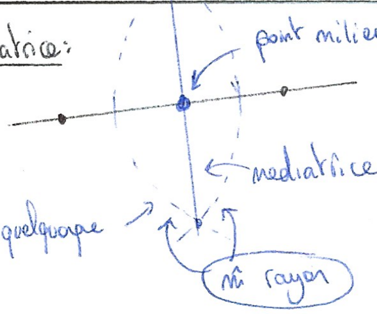
ENSEMBLE

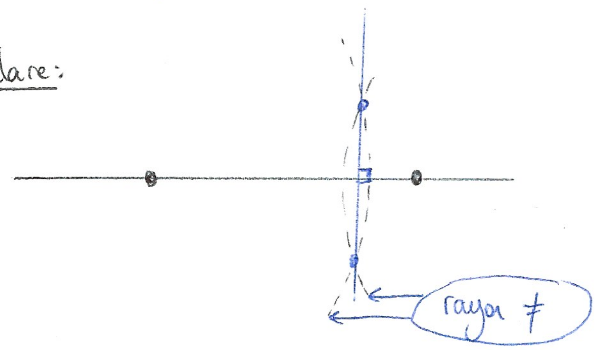
- **Histoire :**
  - Appliquer une formule ⟶ Demonstration via Euclide (−300 av JC)
  - Demonstration : Construbtibilité / Decoupage ⟶ Logique ensembliste (Cantor) (19e siècle) ⟶ ?
    - Paradoxe de Russel (exple : Fractale)
    - Incomplétude de Gödel

- **Constructibilité et decoupage** ⟶ Règles et compas (Alternative : Origami)

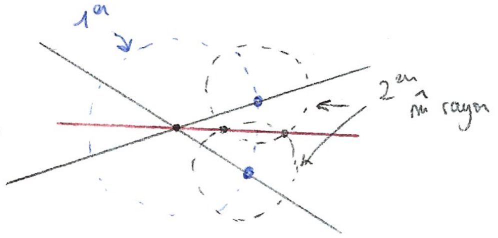
- médiatrice :



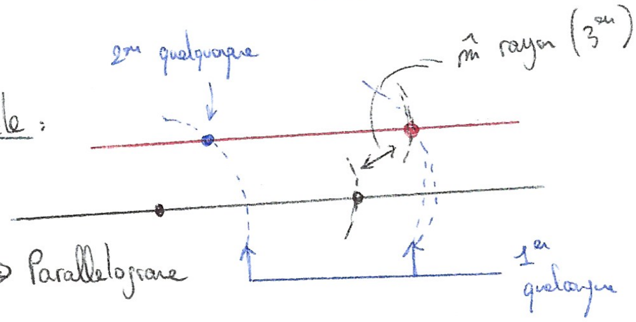
- Perpendiculaire :



- bissectrice :

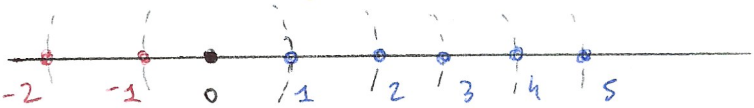


- Parallèle :



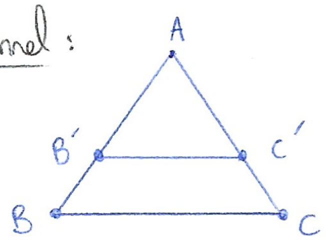
⟹ Parallelogramme

- **Construction des nombres entier :**



$\mathbb{N}$ (naturel)
$\mathbb{Z}$ (relatif)

- **Construction des nombres rationnel :**
  - ↳ Theoreme de Thales :



