombre premiers. La décomposition est unique, à l'ordre des facteurs près.

## Proposition 3.4.5

L'ensemble des nombres premiers est infini.

# Arithmétique modulaire

# Encore une relation d'équivalence

Les horloges n'ont que douze heures. Alors, si à 10h, on ajoute 4 heures, on se retouve à 2h : les horloges comptent **modulo** 12h.

## Définition 6.1.1

Soit un entier $m \geq 2$. On définit la relation d'égalité modulo $m$ sur $\mathbb{Z}$ par

$$x \equiv_m y \Leftrightarrow \exists k \in \mathbb{Z} : y = x + km.$$

On dit alors que $y$ est égal (ou congru) à $x$ modulo $m$. On note aussi

$$x = y \bmod m.$$

## Proposition 6.1.1

Pour tout entier $m \geq 2$, $\equiv_m$ est une relation d'équivalence.

# Et le quotient qui va avec

## Définition 6.1.2

On appelle $\mathbb{Z}_m$ le quotient $\mathbb{Z}/\equiv_m$.
Pour $x \in \mathbb{Z}$, note $[x]$ la classe d'équivalence de $x$ pour $\equiv_m$.

Pour $x \in \mathbb{Z}$, notons $r_m(x)$ le reste de la division euclidienne de $x$ par $m$.

## Proposition 6.1.3

Pour tout entier $m \geqslant 2$, l'application

$$f : \mathbb{Z}_m \to \{0, 1, \ldots, m-1\}, [x] \mapsto r_m(x)$$

est une bijection.
En particulier, le cardinal de $\mathbb{Z}_m$ est $m$.

$\mathbb{Z}$ est un anneau commutatif. Quelle structure algébrique a-t-on sur $\mathbb{Z}_m$ ?

# $(\mathbb{Z}_m, +, [0])$ est un groupe commutatif

**Définition 6.1.3**

L'addition de $\mathbb{Z}_m$ est l'application

$$+ : \mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{Z}_m : ([x], [y]) \mapsto [x] + [y] = [x + y].$$

**Proposition 6.1.4**

L'addition dans $\mathbb{Z}_m$ est bien définie. De plus, elle munit $\mathbb{Z}_m$ d'une structure de groupe commutatif.

# $(\mathbb{Z}_m, +, [0], \cdot, [1])$ est un anneau commutatif

**Définition 6.1.4**

La multiplication de $\mathbb{Z}_m$ est l'application

$$\cdot : \mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{Z}_m : ([x], [y]) \mapsto [x] \cdot [y] = [x \cdot y].$$

**Proposition 6.1.5**

La multiplication dans $\mathbb{Z}_m$ est bien définie. De plus, elle permet de munir $\mathbb{Z}_m$ d'une structure d'anneau commutatif.

# Peut-on faire mieux ?

**Définition 5.2.7**

Un anneau $(A, +, 0, \cdot, 1)$ est intègre si 0 n'a pas de diviseur, i.e., pour tous $x, y \in A$, si $x \cdot y = 0$ alors $x = 0$ ou $y = 0$.

**Proposition 5.2.8**

$(\mathbb{Z}, +, 0, \cdot, 1)$ est un anneau intègre

# Être intègre ne passe pas forcément au quotient

Pour savoir si $\mathbb{Z}_m$ est intègre, on peut faire sa table de multiplication :

$\mathbb{Z}_3$

| $\cdot$ | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 |
| 2 | 0 | 2 | 1 |

Intègre

$\mathbb{Z}_4$

| $\cdot$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 |
| 2 | 0 | 2 | 0 | 2 |
| 3 | 0 | 3 | 2 | 1 |

Pas intègre

# $\mathbb{Z}_m$ n'est pas toujours un corps

**Proposition 6.2.2**

Tout corps est intègre.

**Proposition 6.2.3**

Pour tout $m \geqslant 2$, si $m$ n'est pas premier, alors $\mathbb{Z}_m$ n'est pas un corps.

# Quels sont les éléments inversibles de $\mathbb{Z}_m$ ?

## Définition 5.2.7

Soit $(A, +, 0, \cdot, 1)$ un anneau commutatif. Un élément $x \in A$ est inversible s'il existe $y \in A$ tel que

$$x \cdot y = 1.$$

## Proposition 6.2.11

L'élément $[a] \in \mathbb{Z}_m \setminus \{0\}$ est inversible si, et seulement si, $a$ est premier avec $m$.

**Comment inverser** $[a]$ **?** On cherche $[b]$ tel que $ab + km = 1$.
**Exemple :** Calculer l'inverse de 11 dans $\mathbb{Z}_{26}$.

## Proposition 6.2.12

L'anneau $\mathbb{Z}_p$ est un champ si, et seulement si $p$ est premier.

# Une petite application : critères de divisibilité

## Divisibilité par 3

Un entier $n$ est divisible par 3 ssi la somme de ses chiffres est divisible par 3.

**Exemple :** $3 \mid 2148$ car $2+1+4+8 = 15$ et $3 \mid 15$.

**Justification à l'aide de $\mathbb{Z}_3$ :**

$$\begin{aligned}[2148] &= [2.10^3 + 1.10^2 + 4.10 + 8] \\ &= [2].[10]^3 + [1].[10]^2 + [4].[10] + [8] \\ &= [2] + [1] + [4] + [8] \\ &= [2+4+1+8].\end{aligned}$$

Le cas général se traite exactement de la même façon.