1 Théorie Naïve des ensembles

1.1 Introduction et Définitions

Un objet est dit un objet mathématique s'il a été formelement définie et avec lequel on peut faire des raisonnement deductif et des preuves mathématique. Ainsi de manière naïve, on définit un ensemble comme un collection d'objet mathématique rassemblés d'après, au moins, une propriété communes. Ces propriété sont suffisant pour affirmer si un objet appartient ou non à un ensemble. Les objets sont aussi les élément d'un ensemble. Si x est un élément de l'ensemble E, on le notera tout simplement par : $x \in E$.
On notera ausi un ensemble et ses éléments séparé par des virgule entre deux accolades ou indiquant les propriété de ces élémennt entre deux accolades. Ainsi par exemple, on notera l'ensemble des entiers naturels pair par $\{0, 2, 4, 6, \cdots\}$ ou tout simplement par $\{n \in \mathbb{N} | \text{n est pair}\}$.
Deux éléments d'un ensemble sont égaux s'il définissent les même objet mathématique, ainsi l'ensemble

$$\{-3, 5, \{1, 2, 3\}, 2, 4, 2, \{2, 3, 1\}\}$$

définit le même ensemble que

$$\{-3, 5, 4, 2, \{2, 3, 1\}\}.$$

1.1.1 Exemple

1. On designe respectivement par $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ l'ensemble des nombres entiers naturels, l'ensembles des nombres relatifs, l'ensemble des nombres rationnels, l'ensemble des nombres réels, l'ensemble des nombres complexes.

2. Considérons E l'ensemble des hommes fidèle et infidèle. Cet ensemble n'as pas d'élément car un tel homme n'existe pas. On appelera E l'ensemble vide et on la note par $\emptyset$ ou bien $\{\}$.

Soient A et B deux ensembles. On dit que A est inclus dans B (qu'on notera par $A \subset B$) si tous les éléments de A est un élément de B. On dit aussi dans ce cas que A est partie ou un sous ensemble de B. Ainsi, les deux ensembles sont égaux (qu'on notera $A = B$) si $A \subset B$ et $B \subset A$.
Si E est un ensemble, on notera l'ensemble de partie de E par $\mathcal{P}(E)$.

1.1.2 Remarque

Soit E un ensemble quelconque et n un entier naturel.

1. L'ensemble vide est une partie de E;

2. Supposons que l'ensemble E admet exactement éléments. Alors $\mathcal{P}(E)$ admet exactement 2^n éléments.

On definit l'ensemble $B \backslash A$ comme l'ensemble des éléments de B qui n'appartiennent pas à A. Si de plus $A \subset B$, on notera l'ensemble $B \backslash A$ par C_B^A (ou tout simplement par A^c s'il n'y a pas de confusion). On appelera aussi l'ensemble C_B^A la complementaire de A dans B.
Maintenant, on va introduire deux notions importantes concernants les opérations sur les ensembles, à savoir l'intersection et l'union.
L'ensemble qui ne contient que A et B à la fois sera noté $A \cap B$, tandis que l'ensemble qui ne contient, soit les éléments de A ou soit les éléments B sera noté $A \cup B$.
Si de plus les éléments de A et B n'ont pas d'élément en commun, on dit qu'ils sont disjoints et on a $A \cap B = \emptyset$.
Ainsi on a les proprietes suivantes :

1.1.3 Proposition

Soient A, B, C trois ensembles quelconques:

1. $A \cap A = A \cup A = A$ (Idempotente)
2. $A \cap B = B \cap A,\ A \cup B = B \cup A$ (Commutativité)
3. $A \backslash B = A \cap B^c$
4. $(A \cap B)^c = A^c \cup B^c,\ (A \cup B)^c = A^c \cap B^c$ (Lois de Morgan)
5. $A \cap (B \cap C) = (A \cap B) \cap C,\ A \cup (B \cup C) = (A \cup B) \cup C$ (Associativité)
6. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C), A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (Distributivité)
7. $B = C_C^A \Leftrightarrow A \cup B = C$ et $A \cap B = \emptyset$.