Si $(BC) \parallel (B'C')$

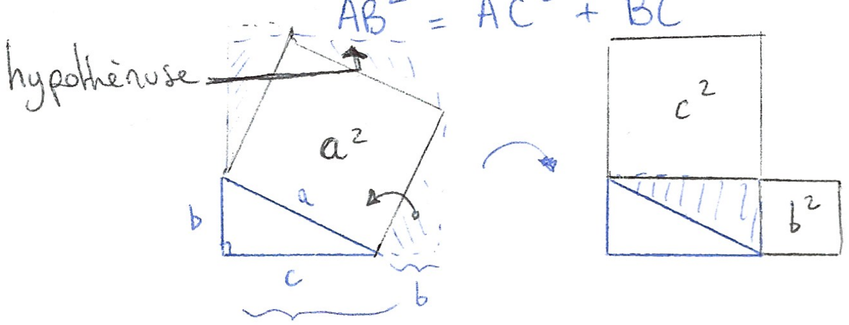
Alors : $\dfrac{AB}{AB'} = \dfrac{AC}{AC'} = \dfrac{BC}{B'C'}$ → + grand / → + petit

homothétie

⟹ $\mathbb{Q}$ (ou Quotient)

- **Decoupage triangle rectangle (et nombre réel) :**
  - ↳ Theorème de Pythagore : Si un triangle ABC est triangle en C, alors

$$AB^2 = AC^2 + BC^2$$



carré : $(c+b)^2$ = Aire totale

si $b = c = 1$
alors $a = \sqrt{2}$
→ nombre $\mathbb{R}$

ENSEMBLE

- Langage et Logique : (→ renommer langage et logique ensembliste)
  - proposition : Phrase soit "vrai", soit "fausse" } construit Theorème / Lemme
  - Axiomes : verité première (conventionnelle)

→ resultat déduit = corolaire ; → si on ne sait pas "vraiment" = conjecture

→ mettre ici base ensemble sans axiome $\subset$, $\cap$, $P(E)$, $\{\}$, $\in$, $\mathbb{N} \subset \mathbb{Z}$ ... diagrame d'Euler

- Quantificateur : $\exists$: "il existe au moins" ; $\forall$: "quelque soit" ou "pour tout"
- Prédicat : Proposition sous forme quantificateur + elements. ⚠ ordre important

Exemple : $(\forall a \in A, \exists \ell \in L, a = \ell) \neq (\exists \ell \in L, \forall a \in A, a = \ell)$

element → ; ensemble ; "appartient à"

- Loi de Morgan : non (A et B) = non (A) ou non (B)

  non (A ou B) = non (A) et non (B)

  (symbole : $\neg$ "non" ; $\wedge$ "et" ; $\vee$ "ou")

→ Les connecteurs logique "ou" et "et" permettent d'encadrer "élement"

- Enoncé d'un Theorème : "Si quelque chose Alors autre chose" | reciproque : $\Leftarrow$

  suffisante → hypothèse ; implication $\Rightarrow$; conclusion ← necessaire

- Equivalence : Si $A \Rightarrow B$ et $B \Rightarrow A$ alors $A \Leftrightarrow B$ (⚠ si A et B faux l'équivalence est vrai)

  ↳ signifie : (A et B) ou (non(A) et non(B))

- Theorème : Toute implication est equivalente à son implication contraposée } si implication direct non évidente

  raisonnement

- Arithmetique : → Nombre entier

élementaire {

- Identité de Bachet-Bezout : Deux nombres entier "a" et "b" sont premiers entre eux, si et seulement si, il existe deux entier "m" et "n", tel que :

$$a \times m + b \times n = 1$$

- Division euclidienne : Soit "a" et "b" deux nombre entiers tel que b soit non nul. il existe au moins un couple d'entier (q, r) tel que "a" soit égal à "$b \cdot q + r$" et tel que "r" soit en valeur absolu plus petit que "b".

