Cours magistral du semestre d'automne 2023

Introduction à la logique et à la théorie des ensembles

Pr. Hugo Duminil-Copin
E-Mail : hugo.duminil@unige.ch

Octobre 2023

Sommaire

1 Introduction

1.1 Éléments de communication mathématique

Il existe 3 types d'objets mathématiques : les énoncés, les preuves et les commentaires.

1.1.1 Les énoncés

Un énoncé est une phrase "syntaxiquement correcte au sens mathématique" auquel on peut associer une valeur VRAIE ou FAUSSE.

Définition 1.1 (Axiome). *Un axiome est un énoncé mathématique supposé VRAI.*

Exemple : Les 5 postulats d'Euclide énoncés dans Les Éléments.
A noter que dans un système d'axiomes, on veut surtout éviter 2 choses :

— Que deux axiomes se contredisent.

— Que l'on puisse tout démontrer par la seule utilisation des axiomes.

Définition 1.2 (Définition). *Une définition est un énoncé qui est vrai ou faux selon l'objet auquel on l'applique.*

Exemple : p est un nombre premier si et seulement s'il est strictement supérieur à 1 et s'il uniquement divisible par 1 et lui-même.

Les théorèmes, propositions, lemmes et corollaires sont des énoncés mathématiques (VRAI et) démontrés comme étant VRAIS.

Définition 1.3 (Théorème). *Les théorèmes sont les résultats qui ont une grande importance.*

Exemples :

Théorème de Fermat-Wiles : Il n'existe pas de triplets d'entiers $(x, y, z) \in \mathbb{Z}^3$ non-nuls tel que $x^n + y^n = z^n, \forall n \geq 3$

Théorème des nombres premiers : Si $\pi(n)$ est le nombre de nombre premiers inférieur ou égal à n, alors $\frac{\pi(n)\log(n)}{n} \to 1$

Définition 1.4 (Lemme). *Les Lemmes sont des énoncés intermédiaires dans une preuve.*

Exemple : Le lemme fondamental du programme Langland.

Définition 1.5 (Corollaire). *Les corollaires sont les conséquences (relativement facile) d'un théorème.*

Définition 1.6 (Proposition). *Les propositions sont les résultats de moindre importance.*

Définition 1.7 (Conjecture). *Les conjectures sont des énoncés que l'on pense VRAI mais non démontrée.*

Exemples :

Conjecture de Riemann

Conjecture de Goldbach

Conjecture des nombres premiers jumeaux

...

Exercice : Quel type d'énoncé sont les assertions suivantes ? :

- Une dérivée nulle est une fonction constante
- $23 \neq 36$
- Il existe un ensemble

1.1.2 Les preuves

Une preuve mathématique, ou démonstration, est un enchaînement logique se basant sur des axiomes ou des énoncés vrais démontré qui permet de conclure qu'un énoncé est Vrai ou Faux.

Exemple : Il existe une infinité de nombres premiers.

Démonstration. Soit $\mathcal{P} = \{n \in \mathbb{N} : p|n \Rightarrow (p = 1 \text{ ou } = n)\}$ Montrons que $\mathcal{P}$ est infini.
$\forall n \in \mathbb{N} : (Card(\mathcal{P}) \geq n \Rightarrow \{p_1 \ ; \ p_2 \ ; \ ... \ ; \ p_n\} \subseteq \mathcal{P}) \Rightarrow (\exists p \in \mathcal{P} : p \mid p_1 p_{n+1})$
$\Rightarrow [(p \in \mathcal{P} \backslash \{p_1, p_n\}) \vee (p|p1p_{n+1} \ \wedge \ p|p_1 p_n)] \Rightarrow [(p \in \mathcal{P} \backslash \{p_1, p_n\}) \vee (p \in \mathcal{P} \vee p|1)]$
$\Rightarrow p \in \mathcal{P} \backslash \{p_1, p_n\} \Rightarrow Card(\mathcal{P}) \geq n + 1$ □

1.1.3 Les commentaires

C'est un accompagnement venant éclairer la preuve. Par exemple les schémas, dessins, illustrations, exemples,remarques, simulations sont des formes de commentaires.

1.2 Un exemple de communication mathématique

Lorsque l'on fait un raisonnement mathématique, il est important d'avoir en tête ces 4 commandements :

1. Définissez les termes.
2. Démontrer tous les énoncés.
3. Suivre les règles de la logique et de la syntaxe.
4. On écrit pour les autres.

1.2.1 Les solides de Platon

Définition 1.8 (Polyèdre, convexité, régularité)**.** *Un polyèdre est une forme géométrique tridimensionnelle ayant des faces planes polygonales se rencontrant selon des segments de droite appelés arrête.*
Un polyèdre est convexe si pour toute paire de point dans le segment reliant les deux points est inclut dans le polyèdre.
Le polyèdre est régulier si pour toute paire de sommets du polyèdre, il existe une isométrie préservant le polyèdre et envoyant le premier sommet sur le deuxième.

Théorème 1.1. *Il existe exactement 5 polyèdres convexes réguliers*

Démonstration. Montrons qu'il existe au moins 5 polyèdres convexes réguliers : *tétraèdre*, *cube*, *octaèdre*, *dodécaèdre*, *isocaèdre*.
Appelons p et q respectivement le nombre d'arête bordant chaque face et le nombre de face rejoignant un sommet. Soit S,A,F le nombre de Sommet, Arrête et Face du polyèdre, on a donc

$$2A = pF$$

et

$$2A = qS$$

D'après le Lemme d'Euler, pour tout polyèdre convexe : $S - A + F = 2$.

$$\frac{2A}{q} - A + \frac{2A}{p} = 2 \iff \frac{1}{p} + \frac{1}{q} - \frac{1}{2} = \frac{1}{A} > 0 \iff \frac{1}{p} + \frac{1}{q} > \frac{1}{2}$$

Les seules solutions de l'équation sont : $(3,3),(3,4),(4,3),(5,3),(3,5)$. On en déduit qu'il existe uniquement 5 quintuplet (p,q,A,S,F) et donc 5 polyèdres convexes réguliers. □

2 Notion mathématique d'ensemble

Définition 2.1. *Un ensemble est une collection d'éléments. Pour tout élément x d'un ensemble E, on note $x \in E$ et on lit "x appartient à E.Si x n'est pas un élément de E, on note $x \notin E$.*

Exemples : $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathcal{P}[x], \{1,2,3\}, \{x \in \mathbb{R} | x^2 \leq 5\}, \mathbb{U} = \{z \in \mathbb{C} | \exists n \in \mathbb{N}^*, z^n = 1\}, \mathcal{P} = \{n \in \mathbb{N} \backslash \{0,1\} | n = rs, r, s \in \mathbb{N} \Rightarrow (r = 1)$ ou $(s = 1)\}, \mathcal{M}_{2,2}$ etc...