Soient A et B deux ensembles. L'ensemble produit définie par:

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

est appelé le produit cartésien de A par B. Bien sur en général, on a $A \times B \neq B \times A$. Enfin, si A et B sont deux paries d'un ensembles E, on dit que A et B sont disjoints si $A \cap B = \emptyset$.

1.2 Applications

Dans cette section, considérons deux ensembles E et F.

1.2.1 Définition

Une application f de l'ensemble E dans l'ensemble F est une relation de correspondance qui a toute élément de $x \in E$, on associe un élément $y \in F$. L'applicatjion f sera noté

$$f : E \mapsto F,\ x \mapsto y := f(x),$$

Ainsi, si $x : f(y)$ on dit que l'élément y est l'image de x par f, tandis que x est l'antécedent de y par F. Bien entendue les variables x et y sont muets. On pourra les noté par d'autre lettres. Par exemple, si e est un élément de E, $f(e)$ est l'image de e par f.
Soit l'application f de E vers F. A et B des sous ensembles respectivement de E et F, les ensembles $f(A)$ et $f^{-1}(B)$ définie par :

$$f(A) := \{f(a) \in F,\ a \in E\},\ f^{-1}(B) := \{a \in E,\ \exists b \in F,\ b = f(a)\} = \{x \in E,\ f(x) \in B\}$$

sont appelé respectivement l'image de A par f et l'image reciproque de B par f. En particulier le sous-ensemble $f(E)$ de F sera noté par $Im(f)$. Par définition, les sous-ensmbles $f(A)$ et $f^{-1}(B)$ sont respectivement des parties de F et E. Soient f une application de E vers F et g une application de F vers G. On définit l'application (ou composée) $g \circ f$ par :

$$g \circ f : E \mapsto G,\ x \mapsto g(f(x))$$

1.2.2 Proposition

Soit f une application de E vers F.

1. Soient A et B deux sous-ensembles de E, on a:

   (i) $A \subset B \Rightarrow f(A) \subset f(B)$;
   (ii) $f(A \cup B) = f(A) \cup f(B)$;
   (iii) $f(A \cap B) \subset f(A) \cap f(B)$;

2. Soient A et B deux sous-ensembles de E, on a:

   (i) $A \subset B \Rightarrow f^{-1}(A) \subset f^{-1}(B)$;
   (ii) $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$;
   (iii) $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$;
   (iv) $f^{-1}(B \backslash A) = f^{-1}(B) \backslash f^{-1}(A)$.

3. Soient $A \subset E$ et $B \subset F$. On a $A \subset f^{-1}f((A))$ et $f^{-1}(f(B)) = B \cap Im(f)$.

4. Soit g une application de F dans G. Si A et B sont respectivement les parties de E et F, on a :

   (i) $g \circ f(A) = g(f(A))$
   (ii) $(g \circ f)^{-1}(B) = g^{-1}(f^{-1}(B))$

1.2.3 Définition

Soit f une application de E dans F, on a :

1. f est injective ou une injection si toute élément de $Im\, f$ admet une antécedent, i.e pour tout e_1, e_2 tel que $f(e_1) = f(e_2)$, on a forcement $e_1 = e_2$.

2. f est surjective ou une surjection si $Im\, f = F$, i.e toute élément de F admet au moins un antécedent.

3. f est bijective ou une bijection si toute élément de F admet un unique antécedent, i.e si elle est à la fois injective et surjective.

1.2.4 Proposition

Soit f une application de E vers F. On a:

1. L'application f est injective si et seulement si pour tout A de E, $f^{-1}(f(A)) = A$.

2. L'application f est surjective si et seulement si pour tout B de F, $f(f^{-1}(B)) = B$.

3. Considérons une application g de F dans G, on a:

   (i) Si f et g sont injectives, alors $g \circ f$ est injective.
   (ii) Si f et g sont surjectives, alors $g \circ f$ est surjective.
   (iii) Si $g \circ f$ est injective, alors f est injective.
   (iv) Si $g \circ f$ est surjective, alors g est surjective.
   (v) Si $g \circ f$ est bijective, alors f est injective et g est surjective.

