Université Paris 7
U3MI36

CHAPITRE 1

THÉORIE DES ENSEMBLES [1]

1.1 AXIOMES DE LA THÉORIE DES ENSEMBLES

On utilise la notion d'ensemble partout en mathématiques (algèbre, analyse, géométrie, probabilités) sans en donner une définition. Même chose pour par exemple la notion d'entier naturel. Ce chapitre se propose de donner une formalisation.

On va par exemple donner des règles pour répondre à la question " une collection donnée d'objets mathématiques est-elle un ensemble ? ".

Pour formaliser il nous faut un langage et une liste d'axiomes.

1.1.1 Le langage :

$$\{=, \in\} \cup \{\neg, \wedge, \vee, \Longrightarrow, \Leftrightarrow, \forall, \exists, (,)\} \cup \{x, y, z, \cdots\}$$

- $\in$ est un symbole de relation qui se lit " appartient ".
  $x \in y$ se lit " l'ensemble x appartient à l'ensemble y ".
- $\neg$, $\wedge$, $\vee$, $\Longrightarrow$, $\Leftrightarrow$ sont des **symboles de connecteur** qui se lisent repectivement, " non ", " et ", " ou ", " implique ", " équivalent à ".
- $\forall$, $\exists$ sont respectivement, le **quatificateur universel** qui se lit " quel que soit " ou " pour tout ", et le **quatificateur existentiel** qui se lit " il existe ".
- x, y, z, $\cdots$ sont des variables.

1.1.2 Les Axiomes :

Attention, à partir d'ici toutes les variables x, y, z, $\cdots$, a, b, $\cdots$, A, B, $\cdots$, sont des ensembles, et les éléments d'un ensemble sont des ensembles.

$\boldsymbol{A_1}$: L'axiome d'extensionalité.

Il dit que deux ensembles ayant les mêmes éléments sont égaux.

L'axiome A_1 : pour tout x, pour tout y (si (pour tout z ($z \in x$ ssi $z \in y$)) alors $x = y$).

[1] **Notes manuscrites de Catherine Muhlrad-Greif**

$$A_1 : \forall x\, \forall y \;\; ((\forall z\; (z \in x \Leftrightarrow z \in y)) \Longrightarrow x = y)$$

Remarque : Si on utilise l'abréviation $x \subset y$ pour $\forall z(z \in x \Longrightarrow z \in y)$ alors A_1 est équivalent à A'_1 : pour tout x, pour tout y ($(x \subset y \wedge y \subset x) \Longrightarrow x = y$).

$$A'_1 : \forall x\, \forall y \;\; ((x \subset y \wedge y \subset x) \Longrightarrow x = y)$$

$x \subset y$ se lit " x est inclus dans y " ou " x est un sous-ensemble de y " ou " x est une partie de y ".

***A*₂** : L'axiome de la paire.

A_2 : pour tout x, pour tout y, il existe z, pour tout u ($u \in z$ ssi ($u = x$ ou $u = y$)).

$$A_2 : \forall x\, \forall y\, \exists z\, \forall u\; (u \in z \Leftrightarrow (u = x \vee u = y)$$

On note $z = \{x, y\}$ ou $z = \{y, x\}$.

z contient x et y et c'est tout.

L'extentionalité garantit l'unicité de z.

Si $x = y$ alors $z = \{x, x\} = \{x\}$ par extention. z est alors un **singleton**. C'est un ensemble à un seul élément.

Remarques :

– En général, $x \notin x$ par exemple $\emptyset \notin \emptyset$.

– $x \in x$ n'est pas impossible.

***A*₃** : L'axiome de la réunion.

A_3 : pour tout x, il existe y, pour tout z ($z \in y$ ssi il existe t ($t \in x$ et $z \in t$)).

$$A_3 : \forall x\, \exists y\, \forall z\; (z \in y \Leftrightarrow \exists t\; (t \in x \wedge z \in t))$$

C-à-d : pour tout ensemble x, il existe un ensemble y dont les éléments sont les éléments des éléments de x.

L'extentionalité garantit l'unicité de y.

On note $\quad y = \bigcup x$.

Exemple : Réunion de deux ensembles.

Etant donné deux ensembles a et b, posons $c = \bigcup\{\,a,\, b\}$. On constate que les élément de c sont exactement ceux de a ou ceux de b.

On note $c = a \cup b$.

***A*₄** : L'axiome des parties.

A_4 : pour tout x, il existe y, pour tout z ($z \in y$ ssi $z \subset x$).

$$A_4 : \forall\, x\; \exists\, y\; \forall\, z\; (z \in y \Leftrightarrow z \subset x)$$

Les éléments de y sont les parties de x.

On note $y = \mathfrak{P}(x)$.