Définition 2.2. *Soient E et F deux ensembles, on dit que E est inclus dans F, noté $E \subset F$, si tout élément de E est un élément de F. On dit que E est une partie de F, les ensembles E et F sont égaux si et seulement si $E = F \Leftrightarrow (E \subset F) \wedge (F \subset E)$.*

On note $F \supset E$ pour signifier $E \subset F$

Exemples :

$\{1,2,2,2,3,1\} \subset \{1,2,3,4\}$

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

Pour montrer que $E \subset F$, on démarre par "Soit $x \in E$, montrons que $x \in F$"
Raisonnement par double-inclusion. Pour montrer que $E = F$, on montre que $E \subset F$ puis que $F \subset E$.

Proposition 2.1. *Soient E, F, G trois ensembles, si $E \subset F$ et $F \subset G$ alors $E \subset G$.*

Démonstration. Soit $x \in E$. Montrons que $s \in G$. Puisque $E \subset F$ on a que $x \in E \Rightarrow x \in F$. Puisque $F \subset G$ on a que $x \in F \Rightarrow x \in G$. □

2.1 Axiomatique de la théorie des ensembles

1. **Existence :** Il existe un unique ensemble, appelé ensemble vide et noté $\emptyset$, tel que quelques soit l'objet x, $x \notin \emptyset$.
2. **Compréhension :** Soit E un ensemble et $A(x)$ des assertions indexées par les éléments de E. Il existe un unique ensemble constitué des éléments de E tels que $A(x)$ est Vraie. On note $F := \{x \in E | A(x)\}$
3. **Puissance :** Soit E un ensemble, il existe un unique ensemble composé de tous les ensembles F inclus dans E. Ces ensembles sont appelé les parties de E, et cet ensemble des parties est noté :$\mathcal{P}(E) = \{F, F \subset E\}$
4. **Union :** Soient E et F deux ensembles, il existe un unique ensemble, noté $E \cup F$ composé des élément de E et F

Exemples : $\emptyset$, $\mathcal{P}(\emptyset) = \{\emptyset\}$, $\mathcal{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$
On a que $\mathbb{Q} \subset \mathbb{R}$ et $\mathbb{Q} \in \mathcal{P}(\mathbb{R})$.

Proposition 2.2. *Soient E, F, G trois ensembles. Alors :*

$E \cup \emptyset = E$

$E \cup F = E \cup F$

$E \cup (F \cup G) = (E \cup F) \cup G = E \cup F \cup G$

Puisque les parenthèses ne sont pas importantes, on les enlèves dans la notation : $E \cup F \cup G$

Démonstration. Cette preuve ne montre que la troisième égalité (les autres sont laissées en exercice).

$(\subset)$: Montrons que $E \cup (F \cup G) \subset (E \cup F) \cup G$.
Soit $x \in E \cup (F \cup G)$. Montrons que $x \in (E \cup F) \cup G$.

Si $x \in E$, alors $x \in E \cup F$ donc $x \in (E \cup F) \cup G$
Si $x \in F \cup G$, alors :
si $x \in F$, il appartient à $E \cup F$ et donc à $(E \cup F) \cup G$.
si $x \in G$, alors $x \in (E \cup F) \cup G$.

$(\supset)$: La deuxième preuve se démontre de la même manière.

□

2.2 Intersection et complémentaire

Définition 2.3. *Soient E et F deux ensembles, on définit l'intersection $E \cap F := \{x \in E \mid x \in F\}$ et l'exclusion $E \backslash F := \{x \in E \mid x \notin F\}$.*

Lorsque F est inclu dans E, $E \backslash F$ est appelé le complémentaire de F dans E. Quand E est évident dans le contexte, on écrit F^c au lieu de $E \backslash F$.
Si $F \cap E = \emptyset$, on dit que E et F sont disjoints.

Proposition 2.3. *Si E, F et G sont trois ensembles, alors :*

$E \cap (F \cap G) = (E \cap F) \cap G$
$E \cap F = F \cap E$
$E \cap \emptyset = \emptyset$

Démonstration. Raisonnement par double inclusion :

$(\subset)$: Montrons $E \cap (F \cap G) \subset (E \cap F) \cap G$
Soit $x \in E \cap (F \cap G)$.
Puisque $x \in E \cap E \cap (F \cap G)$, on $x \in E$ et $x \in F \cap G \subset F$.
Donc $x \in E \cap F$.
Puisque $x \in F \cap G \subset G$, on a $x \in G$.
Donc $x \in (E \cap F) \cap G$.

$(\supset)$: L'autre inclusion se démontre de la même manière.

□

Puisque les parenthèses n'importent pas, on note $E \cap F \cap G$.

Proposition 2.4. *Soient E, F, G trois ensembles, alors :*

$E \cup (F \cap G) = (E \cup F) \cap (E \cup G)$
$E \cap (F \cup G) = (E \cap F) \cup (E \cap G)$

Démonstration. Montrons la première égalité.
Montrons que $(E \cap F) \cup (E \cap G) \subset E \cap (F \cup G)$.

$(\subset)$: Soit $x \in (E \cap F) \cup (E \cap G)$, montrons que $x \in E \cap (F \cup G)$
Si $x \in E \cap F$, alors $x \in E$ et $x \in F \subset F \cup G$ donc $x \in E \cap (F \cup G)$.
Si $x \in E \cap G$, alors $x \in E$ et $x \in E \subset F \cup G$ donc $x \in E \cap (F \cup G)$.

$(\supset)$: Soit $x \in E \cap (F \cup G)$ et montrons que $x \in (E \cap F) \cup (E \cap G)$.
Puisque $x \in F \cup G$, on a deux cas :
Si $x \in F$, alors on a $x \in E \cap F$.
Si $x \in G$, alors on a $x \in E \cap G$.

□

Proposition 2.5 (Les lois de Morgan)**.** *Soient E, F, G trois ensembles, alors*

$E \backslash (F \cap G) = (E \backslash F) \cup (E \backslash G)$
$E \backslash (F \cup G) = (E \backslash F) \cap (E \backslash G)$

Démonstration. Montrons la première égalité par double inclusion.

($\subset$) : Montrons $(E\backslash F) \cup (E \cup G) \subset E\backslash(F \cap G)$.
Soit $x \in (E\backslash F) \cup (E\backslash G)$.