Soit E un ensemble. L'application Id_E de E dans E qui a toute élément x de E, on associe $Id_E(x) := x$ est appelée application identique de E.

1.2.5 Proposition

Soit f une application de E dans F. L'application f est bijective si et seulement s'il existe une application g de F dans E tel que $g \circ f = Id_E$ et $f \circ g = Id_F$. De plus, si f est un bijection, une telle application g est bijective et unique. Elle sera appelé l'application inverse de f. On le notera (par abus de notation) par f^{-1}.

1.2.6 Question

Soit f une application de E dans F. La condition d'existence d'une application g telle que $g \circ f = Id_E$ est elle suffisante pour que f soit bijective ? Si oui donner une preuve, sinon donner une contre exemple.

1.3 Dénombrabilité

Soit E un ensemble. On dit que E est un ensemble finie s'il possède un nombre finie d'élément. Si ce n'est pas le cas, on dit que est infini. Dans le cas où E est finie, on note le nombre d'élément de E par $\#E$ ou $card(E)$.

1.3.1 Proposition

Soient E et F deux ensembles finis:

1. Le nombre d'application de E dans F est $\#F^{\#E}$.
2. Soit f une application de E dans F:
   - (i) Si f est injective, on a $\#E \leq \#F$. Le nombre d'application injective de E dans F est $A_{\#F}^{\#E}$.
   - (ii) Si f est surjective, on a $\#F \leq \#E$.
   - (iii) Si f est bijective, on a $\#E = \#F$. Le nombre d'application bijective de E dans F est $(\#E)!$.
3. Il existe une application bijective de E dans F si et seulement si $\#E = \#F$.

Dans la suite, on notera par F^E l'ensemble des applications de E dans F.

1.3.2 Définition

Soit E un ensemble. On dit que E est dénombrable s'il existe une injection de E dans $\mathbb{N}$. Cela veut dire que l'on peut numeroter les éléments d'un ensemble.

1.3.3 Exemple

L'ensemble des entiers naturels $\mathbb{N}$ est dénombrable. En particulier, les éléments finis sont dénombrables.

1.3.4 Proposition

Soit E un ensemble dénombrable. L'ensemble E est infini si et seulement s'il existe une bijection entre E et $\mathbb{N}$.

1.3.5 Théorème (Cantor)

L'ensemble des nombres réels $\mathbb{R}$ n'est pas dénombrable. En particulier, l'ensemble des nombres irrationnels n'est pas dénombrable.

1.3.6 Corollaire

Un nombre réel est dit transcendant s'il n'est pas algèbrique. L'ensemble des nombres transcendant n'est pas dénombrable.
De maniere générale,

1.3.7 Définition

Soient E et F deux ensembles. On dit que E et F sont équipotents s'il existe une bijection entre E et F.

1.3.8 Exemple

- Deux ensembles E et F sont équipotents s'ils ont les même nombre d'éléments.
- Deux ensembles dénombrables infinis sont toujours équipotents.
- $\mathbb{Q}$ n'est pas équipotents à $\mathbb{R}$.

1.3.9 Proposition

Tout intervalle non reduit à un point est équipotent à $\mathbb{R}$.
Le resultat suivant permet la plus part du temps à montrer que deux ensembles sont équipotents.

1.3.10 Théorème (Cantor-Bernstein)

Soient E et F deux ensembles. Si E est équipotent à un sous ensemble de F et F est équipotent à un sous ensemble de E, alors E et f sont équipotents.

1.3.11 Théorème (Cantor)

Soit E un ensemble. Les ensembles E et $\mathcal{P}(E)$ ne sont pas équipotents.