L'extentionalité garantit l'unicité de y.

Un élément de $\mathfrak{P}(x)$ est une partie de x.

A_5 : Le schéma d'axiome de compréhension.

Il s'agit en fait d'une infinité d'axiomes car pour chaque propriété $\mathcal{P}(x)$ " portant sur les ensembles " et pour tout ensemble x, l'axiome affirme qu'il existe un ensemble y dont les éléments sont les éléments de x qui ont la propriété $\mathcal{P}$.

$$A_5 : \forall\, x\; \exists\, y\; \forall\, z\; (z \in y \Leftrightarrow (z \in x \wedge \mathcal{P}(z)))$$

On note $y = \{\, z \in x\,;\; \mathcal{P}(z)\,\}$.

L'extentionalité garantit l'unicité de y.

Applications du schéma de compréhension

L'axiome A_5 est un trés grand fabriquant d'ensembles. Dans chaque cas l'axiome d'extensionalité assure l'unicité du nouvel ensemble.

Exemple 1 : L'ensemble vide.

Soit a un ensemble, on définit l'ensemble c par compréhension :

$$c = \{\, x \in a\,;\; \mathcal{P}(x)\,\} \quad \text{avec} \quad \mathcal{P}(x) = x \notin a$$

Alors $c = \{\, x \in a\,;\; x \notin a\,\}$.

Un tel ensemble c est unique par extentionalité et ne possède aucun élément.

Notation : $\emptyset$.

Exemple 2 : Intersection de deux ensembles.

Soit a et b deux ensembles, on définit c par compréhension :

$$c = \{ x \in a \,;\ x \in b \} \quad \text{ici } \mathcal{P}(x) = x \in b$$

On note $c = a \cap b$.

Les éléments de l'ensemble c sont exactement les éléments communs aux ensembles a et b.

Exemple 3 : L'ensemble de tous les ensemble n'existe pas.

Supposons qu'un tel ensemble de tous les ensemble existe et appelons le a.

Posons $b = \{ x \in a \,;\ x \notin x \}$.

b est un ensemble car il est défini par compréhension avec $\mathcal{P}(x) = x \notin x$.

Donc $b \in a$ (puisque tout ensemble est un élément de a).

Alors deux cas possibles :

- $b \in b$.

  Alors, en posant $x = b$ dans la définition de b, on aurait $b \in a$ et $b \notin b$. Contradiction.
- $b \notin b$.

  On sait déjà que $b \in a$. Alors $b \in a$ et $b \notin b$. Donc, par définition de b, on aurait $b \in b$. Contradiction.

1.2 DÉFINITION DES OBJETS ENSEMBLISTES USUELS

Remarques :

- Ne pas confondre $\subset$ et $\in$.
- $\emptyset \subset x$ est toujours vraie (vraie pour tout x).
- $\emptyset \in x$ est vrai ou faux selon x.

1.2.1 Couple ou paire ordonnée.

Définition : Etant donné deux ensembles a et b, on appelle " **couple** dont le premier élément est a et le deuxième élément est b ", l'ensemble $\{ \{ a \} , \{ a, b \} \}$ que l'on note (a, b).

Justification : l'axiome de la paire appliqué trois fois justifie l'existence du couple (a, b).

Cette définition du couple n'est pas la seule possible. Toute autre définition est acceptable du moment qu'elle permet de démontrer le théorème suivant.

Théorème : Si $(a, b) = (a', b')$ alors $a = a'$ et $b = b'$.

Théorème : Si a, b sont des éléments d'un ensemble E alors $\{\, a,\ b\,\} \in \mathfrak{P}(E)$ et $(a, b) \in \mathfrak{P}\mathfrak{P}(E)$.

1.2.2 Produit de deux ensembles.

Définition : Etant donné deux ensembles A et B, il existe un ensemble E dont les éléments sont tous les couples (x, y) où $x \in A$ et $y \in B$.
On note $E = A \times B$.

Justification : L'existence de l'ensemble $A \times B$ est justifié par l'instance suivante du schéma d'axiome de compréhension.

$A \times B = \{\, z \in \mathfrak{P}\mathfrak{P}(A \cup B)\,;\ \mathcal{P}(z)\,\}$

où $\mathcal{P}(z) =$ " il existe $x \in A$, il existe $y \in B$, $(x, y) = z$".

L'unicité de $A \times B$ est assurée par l'extensionalité.