Si $x \in E\backslash F$, alors $x \in E$ et $x \notin F$, a fortiori, $x \notin F \cap x \in G$ et donc $x \in E\backslash(F \cap G)$

L'autre cas se montre de la même manière

($\supset$) : Montrons $(E\backslash F) \cup (E \cup G) \supset E\backslash(F \cap G)$. Soit $x \in E\backslash(F \cap G)$

Si $x \notin F$, on a $x \in E\backslash F$

Si $x \notin G$, on a $x \in E\backslash G$

□

Définition 2.4. *Considérons une famille d'ensembles $(A_i)_{i \in I}$ tel que $A_i \subset E$ pour tout $i \in I$. Soit $F \subset E$*

1. *Si $F \subset \bigcup\limits_{i \in I} A_i$, on dit que $(A_i)_{i \in I}$ est un recouvrement de F.*
2. *Si $F = \bigcup\limits_{i \in I} A_i$ et que les $A_i \cap A_j = \emptyset$ pour $i \neq j$, alors $\bigcup\limits_{i \in I} A_i$ est appelée une* partition *de F.*

Pour un recouvrement, chaue $x \in F$ est dans des A_i. Pour une partition, chaque $x \in F$ et exactement un des A_i, et aucun élément des A_i est hors de F.

Définition 2.5. *Soit I un ensemble et $(A_i)_{i \in I}$ une famille d'ensemble inclus dans I. On définit :*

— $\bigcup\limits_{i \in I} A_i := \{x \in E \mid \exists i \in I, x \in A_i\}$

— $\bigcap\limits_{i \in I} A_i = \{x \in E \mid \forall i \in I, x \in A_i\}$

2.3 Produit cartésien et n-uplets

Définition 2.6. *Soient E et F deux ensembles, on définit*

$$E \times F := \{(a, b) \mid a \in E,\ b \in B\}$$

Remarque : Dans la convention (a, b), l'ordre compte ! $(1, 2) \neq (2, 1)$ De manière analogue, $E \times F$ est *a priori* différent de $F \times E$. En fait, la propriété caractéristique de $(\cdot, \cdot)$ est $(x, y) = (x', y')$ si et seulement si $x = x'$ et $y = y'$
Plus généralement, on introduit $E_1, \times, \cdots, \times E_n := \{(x_1, \ldots, x_n), x_i \in E_i \text{ pour tout } i \leq n\} = E_1 \times (E_2 \times (\ldots (E_{n-1} \times E_n) \ldots)$.
On appelle (a, b) un couple ou une paire, (a, b, c) un triplet, (a, b, c, d) un quadruplet et pour la suite on appelle $(a_1, a_2, a_3, a_4, a_5, \ldots, a_n)$ un n-uplet.

3 Logique élémentaire

3.1 Calcul prépositionnel

On va se donner un ensemble $\mathcal{A}$(dénombrable) appelé ensemble des propositions atomiques.

Définition 3.1 (Formule propositionnelle)**.** *L'ensemble des formules propositionnelles (dépendant de $\mathcal{A}$) est défini comme le plus petit ensemble (pour l'inclusion) $\mathcal{L}$ tel que*

1. *$\mathcal{A} \subset \mathcal{L}$.*
2. *Si $A \in \mathcal{L}$, alors $\neg\mathcal{A} \in \mathcal{L}$.*
3. *Si $\mathcal{A}, \mathcal{B} \in \mathcal{L}$, alors $\mathcal{A} \wedge \mathcal{B} \in \mathcal{L}$ et $\mathcal{A} \vee \mathcal{B} \in \mathcal{L}$.*

Définition 3.2 (Sémantique)**.** *Une valuation φ est une fonction qui à chaque élément de $\mathcal{A}$ asscocie Vrai ou Faux. Une valuation équivaut à attribuer une notion de vérité à des propositions atomiques.*

φ attribue une valeur logique aux propositions atomiques. On étend les valeurs de vérités à toutes les formules propositionnelles en suivant les règles suivantes : ET, OU, NON.

Négation : Si A a une valeur VRAIE et FAUSSE, la valeur de $\neg A$ est donnée comme suit :

NON		OU			ET		
		A	B	$A \vee B$	A	B	$A \vee B$
A	$\neg A$	V	V	V	V	V	V
V	F	V	F	V	V	F	V
F	V	F	V	V	F	V	V
		F	F	F	F	F	F

Astuce : afin de montrer $A \vee B$ est vrai, on suppose que A est fausse et on montre que B est vrai.

En utilisant ces règles, on étend les valeurs V et F à toutes les formules propositionnelles.

Définition 3.3 (Tautologie)**.** *Une tautologie est une formule propositionnelle qui est vrai quelque soit ϕ.*

Exemple : $A \vee \neg A$

Définition 3.4. *Soit $A, B \subset \mathcal{L}$, on dit que A et B sont équivalentes si, quelques soient le choix de ϕ, A et B ont la même valeur logique.*

On note $A \Leftrightarrow B$

Exemple : A et $\neg\neg A$ sont équivalentes, $A \vee B$ et $B \vee A$

Proposition 3.1. *Soient $A, B \in \mathcal{L}$, $\neg(A \vee B)$ est équivalent à $(\neg A) \wedge (\neg B)$, de plus, $\neg(A \wedge B)$ est équivalent à $(\neg A) \vee (\neg B)$*

Démonstration. A faire ! □

Proposition 3.2 (Assertion)**.** *Soient $A, B \in \mathcal{L}$, les formules propositionnelles $A \Rightarrow B$, $\neg B \Rightarrow A$ et $\neg A \vee B$ sont équivalentes.*

Définition 3.5. *On défini $A \Rightarrow B$, lu comme A implique B par la table de vérité suivante :*

A	B	$A \Rightarrow B$
V	V	V
V	F	F
F	V	V
F	F	V

Si $A \Rightarrow B$ est vraie, on dit que A est une condition suffisante pour B. A l'inverse on dit que B est une condition nécessaire pour A.

Astuce : Pour démontrer que $A \Rightarrow B$, on suppose que A est VRAIE et on montre que B est VRAIE

Remarque : La négation de $A \Rightarrow B$ est $A \wedge \neg B$.

Proposition 3.3. *Les assertions $A \Rightarrow B, \neg B \Rightarrow \neg A, (\neg A) \vee B, \neg(A \wedge \neg B)$ sont équivalentes*

Démonstration. A faire à la maison ! □

Astuce : Si on veut montrer que $A \Rightarrow B$ est FAUSSE, il faut montrer $A \wedge \neg B$ Astuce : Pour démontrer que $A \Rightarrow B$, on peut démontrer que $\neg B \Rightarrow \neg A$, qui est appelé la contraposée de $A \Rightarrow B$. Annoncez ce type de raisonnement : "On montre le résultat par contraposé. Il est basé sur le tiers - exclu $(C \vee (\neg C))$ est une tautologie).

Si $C = A \Rightarrow B$, vous supposez $\neg C = A \wedge \neg B$. En général, vous montrer $\neg A$, mais sans utiliser A. Donc ce n'est qu'un raisonnement par contraposé).