1.4 Rélation binaire sur un ensemble

Jusqu'à maintenant on a globalement traité un ensemble par sa taille (sa cardinalite). On a quelques propriété pour pouvoir comparer deux ensembles. Dans cette section, on va régarder "plus à l'interieur" d'un ensemble.
On sait depuis plusieurs années que l'on peut comparer toutes les éléments des entiers naturels $\mathbb{N}$. Cela veut dire qu'il existe une "rélation" $(\leq)$ entre deux entiers quelconques. Avec cette rélation, on en déduit plus de propriété de l'ensemble $\mathbb{N}$. Ainsi, notre but ici est de généraliser, puis formaliser cette existence possible d'une rélation entre les éléments d'un ensemble. C'est le début de ce qu'on appelera *la structure algèbrique* d'un ensemble. Soient E et F deux ensembles.
Soient x et y deux éléments respectifs de E et F. Une correspondance entre x et$y$ est la rélation binaire $\mathcal{R}$ entre x et y que l'on notera $x\mathcal{R}y$. Autrement dit, une rélation binaire $\mathcal{R}$ entre E et F est définie par une partie $\mathcal{G}$ du produit cartesien $E \times F$ telle que :

$$\mathcal{G} := \{(x, y) \in E \times F : \ x\mathcal{R}y\}.$$

En particulier une rélation binaire $\mathcal{R}$ sur un enemble E est une partie $\mathcal{G}$ de $E \times E$ telle que :

$$\mathcal{G} := \{(x, y) \in E \times E : x\mathcal{R}y\}.$$

1.4.1 Exemple

1. L'inégalité $(\leq)$ est une rélation binaire sur l'ensemble $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ ou $\mathbb{R}$.
2. L'orthogonalité et la parrallelisme sont des rélations binaires sur les ensembles des droites de $\mathbb{R}^2$ ou $\mathbb{R}^3$.
3. L'inclusion $\subset$ est une rélation binaire sur l'ensemble des parties $\mathcal{P}(E)$ de l'ensemble E.
4. Le graphe d'une fonction numérique est une rélation binaire sur $\mathbb{R}$.

Voici quelques caractéristiques d'une rélation binaire sur un ensemble:

1.4.2 Définition

Soit E un ensemble et $\mathcal{T}$ un rélation binaire sur E. On dit que :

(i) $\mathcal{T}$ est reflexive si pour tout z élément de E , on a $z\mathcal{T}z$,

(ii) $\mathcal{T}$ est symetrique si pour tout a et b éléments de E tel que $a\mathcal{T}b$, on a $b\mathcal{T}a$,

(iii) $\mathcal{T}$ est transitive si pour tout x, y, z éléments de E tel que $x\mathcal{T}y$ et $y\mathcal{T}z$, on a $x\mathcal{T}z$,

(iv) $\mathcal{T}$ est antisymetrique si pour tout n et m éléments de E tel que $m\mathcal{T}n$ et $n\mathcal{T}m$, on a $m = n$.

Soit $\mathcal{R}$ une relation sur un ensemble E et $x \in E$. Le sous ensemble $Cl_{R_g}(x)(resp.\ Cl_{R_d}(x))$ est définie par :

$$Cl_{R_g}(x) := \{a \in E,\ x\mathcal{R}a\}\,(resp.\ Cl_{R_d}(x) := \{a \in E,\ a\mathcal{R}x\}).$$

est appelé le sous ensemble de classe a gauche (resp. le sous ensemble de la classe a droite) de l'élément de x.

1.4.3 Remarque

Si la rélation $\mathcal{R}$ est symetrique, on a $Cl_{R_g}(x) = Cl_{R_d}(x)$. Dans ce cas, on le note tout simplement par $Cl_R(x)$ ou par $\dot{x}$ ou par $\bar{x}$ et sera appelé la classe d'équivalence de l'élément x.