Notations :

- L'ensemble $A \times (B \times C)$ est noté $A \times B \times C$ et ses éléments sont appelés **triplets**.
- Un triplet $(x, (y, z))$ de $A \times B \times C$ est noté (x, y, z).
- L'ensemble $A_1 \times \cdots \times (A_{n-1} \times A_n)$ est noté $A_1 \times \cdots \times A_{n-1} \times A_n$ et ses éléments sont appelés n**-uplets**.
- Un n-uplet $(x_1, \cdots, (x_{n-1}, x_n))$ de $A_1 \times \cdots \times A_{n-1} \times A_n$ est noté $(x_1, x_2, x_3 \cdots, x_n)$.
- $\underbrace{E \times E \times E \cdots \times E}_{n \text{ fois}} = E^n$.

1.2.3 Relation binaire.

Définition : Une relation binaire R sur un ensemble E est (la donnée d') un sous-ensemble de $E \times E$.

Une relation relation *n-aire* sur un ensemble E est (la donnée d') un sous-ensemble de E^n.

On note $(x, y) \in R$ ou xRy ou Rxy ou $R(x, y)$.

R binaire est donc un ensemble de couple.

On peut voir l'égalité sur E comme une relation binaire sur E.

Une relation binaire sur E est dite
- Réfléxive : pour tout $x \in E$, $(x,x) \in R$.
- Symétrique : pour tout $x \in E$, pour tout $y \in E$, si $(x,y) \in R$ alors $(y,x) \in R$.
- Anti-symétrique : pour tout $x \in E$, pour tout $y \in E$, $(xRy \ \wedge \ yRx) \Longrightarrow x = y$.
- Transitive : pour tout $x \in E$, pour tout $y \in E$, pour tout $z \in E$, $(xRy \ \wedge \ yRz) \Longrightarrow xRz$.

Définition : Une relation d'équivalence sur E est une relation binaire sur E qui est réflexive, symétrique et transitive.

Définition : Une relation d'ordre sur E est une relation binaire sur E qui est réflexive, anti-symétrique et transitive.

Etant donné un ensemble E non vide, il existe une unique relation binaire sur E qui soit à la fois relation d'équivalence et relation d'ordre : c'est l'égalité sur E.

1.2.4 Fonction - Applications.

A et B sont deux ensembles.

Définitions : Une application de l'ensemble A dans l'ensemble B, on dit aussi une fonction de domaine A à valeurs dans B, est un sous-ensemble f de $A \times B$ tels que pour tout élément x de A, il existe un unique élément y de B tel que $(x,y) \in f$.

Une fonction f de A dans B est une application f d'une partie D de A dans B. D est appelé **domaine** de f et noté $Domf$.

Notation : On écrit $f(x) = y$ au lieu de $(x,y) \in f$.

$f : A \rightarrow B$ signifie que f est une application de A dans B.

L'image d'une fonction f de A dans B, notée Imf, est l'ensemble $\{\, y \in B \,;\ \text{il existe } x \in A \text{ tel que } \ f(x) = y \,\}$.

Définitions :
- $(\forall\, x \in A)\ D(x)$ est une abréviation de $\forall\, x\ (x \in A \Longrightarrow D(x))$.
- $(\exists\, x \in A)\ D(x)$ est une abréviation de $\exists\, x\ (x \in A \wedge D(x))$.
- $(\exists\, !\, x \in A) D(x)$ est une abréviation de $(\exists\, x\ ((x \in A \wedge D(x))) \wedge \neg((\exists\, x' \in A)\ (x \neq x' \wedge D(x')))$ [2].

[2] $(\exists\, !\, x \in A) D(x)$ est synonyme de "(il existe un unique $x \in A$) D(x) ".

Etant donné deux ensembles A et B il existe un ensemble C de toutes les applications de A dans B.

$$C = \{\, f \in \mathfrak{P}(A\times B)\,;\ \text{pour tout } x \in A \text{ il existe un unique } y \in B \text{ tels que } (x,y) \in f \,\}$$

C est noté B^A ou $\mathcal{F}(A, B)$.

Justification : C est obtenu par application de la compréhension avec la propriété $\mathcal{P}(f) = (\forall\, x \in A)\ (\exists\,!\, y \in B)\ ((x, y) \in f)$.

L'application $f : A \to A$ définie par $f = \{(x, x)\,;\ x \in A\}$ [3] est appelée l'identité dans A.

Remarques :
– Si α est faux alors $(\alpha \Longrightarrow \beta)$ est vrai.
– Si α est vrai et β est faux alors $(\alpha \Longrightarrow \beta)$ est faux.

Remarque : Etude de B^A pour $A = \emptyset$ ou $B = \emptyset$

1) $A = \emptyset$, alors $A \times B = \emptyset$. L'ensemble vide est alors le seul sous-ensemble de $A \times B$.

   $\emptyset$ est-il une application de $\emptyset$ dans B ?