}

$$a = b \cdot q + r$$

Dividende ; Diviseur ; Quotient

$$\begin{array}{l|l} a & b \\ \hline -q_0 & q \\ r_1 & \\ -\ \vdots & \\ r & \end{array}$$

→ PGCD :

Arithmétique (suite)

- **Petit théorème de Fermat :** Si "p" est un nombre premier et si "a" est un entier non divisible par p, alors "$a^{p-1} - 1$" est multiple de "p".

$$a^{p-1} \underset{\text{congru}}{\equiv} 1 \underset{\text{modulo}}{\operatorname{mod}}(p) = 1[p] \iff a^p \equiv a[p]$$

- **Théorème d'Euler :** $\forall n > 0$, $\forall a$ premier avec n (autrement dit : inversible mod n) → PGCD = 1

$$a^{\varphi(n)} \equiv 1 [n]$$

→ indicatrice d'Euler : $\varphi : \mathbb{N}^* \longrightarrow \mathbb{N}^*$ ← strictement positif

$$n \longmapsto \operatorname{card}\left(\{ m \in \mathbb{N}^* \mid m \leq n \text{ et } m \text{ premier avec } n\}\right)$$

- **Infinité de nombre premier avec l'Arithmétique de Peano :**

successeur ; ou

$$\forall n, \exists m, \forall c, \forall d, (c \times d = n + m) \Rightarrow (c = S0 \vee d = S0)$$

Application :

- **Définition :** Soit E, F deux ensembles, On appelle application (ou fonction) de E dans F, la donnée d'une partie G de $\underbrace{E \times F}_{\text{produit cartézien}}$, tq, "$\forall x \in E$, $\exists!$ $y \in F$, tel que (x, y) soit élément de G." (Existence + unicité) $\exists!$

couple

$$f : E \longrightarrow F$$
$$x \longmapsto f(x)$$

antécédant ; image "y"

→ graphe de la fonction : $G = \{(x,y) \in E \times F \mid y = f(x)\} = \{(x, f(x)) \mid x \in E\}$

relation binaire

- **Opération sur les applications :**
  - **Restriction :** A, sous ensemble de E. Restriction de f sur A :

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

  - **Prolongement :** Soit E, F, G, H des ensembles tel que $E \subset G$, $F \subset H$:

$$f : E \longrightarrow F \quad \rightarrow \text{restriction}$$
$$g : G \longrightarrow H$$

on pose une valeur

g est un prolongement de f si $\forall x \in E$, $f(x) = g(x)$

Application (suite)

Opérations (suite)

- **Composition** : Soit E, F, G 3 ensembles tel que : $f : E \longrightarrow F$
  $g : F \longrightarrow G$

$$g \circ f : E \longrightarrow G$$
$$x \longmapsto g(f(x))$$

$$\begin{tikzcd} & F \arrow[dr, "g"] & \\ E \arrow[ur, "f"] \arrow[rr, "g \circ f"'] & & G \end{tikzcd}$$

$x \quad f(x) \quad g(f(x))$

Codomaine : Ensemble d'arrivée. L'image de f est un sous-ensemble de F.

- **Injectivité** : Une application $f : X \to Y$ est injective si $\forall y \in Y$, il existe au plus un $x \in E$, tel que $f(x) = y$. écrit autrement :

$$\forall x \in X, \quad \forall x' \in X \quad (f(x) = f(x') \Rightarrow x = x')$$

contraposé

$$\forall x \in X, \quad \forall x' \in X \quad (x \neq x' \Rightarrow f(x) \neq f(x'))$$

- **Surjection** : Une application $f : X \to Y$, on a :

$$\forall y \in Y, \quad \exists x \in X, \ f(x) = y$$

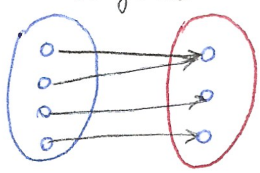
- **Bijection** : Un application $f : E \to F$, on a : (1 unique antécédant)

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

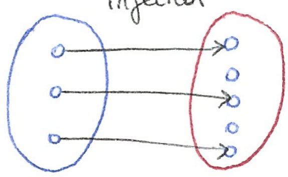
→ propriété : $g \circ f = id_E$ et $f \circ g = id_F$ → application identité

- **Représentation** :