1.4.4 Relation d'equivalence

1.4.5 Définition

Une relation d'équivalence $\mathcal{R}$ sur un ensemble E est dite une rélation d'équivalence si elle est a la fois reflexive, symetrique, et transitive.

1.4.6 Exemples

1. L'égalité sur un ensemble est une relation d'équivalence ;
2. Le parallélisme est une relation d'équivalence sur l'ensemble des droites de R2 ou de R3 ;
3. Soit f une application de E vers F. Le sous ensemble de E^2 défini par :

$$\{(a, b) \in E^2 : f(a) = f(b)\}$$

définit une relation d'équivalence sur E.

1.4.7 Définition

Soit E un ensemble non vide. Une partition de E est une famille de sous-ensembles non vides de E, deux à deux disjoints, dont la réunion est égal à E.

1.4.8 Proposition

Soit F une relation d'équivalence sur un ensemble E. Si x et y deux éléments de E, on a:

1. $x \in Cl_{\mathcal{F}}(x)$;
2. $\dot{x} = \dot{y}$ si et seulement si $y \in \dot{x}$;
3. Si $y \notin \dot{x}$, on a $\dot{x} \cap \dot{y} = \emptyset$

1.5 Corollaire

Soit E un ensemble non vide. L'ensemble des classes d'équivalence de E forme une partition de E. Inversement, toute partition d'un ensemble définit une relation d'équivalence.

1.5.1 Définition

Soit $\mathcal{R}$ une relation d'équivalence sur un ensemble E. L'ensemble $E/\mathcal{R}$ des classes d'équivalences défini par :

$$E/\mathcal{R} := \{\dot{y} : y \in E\}$$

est appelé ensemble quotient de E par $\mathcal{R}$. Ainsi, on en déduit une application de E vers $E/\mathcal{R}$ qui a $x \in E$, on associe la classe $\dot{x}$. Cette application est appelé la projection (ou surjection) canonique de E dans $E/\mathcal{R}$.
En voici un exemple fondamental concernant les relations d'équivalences : Les congruences. Soit n un entier naturel non nul. Pour tout entier a et b, on dit que a est congruent à b modulo n s'il a le même reste que b après division euclidienne par n. Autrement dit, a est congruent à b modulo n si n divise $a - b$. Si c'est le cas on écrit :

$$a \equiv b \bmod n.$$

cette relation est dite la relation de congruence modulo n. Elle sera notée par $n\mathbb{Z}$.

1.5.2 Proposition

La relation binaire $n\mathbb{Z}$ est une relation d'équivalence sur $\mathbb{Z}$.

Soit a un entier. Par définition, la classe $\dot{a}$ est

$$\dot{a} := \{b \in \mathbb{Z} | a \equiv b \bmod n\} = a + n\mathbb{Z}$$

. Ainsi :

$$a \equiv b \bmod nsietseulementsi\dot{a} = \dot{b}.$$

Finalement, l'ensemble quotient $\mathbb{Z}/n\mathbb{Z}$ est définie par :

$$\mathbb{Z}/n\mathbb{Z} := \{\dot{a} | a \in \mathbb{Z}\}.$$

Comme les restes possibles après division euclidienne par n sont : $0, 1, 2, \cdots, n-1$, on conclut que :

$$\mathbb{Z}/n\mathbb{Z} = \bar{0}, \bar{1}, \bar{2}, \cdots, n \bar{-} 1.$$

Maintenant on va munir $\mathbb{Z}/n\mathbb{Z}$ de deux opérations binaires, à savoir l'addition et la multiplication, induites par celles de $\mathbb{Z}$. D'après les propriétés ci-dessus, on conclut qu'on a, pour tout $\dot{a}et\dot{b}$ dans $\mathbb{Z}/n\mathbb{Z}$:

- $\bar{a} + \bar{b} = \overline{a+b}$;
- $\bar{a} \cdot \bar{b} = \overline{ab}$.

S'il n'y a pas de confusion, on pourra omettre la barre sur les entiers. Mais, l'étudiant doit se souvenir toujours dans quel ensemble il travaille.