   A-t-on : $(\forall\, x \in \emptyset)\, (\exists\,!\, y \in B)\ ((x, y) \in \emptyset)$?

   c-à-d a-t-on : $\forall\, x\ (x \in \emptyset \Longrightarrow (\exists\,!\, y \in B)\ ((x, y) \in \emptyset)\,)$?

   Oui car $x \in \emptyset$ est faux (quel que soit x).

   Donc si $A = \emptyset$, $B^A = \{\, \emptyset \,\}$.

2) $A \neq \emptyset$ et $B = \emptyset$. Alors $A \times B = \emptyset$ et, à nouveau $\emptyset$ est le seul candidat à être une application de A dans B.

   $\emptyset$ est-il une application de A $(\neq \emptyset)$ dans $\emptyset$?

   A-t-on : $(\forall\, x \in A)\, (\exists\,!\, y \in \emptyset)\ ((x, y) \in \emptyset)$?

   c-à-d a-t-on : $\forall\, x\ (x \in A \Longrightarrow (\exists\,!\, y \in \emptyset)\ ((x, y) \in \emptyset)\,)$?

   Non car pour un x dans A, $x \in A$ est vrai et $(\exists\,!\, y \in \emptyset)\ (\cdots)\,)$ est faux [4].

   Donc si $A \neq \emptyset$, $B^A = \emptyset$.

---

[3] $f = \{(x, y) \in A^2\,;\ x = y\}$

[4] $(\exists\,!\, y \in \emptyset)\ (\cdots)\,) = (((\exists\, y \in \emptyset)\ (\cdots)\,))\wedge \cdots)$, or $(\exists\, y \in \emptyset)\ (\cdots)\,)$ est faux.

Définitions usuelles : application injective, surjective, bijective, composition, extension aux parties.

Soit $f \in B^A$.

- f injective : pour tout $x \in A$, pour tout $x' \in A$, si $f(x) = f(x')$ alors $x = x'$.
- f surjective : pour tout $y \in B$, il existe $x \in A$ tel que $f(x) = y$.
- f bijective si f est injective et surjective.
- Inverse f^{-1} : si f est bijective, on peut définir $f^{-1} : B \to A$ l'application inverse de f

  $$f^{-1} = \{ (y, x) \in B \times A\,;\ (x, y) \in f \}$$
- Composition : Soient f et g deux applications, $f : A \to B$ et $g : B \to C$.

  Posons $\varphi = \{ (x, z) \in A \times C\,;\ \text{il existe } y \in B,\ (x, y) \in f \text{ et } (y, z) \in g \}$.

  φ est un sous-ensemble de $A \times C$ (par compréhension) et c'est une application de A dans C, car pour tout x dans A, il existe un unique $z \in C$ tel que $(x, z) \in \varphi$, c'est $z = g(f(x))$.

  Notation : $\varphi = g \circ f$.

  Théorème : La composition des applications est associative, c-à-d , soient trois applications $f : A \to B$, $g : B \to C$ et $h : C \to D$ on a :

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

  Notation : $h \circ (g \circ f) = h \circ g \circ f$.
- Extension de f aux sous-ensembles : Soit $f : A \to B$ une application, pas forcement bijective. On associe à f les application $f^{\rightarrow}$ et $f^{\leftarrow}$ ainsi définies :

  $f^{\rightarrow} : \mathfrak{P}(A) \to \mathfrak{P}(B)$ et pour tout $X \in \mathfrak{P}(A)$ $\ f^{\rightarrow}(X) = \{ f(x)\,;\ x \in X \}$ [5].

  $f^{\leftarrow} : \mathfrak{P}(B) \to \mathfrak{P}(A)$ et pour tout $Y \in \mathfrak{P}(B)$ $\ f^{\leftarrow}(Y) = \{ x \in A\,;\ f(x) \in Y \}$.

1.2.5 Familles d'ensembles

[5] $f^{\rightarrow}(X) = \{ y \in B\,;\ \text{il existe } x \in X \text{ tel que } f(x) = y \}$

1) Famille d'ensembles.

Etant donné un ensemble I, une application f de domaine I est aussi appelée famille d'ensembles indexée par I

On la note $(a_i)_{i\in I}$ où $a_i = f(i)$.

Cas particulier (fréquent). f est l'identité sur I, $f(i) = i$. On dit que la famille est associée à l'ensemble I et elle est notée $(i)_{i\in I}$.

L'ensemble d'indices I peut être infini la famille est alors dite infinie.

Si $I = \emptyset$ alors $f = \emptyset$ et on dit que la famille est vide.

Si $I \neq \emptyset$ on dit que la famille est non vide.

2) Réunion d'une famille d'ensembles.

C'est la réunion des éléments de l'image de f.