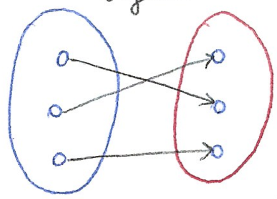
surjection



injection



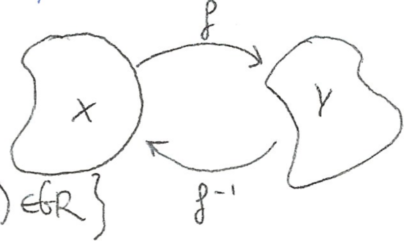
bijection



ex : • $f(x) = x^2 \in \mathbb{R}^+$ • $f(x) = \begin{cases} ax, & x < 5 \\ ax+b, & x \geq 5 \end{cases}$ • $f(x) = a \cdot x + b$

Application réciproque : Si $f : E \to F$ est bijective, alors il existe relation réciproque, tel que :

$$f(\underset{f^{-1}}{g}(y)) = y$$



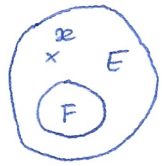
$$G_{R^{-1}} = \{(x, y) \in F \times E \mid (y, x) \in G_R\}$$

Primitive de l'Application :

(axiome ZFC) $\longrightarrow \forall x \forall y \forall y' \left([(x,y) \in G \text{ et } (x, y') \in G] \Rightarrow y^* = y' \right)$

Théorie des ensembles :

- **Inclusion et Appartenance :**
  - ▷ $x \in E$: "appartient à", x, un élément
  - ▷ $F \subset E$; "inclu dans", F, une partie de E



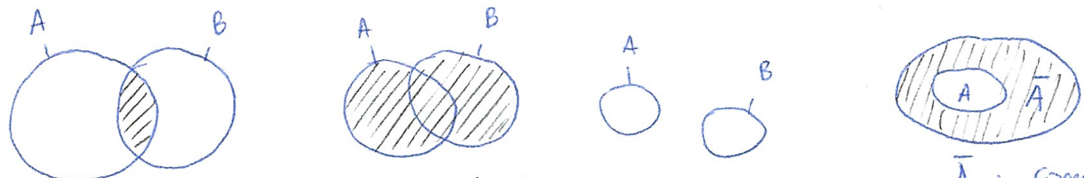
- **Ensemble :** regroupement d'objet : $\{a; b; a\} = \{a; b\}$ ou $\mathbb{N}$
  - ensemble vide : $\phi = \{\,\}$
- **n-uplet :** Collection ordonnée de n objet → $n = 2 \Rightarrow$ couple (a, b)
- **Cardinal :** E un ensemble fini (dénombrable), noté $\mathrm{Card}(E)$ désigne le nombre d'élément de E.

- **Ensemble des partie de E :** $\mathcal{P}(E) = \{\phi; \{1\}; \{2\}; \{3\}; \{1\ 2\}; \{1\ 3\}; \{2\ 3\}; E\}$

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

  $\mathrm{Card}(P(E)) = 2^{\mathrm{card}(E)}$

- **Relation :**



intersection $A \cap B$ — union $A \cup B$ — disjoint $A \cap B = \phi$ — $\bar{A}$: complementaire

- **Ensemble de Base :**

  $\mathbb{Q} = \left\{ \frac{a}{b},\ a \in \mathbb{Z} \text{ et } b \in \mathbb{N}^* \right\}$

  $\mathbb{R} = \left\{ n, a_1 a_2 \dots \mid n \in \mathbb{Z},\ \forall i, a_i \in \{0, \dots, 9\} \right\}$

  produit cartezien → $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ = ensemble des vecteurs du plan

- **Axiomes :**

  Z
  - **Extensionnalité :** $(A \subset B \text{ et } B \subset A) \Rightarrow A = B$
  - **Constructions :** Paire, Reunion, Partie, infini, comprehension, vide

  F
  - **Remplacement :**
  - **Fondation :** $\forall x\, [x \neq \phi \Rightarrow \exists y (y \in x \wedge y \cap x = \phi)]$ → element minimum