Proposition 3.4. *Soient $A, B \in \mathcal{L}$, $A \Leftrightarrow B$ est équivalent à $(A \Rightarrow B) \wedge (A \Leftarrow B)$*

Démonstration. A faire □

Astuce : Pour démontrer $A \Leftrightarrow B$ nous avons 2 choix :

— $A \Leftrightarrow C_1, C_1 \Leftrightarrow C_2 \cdots C_n \Leftrightarrow B$

— On montre par double implication $A \Rightarrow B$ puis $B \Rightarrow A$

3.2 Calcul des prédicats

Définition 3.6. *Considérons les variables comme une liste de symboles notés $x, y, z, \dots$, alors un prédicat prend en compte une ou plusieurs variables et renvoie Vrai ou Faux.*

Exemple : $(x^2 + y^2) = x^2 + y^2$ renvoie faux dans le cas général. Le polynôme P de degré n à coefficients dans E a n racines

Par x, y, z des variables, on note $A(x, y, z)$ le prédicat. A n'a pas de valeur mais $A(x, y, z)$ en a une. On peut combiner les prédicats.

On peut utiliser $\neg, \vee, \wedge$ sur les prédicats : $\neg A(x) \vee (B(x, z) \wedge C(y, z))$.

Définition 3.7 (Quantificateurs)**.** *Soit $A(x, y, \dots)$ un prédicat*

— *Le prédicat $\forall x \in E, A(x, y \dots)$ se lit "pour tous les x dans E, alors $A(x, y, \dots)$". $\forall$ est le quantificateur universel*

— *Le prédicat $\exists x \in E, A(x, y, \dots)$ se lit "il existe un x dans E, alors $A(x, y, \dots)$. $\exists$ est le quantificateur existentiel.*

Le prédicat $\forall x \in E, A$ est vrai si et seulement si pour tout $x \in E, A(x)$ est vrai. Le prédicat $\exists x \in E, A$ est vrai si et seulement s'il existe un $x \in E, A(x)$ est vrai.

Proposition 3.5 (négation)**.** — *La négation du prédicat $\forall x \in E, A$ est : $\exists x \in E, \neg A$*

— *La négation du prédicat $\exists x \in E, A$ est : $\forall x \in E, \neg A$*

Preuve : Se fait par sémantique.

Remarque :

— L'ordre est important, $\forall x \in \mathbb{R}_+, \exists y \in \mathbb{R}_-, x = y^2$ est vrai. Mais $\exists x \in \mathbb{R}_-, \forall x \in \mathbb{R}_+, x = y^2$ est fausse.

— Si on a $\forall x \in E, A(x, y, z, \dots) = B(y, z, \dots)$

Exemple :

— $\exists x_0 \in \mathbb{R}, x_0^2 = 0$

— $\forall (a, b, c) \in \mathbb{C}^* \times \mathbb{C}^2, \exists z \in \mathbb{C}, az^2 + bz + c = 0$

— $\forall \epsilon > 0, \forall x \in \mathbb{R}, x_0 \in \mathbb{R}, \exists \delta > 0, [|x - x_0| < \delta \Rightarrow |f(x) - f(x_0)| < \epsilon]$

— $\forall \epsilon > 0, \exists \delta > 0, \forall x \in \mathbb{R}, x_0 \in \mathbb{R}, [|x - x_0| < \delta \Rightarrow |f(x) - f(x_0)| < \epsilon]$

On peut échanger deux $\forall$ qui se suivent ou deux $\exists$ qui se suivent !

$$\neg(\forall x \in E, A(x)) \Leftrightarrow \exists x \in E, \neg A(x)$$

et de la même manière

$$\neg(\exists x \in E, A(x)) \Leftrightarrow \forall x \in E, \neg A(x)$$

Exemples :

— $\neg(\forall \epsilon > 0, \forall x \in \mathbb{R}, x_0 \in \mathbb{R}, \exists \delta > 0, [|x - x_0| < \delta \Rightarrow |f(x) - f(x_0)| < \epsilon]) \Leftrightarrow \exists \epsilon > 0, \exists x \in \mathbb{R}, \exists x_0 \in \mathbb{R}, \forall \delta > 0, [|x - x_0| < \delta \wedge |f(x) - f(x_0)| \geq \epsilon]$

Astuce : Pour montrer $\forall x \in E, A(x)$ est vrai, on pose :

$$\text{Soit } x \in E, \ldots$$

Ou alors on peut faire une preuve par un contre exemple : Trouver un x tel que l'assertion $A(x)$ est fausse.

Exemple : $\forall x \in \mathbb{R}, \forall y \in \mathbb{R}, [x < y \Rightarrow \exists \Rightarrow, x < z < y$

Démonstration. Soit $x \in \mathbb{R}$ et $y \in \mathbb{R}$ tels que $x < y$. Montrons qu'il existe $z \in \mathbb{R}, x < z < y$. Prenons $z = \frac{x+y}{2}$. On a bien $x < z < y$ $\square$

4 Applications

4.1 Définitions

Définition 4.1. *Soit E et F deux ensembles quelconques et $A \subset E \times F$. Alors A est un graphe fonctionnel si*

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

Définition 4.2. *Une application (ou fonction) est la donnée de deux ensembles E et F et d'un grpahe fonctionnel $A \subset E \times F$.*
Notation : f, qui est la donnée de (E, F, A), est notée

$$f : \begin{array}{ccc} E & \to & F \\ x & \mapsto & f(x) \text{ qui est l'unique } y \in F \text{ tel que } (x,y) \in A \end{array}$$

f envoie chaque élément de E sur un élément de F.

Exemples :

- $\chi_{\mathbb{Q}} : \begin{array}{ccc} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & \left\{ \begin{array}{ll} 1 & \text{si } x \in \mathbb{Q} \\ 0 & \text{sinon} \end{array} \right. \end{array}$
- $f : \begin{array}{ccc} \mathbb{R}^2 & \to & \mathbb{R} \\ (x,y) & \mapsto & x^2 + y^2 \end{array}$
- fonction carrée puis la fonction carrée juste sur les positifs !
- la fonction tangeante
- La fonction de Dirac : $\delta_{x_0} : \begin{array}{ccc} E & \to & \{0,1\} \\ x & \mapsto & \left\{ \begin{array}{ll} 1 & \text{si } x = x_0 \\ 0 & \text{sinon} \end{array} \right. \end{array}$
- L'application identité
- Les suite de $\mathbb{N}$ dans $\mathbb{E}$
- Une famille indéxée par I et à valeurs dans E est une application $x : \begin{array}{ccc} I & \to & E \\ i & \mapsto & x(i) \end{array} \equiv (x_i)_{i \in I}$
- $\pi : \begin{array}{ccc} \mathbb{N} & \to & \mathbb{N} \\ n & \mapsto & \text{le nombre de nombre premiers inférieurs à } n \end{array}$

  On a le beau résultat : $\frac{\pi(n) \log n}{n} \to 1$

4.2 Deux théorèmes classiques de la théorie des ensembles

Théorème 4.1 (Théorème de Cantor)**.** *Soit E un ensemble, il n'existe pas de surjection de E dans $\mathcal{P}(E)$*

Démonstration. Preuve par l'absurde.