On la note $\bigcup\limits_{i\in I} a_i$. On a donc

$$\bigcup_{i\in I} a_i = \bigcup Im\, f$$

Remarques : $\forall\, i \in I \;\; a_i \subset \bigcup\limits_{i\in I} a_i$.

Cas particuliers :

- $\bigcup\limits_{x\in a} x$ est la réunion de la famille $(x)_{x\in a}$ associée à a.
- Si $I = \emptyset$, on a obligatoirement $f = \emptyset$, donc $Im\, f = \emptyset$, donc $\bigcup Im\, f = \emptyset$. Il n'existe donc qu'une seule famille indexée par $\emptyset$ et sa réunion est vide.

3) Intersection d'une famille d'ensembles.

Soit $(a_i)_{i\in I}$ une famille d'ensembles et supposons $I \neq \emptyset$. Soit $i_0 \in I$. Définissons par compréhension un ensemble C :

$$C = \{\, x \in a_{i_0} \,;\; \text{pour tout } i \in I, x \in a_i \,\}$$

On voit qu'un ensemble x est un élément de C ssi pour tout $i \in I$, x est un élément de a_i.

Si $i_1 \in I$, il est clair que

$$\{\, x \in a_{i_0} \,;\; \text{pour tout } i \in I, x \in a_i \,\} = \{\, x \in a_{i_1} \,;\; \text{pour tout } i \in I, x \in a_i \,\}.$$

Ceci justifie que l'ensemble C soit considéré comme l'intersection de tous les a_i de la famille.

On note $C = \bigcap_{i \in I} a_i$.

Cas particulier : $\bigcap_{x \in a} x$ est l'intersection de la famille ($(x)_{x \in a}$) associée à a.

4) Produit d'une famille d'ensembles.

Il existe un ensemble C dont les éléments sont les applications φ de domaine I à valeurs dans $\bigcup_{i \in I} a_i$ et tels que pour tout $i \in I$, $\varphi(i) \in a_i$.

Preuve : $C = \{ \varphi \in \bigcup_{i \in I} a_i{}^I \,;\ \varphi(i) \in a_i$ pour tout $i \in I \}$.

C existe par compréhension et est unique par extensionalité.

On note : $C = \prod_{i \in I} a_i$.

Si l'un des a_i est vide alors $\prod_{i \in I} a_i = \emptyset$.

Si $I = \emptyset$ alors $\prod_{i \in I} a_i = \{\emptyset\}$.

L'axiome du choix : Le produit d'une famille non vide d'ensembles non vides est non vide.

1.3 $\mathbb{N}$ l'ensemble des entiers naturels

1.3.1 $\mathcal{Z}$ la théorie des ensembles de $\mathcal{Z}ermelo$.

$$\mathcal{Z} \left\{ \begin{array}{l} - \text{ extensionnalité} \\ - \text{ paire} \\ - \text{ union} \\ - \text{ parties} \\ - \text{ schéma d'axiome de compréhension} \\ - \text{ axiome de l'infini} \end{array} \right.$$

L'axiome de l'infini :

$$\exists\, a \ (\ \emptyset \in a \ \text{ et } \ \forall\, x \ (\text{ si } x \in a \text{ alors } x \cup \{x\} \in a \ )\ )$$ [6]

[6] $\exists\, a\ (\ \emptyset \in a\ \wedge\ \forall\, x\ (x \in a \Longrightarrow x \cup \{x\} \in a\ )\ )$

Autrement dit : il existe un ensemble a tel que

$$\begin{array}{ll} (1) & \emptyset \in a \\ (2) & \text{pour tout } x, \ \text{si } x \in a \text{ alors } x \cup \{x\} \in a \end{array}$$

Voici quelques ensembles qui sont dans a :

$\emptyset, \quad \emptyset \cup \{\emptyset\} = \{\emptyset\},$

$\{\emptyset\} \cup \{\{\emptyset\}\} = \{\emptyset, \ \{\emptyset\}\}$

$\{\emptyset, \ \{\emptyset\}\} \cup \{\{\emptyset, \ \{\emptyset\}\}\} = \{\emptyset, \ \{\emptyset\}, \ \{\emptyset, \ \{\emptyset\}\}\} \ \cdots$

Ces ensembles sont éléments de tout ensemble a qui vérifie l'axiome de l'infini.

1.3.2 Définition de $\mathbb{N}$.

Théorème et définition : Il existe un unique ensemble $\mathbb{N}$ qui satisfait les conditions (1) et (2) et qui est inclus dans tout ensemble X satisfaisant ces mêmes conditions.

Les éléments de $\mathbb{N}$ sont appelés des entiers.

Preuve :
– Unicité. Triviale.