  C
  - **Choix :** $\forall X\, [\phi \notin X \Rightarrow \exists f : X \to \cup X,\ \forall A \in X, (f(A) \in A)]$

    fonction de choix

    ↳ pas necessaire si ensemble fini

ENSEMBLES

- <u>Structure Algébriques.</u> → fondée sur Théorie des ensemble : (Ensemble + loi de composition)

- <u>Loi de composition internes :</u> Sur un ensemble E, toute application $*$ du produit cartésien $E \times E$ dans E

$$* : E \times E \to E$$
$$\underbrace{(x,y)}_{\text{composition}} \mapsto x * y \quad \} \text{ relation = composition}$$

→ Un ensemble E muni d'une loi de composition interne $*$ est notée $(E, *)$

- <u>Groupe</u> : Ensemble muni d'une loi de composition interne $(G, *)$
  - <u>propriétés</u> :
    - l.c.i : $\forall a, b \in G, \quad a * b \in G$
    - Associativité : $(a * b) * c = a * (b * c)$ vrai
    - Element neutre : $\exists! e \in G, \quad e * a = a * e = a$
    - $(\exists b \in G) \to$ Symétrique : $\underbrace{a * b = b * a}_{\text{commutativité (abelien) n'est pas toujours vrai}} = e_G$
  - <u>element regulier</u> : $a \in E$ regulier si $\forall b, c \in E, \; a * b = a * c \Rightarrow b = c$
  - <u>sous groupe</u> : $H \leqslant G$ st un sous groupe, $H \subseteq G$ → conserve propriété groupe → $e_G \in H$
  - <u>groupe distingué</u> H un sous-groupe distingué $H \triangleleft G$ si $x H x^{-1} = H \quad (\forall x \in G)$
  - <u>groupe engendré</u> : Plus petit sous groupe contenant g : $\langle g \rangle = \{\dots, g^{-1}, 1, g, g^2, \dots\}$
  - <u>groupe cyclique</u> $\exists g \in G, \quad G = \langle g \rangle \to \langle g \rangle$ est un générateur de G
  - <u>Morphisme</u> $\varphi : (\mathbb{Z}^+) \to (\langle g \rangle, \times)$, $k \mapsto g^k$ } φ morphisme de groupe car : $\varphi(k+l) = g^{k+l} = \varphi(k) \times \varphi(l)$
    <u>Noyaux</u> $Ker(f) = \{x \in G \mid f(x) = e_H\} = n\mathbb{Z} \subset G$
  - <u>groupe symétrique</u> : permutation : $\sigma : \{1, \dots, n\} \to \{1, \dots, n\}$, $i \mapsto \sigma(i)$

Th de Lagrange $x^n = e$

+ bijection = isomorphisme (?)

- <u>Anneaux</u> : A est un ensemble, $(A, +, \cdot)$ est un anneaux
  - <u>Propriété</u> : m̂ prop groupe ~~et~~ distributivité à + ; $\forall x, y, z \in A, \; x(y+z) = xy + xz$
  - <u>element inversible</u> $a \in A$ inversible ssi $\exists b \in A \mid a \times b = b \times a = 1_A$ → element neutre
  - <u>Corps</u> $\mathbb{K}$ ssi $(\mathbb{K}, +, \times)$ un anneau tel que tout element non nuls soit inversible ; $\mathcal{U}(\mathbb{K}) = \mathbb{K}^*$
  - <u>Sous-Anneaux</u> $P \subset A$ sous anneaux si stable addition, inverse et multiplication ⊕ $1_A \in P$
  - <u>Morphisme</u> verifie pour + et × : $f(x * y) = f(x) * f(y)$ $\quad Ker(f) \not\subset A$
  - <u>Idéal</u> I ideal de A si : $(I, +) \leqslant (A, +)$ → Sous groupe

- <u>Loi de composition externes</u> : loi de composition où $F \neq E$
  ↳ voir espace vectoriel (Algebre)