$$\text{Soient } S : E \mapsto \mathcal{P}(E) \text{ et } S := \{x \in E, x \notin S(x)\}$$

Montrons que A n'a pas de préimage :
Supposons $\exists a \in E, S(a) \in A$. Alors :

$$\text{si } a \in A \text{ alors } a \in S(a) \in A \Rightarrow\Leftarrow$$

$$\text{si } a \notin A \text{ alors } a \in S(a) \in A \Rightarrow\Leftarrow$$

□

Théorème 4.2 (Théorème de Cantor - Schröder - Bronstein)**.** *Soient E et F deux ensembles. S'il existe une injection de E dans F et une injection de F dans E, alors il existe une bijection de E dans F.*

Démonstration. Intuitivement, on souhaite découper E en deux ensembles : Y et $E\backslash Y$ tels que $E\backslash Y = g(F\backslash f(Y))$ et $Y = E\backslash g(F\backslash f(Y))$

Proposition 4.1 (Théorème du point fixe)**.** *Soit $f : \mathcal{P}(E) \to \mathcal{P}(E)$ tel que $A \subset B \Rightarrow f(A) \subset f(B)$, alors :*

$$\exists Y \in \mathcal{P}(E),\ f(Y) = Y$$

Soient $f : E \to F$ et $g : F \to E$ deux applications injectives. Posons :

$$h : \begin{array}{ccc} \mathcal{P}(E) & \to & \mathcal{P}(E) \\ X & \mapsto & E \setminus g(F \setminus f(Y)) \end{array}$$

On vérifie aisément que $A \subset B \Rightarrow h(A) \subset h(B)$

$$\exists Y \subset E \text{ tq } Y = h(Y) = E\backslash g(F\backslash f(Y))$$

On pose :

$$\Psi : \begin{array}{ccc} E & \to & F \\ x & \mapsto & \begin{cases} f(x) & \text{si } x \in Y \\ !y \text{ tq } g(y) = x & \text{si } x \in E\backslash Y \end{cases} \end{array}$$

L'injectivité de g garantie l'unicité. Puisque $E\backslash Y = g(F\backslash f(Y))$ donc $\forall x \in E\backslash Y, \exists y \in F\backslash f(Y), x = g(y)$ On peut alors montrer que Ψ est bijectif.

□

5 Relation d'ordre

5.1 Définitions

Définition 5.1. *Une relation sur E, notée, $\leq$, est un prédicat prenant 2 éléments x et y de E et rendant Vrai ou Faux.*

Définition 5.2. *Soit E un ensemble et $\leq$ une relation sur E. $\leq$ est une relation d'ordre si et seulement si :*

1. *$\leq$ est réfléxive : $\forall x \in E,\ x \leq x$*
2. *$\leq$ est transitive : $\forall x, y, z \in E,\ x \leq y$ et $y \leq z \Rightarrow x \leq z$*
3. *$\leq$ est anti symétrique : $\forall x, y \in E,\ x \leq y$ et $y \leq x \Rightarrow x = y$*

Exemples : $\leq$ est une relation d'ordre. Mais $<$ n'en est pas une.
Pour montrer que $\leq$ est une relation d'ordre, on divise la preuve en 3 parties :

1. On montre que $\leq$ est réfléxive : Soit $x \in E \dots$
2. On montre que $\leq$ est transitive : Soient $x, y, z \in E$ tq $x \leq y$ et $y \leq z \dots$
3. On montre que $\leq$ est antisymétrique : Soient $x, y \in E$ tq $x \leq y$ et $y \leq x \dots$

Définition 5.3 (Espace ordonné)**.** *$(E, \leq)$ est un espace ordonné si $\leq$ est une relation d'ordre sur E.*

Définition 5.4 (Relation totale)**.** *$\leq$ est une relation d'ordre dite totale si*

$$\forall x, y \in E, x \leq y \text{ ou } y \leq x$$

Exemples :

$(\mathbb{R},\ \geq)$; $(\mathbb{R},\ \geq)$; $(\{1\}, =)$ sont des relation d'ordre totales.

$(\mathbb{R},\ \geq)$; $(\mathcal{P}(E),\ \subset)$; $(\mathbb{N}^*,\ \div)$ ne sont pas des relations d'ordre totales.

5.2 Majorants, minorant, ...

Définition 5.5. *Soit $(E,\ \leq)$ un ensemble ordonné et $F \subset E$ un ensembe non-vide. Soient $m, M \in E$*

1. *M est un majorant de F si $\forall x \in F, x \leq M$*
2. *m est un minorant de F si $\forall \in F, m \leq x$*
3. *M' est le suprémum de F si M' est un majorant de F et si $\forall M \in E, M' \leq M$*
4. *m' est l'infimum de F si m' est un minorant de F et si $\forall M \in E, m \leq m'$*

Remarque :

Si le suprémum de F appartient à F, alors on dit que c'est le maximum de F.

Si l'infimum de F appartient à F, on l'appelle le minimum de F

Ces éléments n'existent pas forcément

Proposition 5.1. *S'il existe un suprémum/infimum, alors celui-ci est unique*

Démonstration. La preuve est laissée en exercice. □

Exemples :

$(\mathbb{R}, \leq)$; $(\mathbb{N}^*, \div)$ n'ont pas de majorants.

Soit $E = \{k_1, \ldots, k_n\}$ un ensemble fini, alors $k = \prod_{i=1}^{n} k_i$ est un majorant de E et $ppcm(k_1, \ldots, k_n)$ est le suprémum de E.

$2\mathbb{N}^*$ est minoré par 2.

Proposition 5.2. *Soient E, F, G trois ensembles tels que $G \subset F \subset E$ avec $(E, \leq)$ ordonné, on a :*

$$\sup G \leq \sup F \text{ et } \inf G \leq \inf E$$

Démonstration. La preuve est laissée en exercice. □

Remarque : Quand $(x_i)_{i\in I}$, on appelle $\sup_{i\in I} x_i := \sup x_i, i \in I$. Si $I \subset J \Rightarrow \sup_{i\in I} x_i \leq \sup_{j\in J} x_j$.

Proposition 5.3 (Critère de $\mathbb{R}$ muni de l'ordre usuel)**.** *Soient $E \subset \mathbb{R}$ et $M \in \mathbb{R}$ alors on a les équivalences suivantes :*

— *M est le suprémum de E*

— $[\forall x \in E, x \leq M]$ *et* $[\forall y \in \mathbb{R}, y < M] \Rightarrow [\exists x \in E, y < x]$

Démonstration. Démonstration : Laissée en exercice □

5.3 Application croissantes, décroissantes et monotones

Définition 5.6. *Soient 2 ensembles ordonnés $(E, \mathcal{R})$,$(F, \mathcal{R}')$ et $f : E \to F$.*
On dit que f est croissante si $\forall x, y \in E, x\mathcal{R}y \Rightarrow f(x)\mathcal{R}' f(y)$.
On dit que qu'elle est strictement croissante si elle est croissante et injective.
On définit de même une fonction décroissante si $\forall x, y \in E, x\mathcal{R}y \Rightarrow f(y)\mathcal{R}f(x)$.
On dit également qu'une fonction est strictement décroissante si elle est décroissante et injective. Une application est dite monotone si elle est croissante ou décroissante.