1.5.3 Exemples

Pour $n = 6$, on a les tables suivantes : Pour l'addition:

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Pour la multiplication :

×	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Soit a un entier. On dit que a est inversible dans $\mathbb{Z}/n\mathbb{Z}$ s'il existe un entier u tel que

$$\bar{u} \cdot \bar{a} = \bar{1}.$$

C'est à dire :

$$au \equiv 1 \bmod n.$$

Si c'est le cas, on dit que u est l'inverse de a dans $\mathbb{Z}/n\mathbb{Z}$. Noter bien que u est aussi inversible et que a est son inverse. L'ensemble des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ est noté par $(\mathbb{Z}/n\mathbb{Z})^\times$. D'après la table de multiplication ci-dessus, on a par exemple :

$$(\mathbb{Z}/6\mathbb{Z})^\times = 1, 5.$$

L'inverse de 1 est lui-même, de même pour 5.

1.5.4 Théorème

Soit a un entier. L'élément a de $\mathbb{Z}/n\mathbb{Z}$ est inversible si et seulement si a et n sont premiers entre eux. C'est à dire :

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{a \in \mathbb{Z}/n\mathbb{Z} | pgcd(a, n) = 1\}.$$

Ainsi, pour vérifier si un élément a est inversible dans $\mathbb{Z}/n\mathbb{Z}$, il suffit de calculer le pgcd de a et n. S'ils sont premiers entre eux, on conclut que a est inversible. Pour calculer l'inverse, on cherche un couple d'entier (u, v) tel que

$$au + nv = 1$$

en utilisant l'algorithme d'Euclide. Ainsi, l'inverse de a est u.

1.5.5 Relations d'ordre

1.5.6 Définition

Soit $\mathcal{R}$ une relation sur un ensemble E. On dit que $\mathcal{R}$ est une relation d'ordre si elle est à la fois réflexive, antisymétrique et transitive. Deux éléments x et y de l'ensemble E sont dits comparables si $x\mathcal{R}y$ ou $y\mathcal{R}x$. Si de plus tout les éléments de E sont deux à deux comparables, on dit que l'ordre est totale. Sinon, l'ordre est dit partiel.

1.5.7 Exemples

1. L'ordre usuelle $\leq$ sur $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ ou sur $\mathbb{R}$ est une relation d'ordre (Ordre total);
2. L'inclusion sur l'ensemble des parties $P(E)$ d'un ensemble E est une relation d'ordre (Ordre partiel) ;
3. La divisibilité sur l'ensemble des entiers $\mathbb{Z}$ est une relation d'ordre (Ordre partiel).

Noter bien que dans la plus part des cas, par abus, on notera une relation d'ordre par $\leq$. Soient $(E, \leq)$ un ensemble ordonné et A une partie de E :

- Un élément M de E est appelé un majorant de A si pour tout élément x de A, on a $x \leq M$;
- Un élément m de E est appelé un minorant de A si pour tout élément x de A, on a $m \leq x$;
- Un élément de A est appelé le plus grand élément de A s'il majore tous les éléments de A et est noté par $max(A)$;
- Un élément de A est appelé le plus petit élément de A s'il minore tous les éléments de A et est noté par $min(A)$;
- Si l'ensemble des majorants de A admet un plus grand élément, cet élément est appelé borne supérieure et est noté $sup(A)$;
- Si l'ensemble des majorants de A admet un plus grand élément, cet élément est appelé borne inférieure et est noté $inf(A)$.
- Si A admet une borne supérieure, on dit que la partie Aest majorée. Si A admet une borne inférieure, on dit que la partie A est minorée. Si de plus, elle est minorée et majorée, on dit que A est bornée.

1.5.8 Remarque

Si la partie A admet un maximum, elle admet une borne supérieure et on a $max(A) = sup(A)$. De même, si A admet un minimum, elle admet une borne inférieure et on a $min(A) = inf(A)$.