– Existence. Soit A un ensemble qui satisfait (1) et (2) .
(Il en existe d'après l'axiome de l'infini.)
Considérons l'ensemble $\mathcal{Y}$ des sous-ensembles de A qui satisfont (1) et (2).
Considérons la famille associée à l'ensemble $\mathcal{Y}$ (c-à-d la famille indexée par $\mathcal{Y}$ et correspondant à l'identité dans $\mathcal{Y}$).
Notons N_A l'intersection de cette famille :

$$N_A = \bigcap_{X \in \mathcal{Y}} X.$$

Cette intersection existe puisque $\mathcal{Y}$ n'est pas vide [7].

Rappelons que par définition de l'intersection d'une famille d'ensembles, les éléments de l'ensemble N_A sont exactement les éléments communs à tous les ensembles X de $\mathcal{Y}$.

Remarquons que pour tout $X \in \mathcal{Y}$, $N_A = \bigcap_{X \in \mathcal{Y}} X \subset X$, donc $N_A \subset X$.

[7] $A \in \mathcal{Y}$.

- Montrons que N_A vérifie (1) et (2).

  (1) L'ensemble $\emptyset$ appartient à tous les éléments de X de $\mathcal{Y}$ [8], donc l'ensemble $\emptyset$ est un élément de N_A.

  (2) Soit $x_0 \in N_A$, alors pour tout $X \in \mathcal{Y}$, $x_0 \in X$, et comme X vérifie la condition (2), $x_0 \cup \{x_0\} \in X$. Donc pour tout $X \in \mathcal{Y}$, $x_0 \cup \{x_0\} \in X$ et ainsi $x_0 \cup \{x_0\} \in N_A$.

- Montrons que N_A est inclus dans tout ensemble B vérifiant les conditions (1) et (2).

  Soit un ensemble B vérifiant les conditions (1) et (2), il est clair que $A \cap B$ vérifie aussi (1) et (2) et que $A \cap B \subset A$.
  Donc $A \cap B \in Y$, ainsi $N_A \subset A \cap B$ [9], d'où $N_A \subset B$.

Corollaire 1 : Le principe d'induction.

Si un ensemble W possède les propriétés (1) et (2) c-à-d si

$$\begin{array}{ll} (1) & \emptyset \in W \\ (2) & \text{pour tout } x, \text{ si } x \in W \text{ alors } x \cup \{x\} \in W \end{array}$$

alors $\mathbb{N} \subset W$.

Preuve : Trivial.

Quelques éléments de $\mathbb{N}$:

$\emptyset, \quad \emptyset \cup \{\emptyset\} = \{\emptyset\},$

$\{\emptyset\} \cup \{\{\emptyset\}\} = \{\emptyset, \{\emptyset\}\}$

$\{\emptyset, \{\emptyset\}\} \cup \{\{\emptyset, \{\emptyset\}\}\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} \cdots$

Notation :

$\emptyset = 0, \ \{\emptyset\} = 1, \ \{\emptyset, \{\emptyset\}\} = 2, \ \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} = 3, \cdots.$

Si n est un élément de $\mathbb{N}$, on note l'entier $n \cup \{n\} = n^+$.

Le principe d'induction reflète la construction de $\mathbb{N}$. C'est l'outil priviligié pour les démonstrations sur les entiers.

Corollaire 2 : Le principe d'induction appliqué à une propriété $P(x)$.

[8] Si $X \in \mathcal{Y}$ alors X vérifie (1) qui dit que l'ensemble $\emptyset$ appartient$X$.
[9] On rappelle que, pour tout $X \in \mathcal{Y}$, $N_A \subset X$.

Soit P une propriété définie, au moins, sur les entiers. Si

(1) $P(0)$ est vrai et si
(2) pour tout $x \in \mathbb{N}$, si $P(x)$ est vrai alors $P(x^+)$ est vrai

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

Preuve : On considère l'ensemble $W = \{x \in \mathbb{N}\,;\ P(x)\}$ et on lui applique le corollaire précédent.

Dans le cadre des entiers munis de l'ordre le principe d'induction s'appelle principe de récurrence.

1.3.2 Propriétés de $\mathbb{N}$ - L'ordre usuel sur $\mathbb{N}$.

L'ensemble $\mathbb{N}$ possède les propriétés suivantes (et beaucoup d'autres !) :

1) Tous les éléments d'un entier sont des entiers.

2) Si n est un entier et si $m \in n$ alors $m \subset n$.

3) Si n est un entier, $n \notin n$.

4) Si m, n sont des entiers, et $m \subset n$, alors $m = n$ ou bien $m \in n$.

Preuve :

1) Par induction. La propriété concernée est

$$P(x) : \text{pour tout } m \text{ (si } m \in x \text{ alors } m \in \mathbb{N})$$

(1) $P(0)$ est vraie car 0 n'a pas d'élément.