Exemples :

$f : \begin{array}{ccc} \mathbb{R}_+ & \to & \mathbb{R}_+ \\ x & \longmapsto & |x| \end{array}$ est une application croissante

$g : \begin{array}{ccc} \mathbb{R} & \to & \mathbb{R} \\ x & \longmapsto & |x| \end{array}$ n'est pas une application monotone

$h : \begin{array}{ccc} (\mathbb{N}^*, \mid) & \to & (\mathbb{N}*, \leq) \\ n & \longmapsto & n \end{array}$

$i : \begin{array}{ccc} (\mathbb{N}^*, \leq) & \to & (\mathbb{N}*, \mid) \\ n & \longmapsto & n \end{array}$ n'est pas monotone car $2 \leq 3$ mais $2 \nmid 3$.

Proposition 5.4. *Soient E, F, G trois ensembles ordonnées. Soient $f : E \to F$ et $g : F \to G$, alors*

1. *Si f et g sont monotones de même sens, alors $g \circ f$ sera croissante.*
2. *Si f et g sont monotones de sens opposés, alors $g \circ f$ sera décroissante.*

Démonstration. La preuve laissée en exercice. □

Définition 5.7. *f est majorée s'il existe $M \in E$ tel que $\forall x \in E, f(x) \leq M$. On appelle suprémum de f, noté $\sup f$, le plus petit M vérifiant $\forall x \in E, f(x) \leq M$*

Remarque : $\sup f = \sup \{f(x) | x \in E\} = \sup f(E)$

6 Entiers naturels et principe de récurrence

Théorème 6.1 (Axiomes de Peano). *Il existe un unique triplet* $(n, \mathbb{N}, \mathcal{S})$ *tel que :*

1. $\mathbb{N}$ *est un ensemble*
2. n *est un élément de* $\mathbb{N}$
3. $\mathcal{S}$ *est une fonction de* $\mathbb{N}$ *dans* $\mathbb{N}$ *tel que*
   - $\mathcal{S}$ *est injective*
   - $\mathcal{S}(\mathbb{N}) = \mathbb{N}\backslash\{0\}$
   - $\forall A \subset \mathbb{N}, [0 \in A$ *et* $n \in A \Rightarrow \mathcal{S}(n) \in A] \Rightarrow A = \mathbb{N}$

$\mathcal{S}$ *est appelé la fonction successeur et* $\mathcal{S}(n)$ *est appelé le successeur de* n*.*
On note : $\mathcal{S}(0) = 1, \mathcal{S}(n) = n + 1$ *ce qui garantie le principe de récurrence.*

Théorème 6.2 (Principe de récurrence). *Soit* $(\mathcal{H}_n)$ *une famille d'assertion indexée par* $n \in \mathbb{N}$*. Si l'assertion* $[\mathcal{H}_0$ *et* $\forall n \in \mathbb{N}, \mathcal{H}_n \Rightarrow \mathcal{H}_{n+1}]$ *est vraie, alors* $\mathcal{H}_n$ *est vrai pour tout* $n \in \mathbb{N}$*.*

Démonstration. Définissons $A := \{n \in \mathbb{N}, \mathcal{H}_n\}$.
Puisque $\mathcal{H}_0$ et $\Rightarrow \mathcal{H}_{n+1}, \forall n \in \mathbb{N}$. Alors en particulier,
$\mathcal{H}_0$ est vraie, ce qui implique que $0 \in A$.
Soit $n \in \mathbb{N}$ tels que $n \in A$.
De plus : $\mathcal{H}_n \Rightarrow \mathcal{H}_{n+1}$ est vraie, ce qui implique que $\mathcal{H}_{n+1}$ est vraie.
L'axiome de Peano est donc impossible, donc $A = \mathbb{N}$. □

Remarque :

1. Pour faire une démonstration par récurrence, on procède comme suit :
   Définissons $\mathcal{H}_n$: "_ _ _ _ _"
   Montrons $\mathcal{H}_0$: "_ _ _ _ _"
   Soit $n \in \mathbb{N}, \mathcal{H}_n$, montrons $\mathcal{H}_{n+1}$
2. La récurrence peut être généralisée de la façon suivante :
   $[\mathcal{H}_k$ et $\forall n \geq k, \mathcal{H}_n \Rightarrow \mathcal{H}_{n+1}]$ alors[] $\mathcal{H}_n$ est vrai $\forall \geq K$.
   $[\mathcal{H}_0$ et $\forall n \in \mathbb{N}, \mathcal{H}_{2n} \Rightarrow \mathcal{H}_{2n+2}]$
3. La récurrence forte :
   $[\mathcal{H}_0$ et $(\forall n \in \mathbb{N}, (\forall k \leq n, \mathcal{H}_k)) \Rightarrow \mathcal{H}_{n+1}]$, alors $\mathcal{H}_n$ est vraie $\forall n \in \mathbb{N}$
   $\mathcal{H}_n = \{\forall k < n, \mathcal{H}_k\}$
4. $\mathcal{H}_n$ est l'hypothèse de récurrence.

Proposition 6.1 (Construction de + et ×). *Il existe deux fonctions :*

$\oplus : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$
$\ominus : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$

qui satisfont ces propriétés :

1. $\forall n \geq 0, \oplus(n, 0) = n, \oplus(n, 1) = \mathcal{S}(n) = n + 1$
2. $\forall n \geq 0, \otimes(n, 0) = 0, \otimes(n, 1) = n$
3. $\forall n, k \geq 0, \oplus(n, k) = \oplus(k, n)$ *et* $\otimes(n, k) = \otimes(k, n)$
4. $\forall n, k, l \geq 0, \oplus(n, \oplus(k, l)) = \oplus(\oplus(n, k), l)$ *et* $\otimes(n, \otimes(k, l)) = \otimes(\otimes(n, k), l)$
5. $\forall n, k, l \geq 0, \otimes(n, \oplus(k, l)) = \oplus(\otimes(n, k), \otimes(n, l))$

Démonstration. On définit $\oplus(n, .)$ par récurrence.

$$\mathcal{H}_k : \text{"} \oplus (n, k) \text{ est bien défini "}$$

Montrons $\mathcal{H}_0$:

$$\oplus(n, 0) := n$$

Soit $k \in \mathbb{N} : \mathcal{H}_k$, montrons $\mathcal{H}_{k+1}$

$$\oplus(n, k+1) = \mathcal{S}(\oplus(n,k))$$

On définit $\otimes(n,.)$ par récurrence.