(2) Soit $n \in \mathbb{N}$ et supposons $P(n)$ vraie. Considérons $n^+ = n \cup \{n\}$.

Les éléments de n^+ sont les éléments de n qui sont des entiers puisque $P(n)$ est vraie, et n qui est un entier. Donc tous les éléments de n^+ sont des entiers et ainsi $P(n^+)$ est vraie.

D'où, d'après Corollaire 2, pour tout $n \in \mathbb{N}$ on a $P(n)$.

2) Par induction. La propriété concernée est

$$P(x) : \text{pour tout } m \text{ (si } m \in x \text{ alors } m \subset x)$$

(1) $P(0)$ est vraie car 0 n'a pas d'élément.

(2) Soit $n \in \mathbb{N}$ et supposons $P(n)$ vraie. Considérons $n^+ = n \cup \{n\}$.

Soit $m \in n^+$. Alors ou bien $m \in n$, et donc $m \subset n$ par hypothèse d'induction, donc $m \subset n \cup \{n\}$, ou bien $m = n$, donc $m \subset n \cup \{n\}$.

Donc : pour tout m, si $m \in n^+$ alors $m \subset n^+$. D'où $P(n^+)$ est vrai et d'après Corollaire 2, pour tout $n \in \mathbb{N}$ on a $P(n)$.

3) Par induction. La propriété concernée est

$$P(x) : x \notin x.$$

C'est évident si $n = 0$ (n n'a pas d'élément). Supposons que $n \notin n$, et que $n \cup \{n\} \in n \cup \{n\}$. On a alors ou bien $n \cup \{n\} = n$, ou bien $n \cup \{n\} \in n$. Dans le premier cas on a $n \in n$ ce qui conterdit l'hypothèse. Dans le second, on a $n \cup \{n\} \subset n$ (propriété 2)). Or $n \in n \cup \{n\}$, donc $n \in n$ contrairement à l'hypothèse

<u>***Exo n^o* 1**</u> **:** :

a) Tout élément $n \neq 0$ de $\mathbb{N}$ a un prédécesseur (c'est-à-dire un entier m tel que $m^+ = n$).
b) Pour tout entier n, si $p^+ = n$ alors p est un entier et $p < n$.

Preuve :

a) Soient $B = \{n \in \mathbb{N} ;$ il existe $m \in \mathbb{N}$ tel que $m^+ = n\}$ et $A = B \cup \{0\}$. Alors $0 \in A$; si $x \in A$, on a évidement $x^+ \in B$ (par déf de B), donc $x^+ \in A$. Donc, par induction, $\mathbb{N} \subset A$; cela veut dire que tout entier $\neq 0$ a un prédécesseur ($\in B$).

b) Si $p^+ = n$ alors $p \in n$. D'après la propriété 1) ci-dessus p est un entier, d'après la propriété 2) ci-dessus $p \subset n$, et d'après la propriété 3) ci-dessus $p \notin p$ et donc $p \neq p^+$, d'où $p < n$ (voir déf de $<$ dans $\mathbb{N}$ chap 1 page 14).

Définition de l'ordre usuel dans $\mathbb{N}$.

Définition : Soient m et n deux entiers. On pose $m \leq n$ si $m \subset n$

Théorème : $\leq$ est une relation d'ordre total sur les entiers.

c-à-d $\leq$ est réflexive, antisymétrique et transitive et $\leq$ est totale : soient m et n deux entiers, on a $m \leq n$ ou $n \leq m$.

Preuve : Induction.

Théorème : Tout ensemble d'entiers qui est non vide possède un plus petit élément pour l'ordre $\leq$.

Preuve : Soit X un sous-ensemble de $\mathbb{N}$, non vide, et supposons qu'il n'a pas de plus petit élément. On applique le principe d'induction à la propriété

$$P(n) = \text{"}n \text{ est un entier et aucun entier } m \leq n \text{ n'est élément de } X\text{"}$$

et on montre que $(\forall\, n \in \mathbb{N})\ P(n)$. Cela implique que X est vide contrairement à l'hypothèse faite.

Dans la preuve du Th suivant on utilise la propriété suivante qu'on admettra :

Pour tous entiers n et p, si $n^+ = p^+$ alors $n = p$.

Théorème : Définition d'une fonction par induction (récurrence) sur les entiers.

Soit E un ensemble non vide. Soit $a \in E$ et soit H une application de $\mathbb{N} \times E$ dans E. Il existe une unique application de $\mathbb{N}$ dans E telle que

$$f(0) = a \quad \text{et } f(n^+) = H(n, f(n))$$

pour tout entier n.

Preuve :

- Unicité : Considérons f et g ayant ces propriétés.