$$\mathcal{H}_k : \text{"} \otimes (n,k) \text{ est bien défini "}$$

Montrons $\mathcal{H}_0$:

$$\otimes(n,0) := 0$$

Soit $k \in \mathbb{N} : \mathcal{H}_k$, montrons $\mathcal{H}_{k+1}$

$$\otimes(n,k+1) = \oplus(\otimes(n,k), \otimes(n,1))$$

On notera à présent $f(x,.) : \begin{array}{ccc} F & \to & G \\ y & \mapsto & f(x,y) \end{array}$ □

Définition 6.1 (ordre).

$$\forall n, m \in \mathbb{N}, n \geq m \Leftrightarrow \exists k \in \mathbb{N}, n = m + k$$

Théorème 6.3 ($\mathbb{N}$ est bien ordonné). *Toute partie non-vide de $\mathbb{N}$ a un plus petit élément*

Démonstration. Par récurrence,

$$\mathcal{H}_n : \text{"}\forall A \subset \mathcal{P}(\mathbb{N}) \neq \emptyset, \exists a \in A, \forall n \in A, a \leq n\text{"}$$

Montrons $\mathcal{H}_0$: Tout A contenant des éléments plus grand ou égal à 0 contient 0. Comme 0 est le plus petit élément de $\mathbb{N}$, c'est aussi le plus petit élément de A. Soit $n \in \mathbb{N}, \mathcal{H}_n$ vraie, montrons $\mathcal{H}_{n+1}$:
Soit $A \subset \mathcal{P}(\mathbb{N} : a \in A, a \leq n+1$.
Si $a < n$, alors par l'hypothèse de récurrence, il s'agit bien du plus petit élément.
Si $n+1 \in A, \forall k \leq n, k \notin A$.
Donc $\forall a \in A, a \geq m+1$ et m+1 est le plus petit élémentde A, donc $\mathcal{H}_n$ est vrai pour tout $n \in \mathbb{N}$. □

Théorème 6.4 (Principe de descente infini). *Toute suite suite décroissante d'entiers naturels est* stationnaire.

Démonstration. Soit (u_n) une suite décroissante d'entiers naturels. Notons $A := \{u_n, n \in \mathbb{N}\}$

$$A \neq \emptyset \Rightarrow \exists N \in \mathbb{N}, u_N \leq a, \forall a \in A$$

$$\Leftrightarrow \forall n \geq N u_n \leq u_N$$

Car (u_n) est décroissante. Mais puisque u_N est minimal

$$\Leftrightarrow u_n \geq u_N \Rightarrow \forall n \geq N, u_n = u_N$$

□

Théorème 6.5 (Division euclidienne). *Soient $a \in \mathbb{N}$ et $q \in \mathbb{N}^*$. Alors*

$$\exists!(p,r) \in \mathbb{N}^2 : 0 \leq r < p \text{ et } a = pq + r$$

Démonstration. <u>Unicité :</u> Soient (p,r), (p',r') $\in \mathbb{R}^2$:

$$pq + r = a = p'q + r' \Leftrightarrow r - r' = q(p - p')$$

Or : $r - r' < q$
$\Leftrightarrow \mathrm{(p - p')q < q \Leftrightarrow p - p' = 0 \Rightarrow r = r'}$

<u>Existence :</u> fixons $p \in \mathbb{N}^*$, On raisonne par récurrence.

$$\mathcal{H}_n : \text{"}\forall a \leq n, \exists (p,r) \in \mathbb{N} \times \mathbb{N}, a = pq + r, r \in |[0,q|]\text{"}$$

Montrons $\mathcal{H}_0$:

$$0 = 0 \cdot p + 0$$

On pose $(q, r) = (0, 0)$

$$\mathcal{H}_p : a = 0 \cdot p + a$$

On pose $(q, r) = (0, a)$ Soit $n > p$, supposons $\mathcal{H}_n$ et montrons $\mathcal{H}_{n+1}$:
Si $a < n$, alors $\mathcal{H}_n$ impose l'existence de (q, r) tel que $a = pq + r$ et $0 \leq r < p$
Si $a = n$, alors $0 < a - p < n$, alors $\mathcal{H}_n$ impose l'existence de $(q', r') \in \mathbb{N}^2$ tel que $a - p = pq' + r$ et $0 \leq r' < p$.
Alors $a = p(q' + 1) + r'$. Il suffit donc de poser $q = q' + 1$ et $r = r'$ □

7 Ensembles finis et notion de cardinal

7.1 Définitions

Définition 7.1 (Equipotence)**.** *Soient E et F deux ensembles. E et F sont dits équipotents s'il existe une bijection tel que*

$$f : E \to F$$

On peut voir que l'équipotence comme "E et F ont la même cardinalité".

Proposition 7.1. *Soient $m, n \in \mathbb{N}$*

1. *S'il existe une bijection de E dans $[\![1, n]\!]$, alors $\forall a \in E$, il existe une bijection de $E \backslash \{a\}$ dans $[\![1, n-1]\!]$.*
2. *S'il existe une injection de $[\![1, m]\!]$ dans $[\![1, n]\!]$, cela implique que $m \leq n$.*
3. *S'il existe une surjection de $[\![1, m]\!]$ dans $[\![1, n]\!]$, cela implique que $m \geq n$.*
4. *S'il existe une bijection de $[\![1, m]\!]$ dans $[\![1, n]\!]$, cela implique que $m = n$.*

Démonstration. Pas présent à l'examen. □

Définition 7.2. *Soit E un ensemble. E est fini si $E \neq \emptyset$ ou s'il existe $n \in \mathbb{N}$ tel que E et $[\![1, n]\!]$ sont équipotents. Dans ce cas, n est appelé* ***cardinal*** *de E et est noté $Card(E)$ ou bien $|E|$.*

Proposition 7.2. *Soit E un ensemble fini :*

1. *Soit $f : E \to F$ bijective, alors $Card(F) = Card(E)$*
2. *Soit $A \subset E$, alors $Card(A) \leq Card(E)$*
3. *Soit $f : E \to F$, alors $f(E)$ est fini et $Card(f(E)) \leq Card(E)$, de plus, si $Card(f(E)) = Card(E)$, cela implique que f est injective.*

Démonstration. Pas présent à l'examen. □

Théorème 7.1 (Principe des tiroirs)**.** *Soit E, F deux ensembles finis et $f : E \to F$.*

$$Card(E) > Card(F) \Rightarrow f \texttt{ non-injective}$$

Démonstration. Par contraposée, supposons que f est injective. D'après la propriété précédente on a :

$$Card(f(E)) = Card(E)$$

Mais puisque $f(E) \subset F$ et F est un ensemble fini

$$Card(f(E)) \leq Card(E)$$

.
Donc

$$Card(F) \leq Card(E)$$

. □

Proposition 7.3. *Soient E, F deux ensembles finis et $f : E \to F$,*

$$Card(E) = Card(F) \Leftrightarrow f \text{ bijective}$$

Démonstration. $f : E \to f(E)$ est injectif, donc $Card(E) = Card(F) = Card(f(E))$ ce qui montre que$f$ est surjectif et donc bijectif. □