  Si $f \neq g$, l'ensemble $\{n \in \mathbb{N};\ f(n) \neq g(n)\}$ est non vide, donc a un plus petit élément m ; $m \neq 0$ car $f(0) = g(0) = a$. Donc (d'après l'exo 1 a)) m admet un prédécesseur p ($< m$ voir exo 1 b)) ; on a $f(p) = g(p)$, donc $H(p, f(p)) = H(p, g(p))$ soit $f(p^+) = g(p^+)$, c'est-à-dire $f(m) = g(m)$, ce qui contredit la définition de m.

- Existence : On considère les sous-ensembles M de $\mathbb{N} \times E$ qui ont les propriétés

  $$(0, a) \in M \ ; \qquad \text{si } (n, y) \in M \text{ alors } \quad (n^+, H(n, y)) \in M \quad (*)$$

  Il est clair que l'intersection M_0 de tous ces sous-ensembles M de $\mathbb{N} \times E$ a encore ces propriétés. C'est donc le plus petit sous-ensemble de $\mathbb{N} \times E$ qui a ces propriétés. On va en déduire que c'est (le graphe d') une application de $\mathbb{N}$ dans E.

  Pour tout entier n, il existe $y \in E$ tel que $(n, y) \in M_0$: c'est vrai pour $n = 0$, puisque $(0, a) \in M_0$; si c'est vrai pour n, c'est vrai pour n^+ d'après la deuxième propriété satisfaite par M_0.

  Pour tout entier n, si $(n, y) \in M_0$ et $(n, z) \in M_0$, alors $y = z$; on raisonne par l'absurde, et on considère le premier m tel qu'il existe $y, z \in E$, $y \neq z$, $(m, y) \in M_0$ et $(m, z) \in M_0$.

Si $m = 0$, on a par exemple $y \neq a$; soit M_0' l'ensemble obtenu en otant $(0, y)$ de M_0 ($M_0' = M_0 - \{(0, y)\}$). Alors M_0' a les deux propriétés ci-dessus (*), et est strictement inclus dans M_0, ce qui conterdit la définition de M_0.

On a donc $m \neq 0$, et par suite m a un prédécesseur p ($m = p^+$ et $p < m$). D'après la définition de m, il existe un élément t et un seul de E tel que $(p, t) \in M_0$; alors $(p^+, H(p, t)) \in M_0$ et on a, par exemple $y \neq H(p, t)$.

On pose $M_0' = M_0 - \{(m, y)\} = M_0 - \{(p^+, y)\}$. Alors M_0' a les deux propriétés ci-dessus (*) : car $(0, a) \in M_0$ et $(0, a) \neq (m, y)$, donc $(0, a) \in M_0'$.

Si $(n, u) \in M_0'$ alors $(n^+, H(n, u)) \in M_0$ et $(n^+, H(n, u)) \neq (m, y)$: c'est évident si $n^+ \neq m$, et si $n^+ = m$ alors $n = p$ [10], donc $u = t$ [11] et $y \neq H(p, t)$. Donc $(n^+, H(n, u)) \in M_0'$.

Comme M_0' est strictement inclus dans M_0, on a donc contredit la définition de M_0.

M_0 est donc (le graphe d') une application de $\mathbb{N}$ dans E et on a bien

$$f(0) = a \quad \text{et } f(n^+) = H(n, f(n))$$

pour tout entier n.

Quand on utilise la notation de l'ordre usuel sur les entiers, on parle de récurrence plutôt que d'induction.

1.3.3 Principe de récurrence sur les entiers sous trois formes :

$P(x)$ est une propriété définie sur $\mathbb{N}$.

$p < q$ ssi $p \leq q$ et $p \neq q$.

(I) Si $P(0)$ et $\forall n \in \mathbb{N}$ ($P(n) \Longrightarrow P(n+1)$), alors $\forall n \in \mathbb{N}$ $P(n)$.

(I') Soit a un entier. Si $P(a)$ et ($\forall n \in \mathbb{N}$ et $n \geq a$) ($P(n) \Longrightarrow P(n+1)$) alors ($\forall n \in \mathbb{N}$ et $n \geq a$) $P(n)$.

(II) Si $\forall p \in \mathbb{N}$ ((($\forall n \in \mathbb{N}$ et $n < p$) $P(n)$)$\Longrightarrow P(p)$) alors $\forall n \in \mathbb{N}$ $P(n)$.

(III) Pour tout sous-ensemble X de $\mathbb{N}$, si X est non vide alors X possède un plus petit élément au sens de l'ordre $\leq$.

[10] Pour tous entiers n et p, si $n^+ = p^+$ alors $n = p$.
[11] t est le seul élément de E tel que $(p, t) \in M_0$. Or $(n, u) \in M_0' \subset M_0$ et $n = p$.