7.2 Analyse combinatoire des ensembles finis

Théorème 7.2. *1. $Card(E \cup F) = Card(E) + Card(F) - Card(E \cap F)$*

2. Si $E \subset F$,$Card(F \backslash E) = Card(F) - Card(E)$

3. Si $E \times F$ est un ensemble fini, alors $Card(E \times F) = Card(E) * Card(F)$

4. On note F^E les fonction de E dans F, on a alors $Card(F^E) = Card(F)^{Card(E)}$

Démonstration. La démonstration est laissée en exercice. ;-) ☐

Théorème 7.3 (Principe de Bergers)**.** *Soit E un ensemble fini*

1. Soit $(E_i)_{i \in I}$ une partition de E,

$$Card(E) = \sum_{i \in I} Card(E_i)$$

2. Soit $f : E \to F$,

$$Card(E) = \sum_{y \in F} f^{-1}(\{y\})$$

Démonstration. Soit $f : E \to E$ une bjection. On dit que f est une permutation de E. On note $S(E)$ l'ensemble des permutations de E. On définit la factorielle de n, notée $n! = 1 \times 2 \times 3 \times \cdots \times n$. Pour $0 \leq p \leq n$, on définit "p parmi n" comme $\binom{n}{p} = \frac{n!}{p!(n-p)!} = \frac{n(n-1)(n-p+1)}{p!}$. ☐

Proposition 7.4. *1. $Card(\mathcal{P}(E)) = 2^{Card(E)}$*

2. Soit $p < Card(E)$.Le nombre de p-uplets $(x_1, \ldots, x_p) \in E^p$ tel que les x_i sont distincts sont $\frac{n!}{(n-p)!}$

3. $Card(\mathcal{S}(E)) = n!$

4. Le nombre de sous-ensemble à p éléments parmi n éléments de E est $\binom{n}{p}$

Démonstration. Soit $E = \{x_1, \ldots, x_n\}, \mathbb{I}_A(x) = \begin{cases} 1 & \text{si } x \in A \\ 0 & \text{sinon} \end{cases}$ Démonstration à terminer soi-même ! ☐

Proposition 7.5. *Soit $0 \leq p \leq n$ deux entiers,*

1. $\binom{n}{k} = \binom{n}{n-k}$

2. Si $n \geq 1$ et $p \geq 1$, alors $p\binom{n}{p} = n\binom{n-1}{p-1}$

3. La formule de Pascal : $\binom{n+1}{p+1} = \binom{n}{p} + \binom{n}{p+1}$

4. Binôme de Newton : $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$

Démonstration. La démonstration est à faire soi-même ! ☐

8 Ensembles infinis

Définition 8.1. *Un ensemble E est dit dénombrable s'il est équipotent avec* $\mathbb{N}^*$

Remarque : Parfois, "dénombrable" recouvre aussi le cas de ensembles finis. Un ensemble qui n'est pas dénombrable est dit indénombrable.

Exemples :

$\mathbb{N}$, $2\mathbb{N}$, $\mathbb{Z}$, $\mathbb{N}^2$, $\mathbb{Q}$ sont des ensembles dénombrables.

Théorème de Cantor : $\mathbb{R}$ n'est pas dénombrable.

9 Relations d'équivalence

9.1 Définition

R est une relation d'équivalence sur E si et seulement si :
- $\forall x \in E, xRx$ (Réflexivité)
- $\forall x, y, z \in E, [(xRy \text{ et } yRz) \Rightarrow xRz]$ (Transitivité)
- $\forall x, y \in E, xRy \Rightarrow yRx$ (Symétrie)

Pour montrer que R est une relation d'équivalence, il faut procéder comme suit :
- Montrons que R est réflexif. Soit $x \in E$ tel que xRx ...
- Montrons que R est transitif. Soient $x, y, z \in E$ tels que xRy et yRz. Montrons xRz ...
- Montrons que R est symétrique. Soient $x, y \in E$ tels que xRy. Montrons que yRx ...

Exemples :
1. " = " sur E est une relation d'équivalence
2. Soit E un emsemble et $\pi : E \to F$, alors xRy si et seulement si $\pi(x) = \pi(y)$

9.2 Définition

Soit E un ensemble et R une relation d'équivalence sur E. Pour $x \in E$, on appelle la cla classe d'équivalence de x l'ensemble $\bar{x} = \{y \in E, yRx\}$.
Un élément d'une classe d'équivalence est appelé un représentant de la classe d'équivalence On appelle espace ou ensemble quotient de E l'ensemble $E/R = \{\bar{x}, x \in E\}$.
L'application $\phi : \begin{array}{l} E \to E/R \\ x \mapsto \bar{x} \end{array}$ est la projection canonique.

9.3 Théorèmes

Soit E un ensemble et R une relation d'équivalence sur E. L'ensemble des classes d'équivalences de R sur E forme une partition de E.

Démonstration. □

Construction de $\mathbb{Z}$: Il existe un ensemble $\mathbb{Z}$ ainsi que des opérations $+_{\mathbb{Z}}, *_{\mathbb{Z}}$ ainsi que des éléments $0_{\mathbb{Z}}, 1_{\mathbb{Z}}$ tels que :

$(\mathbb{Z},\ +_{\mathbb{Z}},\ *_{\mathbb{Z}},\ 0_{\mathbb{Z}},\ 1_{\mathbb{Z}})$ forme un anneau commutatif (unitaire).

il existe une injection de $\mathbb{N}$ dans $\mathbb{Z}$ tel que $i(0) = 0_{\mathbb{Z}}, i(1) = 1_{\mathbb{Z}}, i(n +_{\mathbb{Z}} m) = i(n) +_{\mathbb{Z}} i(m), i(n *_{\mathbb{Z}} m) = i(n) *_{\mathbb{Z}} i(m)$

Construction de $\mathbb{Q}$:
Construction de $\mathbb{R}$: Il existe une ensemble $\mathbb{R}$ muni de deux opération $+_{\mathbb{R}}$ et $*_{\mathbb{R}}$ ainsi qu'une fonction $|.|$ et de deux éléments $0_{\mathbb{R}}$ et $1_{\mathbb{R}}$ qui vérifient :

$(\mathbb{R}, +_{\mathbb{R}}, *_{\mathbb{R}}, 0_{\mathbb{R}}, 1_{\mathbb{R}}, |.|)$ est un corps normé

Il existe une injection $i : \mathbb{Q} \to \mathbb{R}$ tel que $i(0_{\mathbb{Q}}) = 0_{\mathbb{R}}$ et $i(1_{\mathbb{Q}}) = 1_{\mathbb{R}}$

Toute suite de Cauchy est à valeur dans $\mathbb{R}$ est convergente

Démonstration. □