1.1.5 Quantificateurs et prédicats

En mathématiques, on utilise, souvent, des expressions de la forme : "pour tout ...", "quelque soit ...", "il existe au moins ...", "il existe un, et un seul ...", ... Ces expressions précisent comment les éléments d'un ensemble peuvent vérifier une certaine propriété. Ces expressions sont appelées des quantificateurs.
On distingue deux types de quantificateurs :

- Le quantificateur universel, noté $\forall$, se lit "quel que soit", "pour tout",....
- Le quantificateur existentiel, noté $\exists$, se lit "il existe". La notation $\exists!$ signifie "il existe un, et un seul".

Exemple 1.1.19. *Soit $E = \{n \in \mathbb{N}/n > 2\}$. L'assertion : "Pour tout x élément de E, x est supérieur strictement à 2" peut être représentée par :*

$$\forall x \in E, x > 2 \text{ ou par}$$
$$\forall x \in E, P(x), \text{ avec } P(x) \text{ est l'expression "}x \text{ est supérieur strictement à 2".}$$

L'assertion : $\forall x \in E, x > 2$ est une assertion vraie ; cependant, l'assertion : $\exists x \in E : x \leq 2$ est une assertion fausse.

Dans l'exemple précédent, l'expression "$x > 2$" est formée de deux parties : x qui est le sujet et la deuxième partie est "> 2, i.e., la propriété que le sujet x peut vérifié ; cette expression est appelée un **prédicat**.

Exemples 1.1.20.

1. *Soit $P(x)$ l'expression $x > 4$. $P(5)$ est l'assertion $5 > 4$ qui est vraie tandis que $P(3)$ est l'assertion fausse : $3 > 4$.*
2. *Soit $P(x, , y, z)$ l'expression $z = x + y$, alors $P(1, 3, 4)$ est l'assertion : $4 = 1 + 3$.*

Remarque 1.1.21. *$P(x)$ n'est pas une assertion ; cependant en attribuant une valeur à x, on obtient une assertion.*

Proposition 1.1.22. *Soit E un ensemble, P et Q des prédicats. Alors, on a les équivalences suivantes :*

1. $[\neg(\forall x \in E, P(x))] \Leftrightarrow \exists x \in E, \neg(P(x))$.
2. $[\neg(\exists x \in E, P(x))] \Leftrightarrow \forall x \in E, \neg(P(x))$.
3. $[\forall x \in E, (P(X) \wedge Q(x)] \Leftrightarrow [(\forall x \in E, P(x)) \wedge (\forall x \in E, Q(x))]$.
4. $[\exists x \in E, (P(X) \vee Q(x))] \Leftrightarrow [(\exists x \in E, P(x)) \vee (\exists x \in E, Q(x))]$.

Exemple 1.1.23. *Soit $(u_n)_{n\in\mathbb{N}}$ une suite réelle.*

- (u_n) *est convergente* $\Leftrightarrow (\exists l \in \mathbb{R})$ *tel que* $(\forall \epsilon > 0), (\exists N \in \mathbb{N}) : (\forall n \in \mathbb{N})$
$$n \geq N \Rightarrow |u_n - l| \leq \epsilon.$$
- (u_n) *est divergente* $\Leftrightarrow (\forall l \in \mathbb{R}), (\exists \epsilon > 0) : (\forall N \in \mathbb{N})(\exists n \in \mathbb{N})$
$$n \geq N \textbf{ et } |u_n - l| > \epsilon.$$

Remarques 1.1.24.

1. *L'ordre des quantificateurs dans une assertion est très important. Par exemple, l'assertion : $\forall x \in \mathbb{R}^\star, \exists y \in \mathbb{R}^\star : xy = 1$ est vraie tandis que l'assertion : $\exists y \in \mathbb{R}^\star : \forall x \in \mathbb{R}^\star, xy = 1$ est fausse.*
2. *Dans un prédicat $P(x)$, la lettre x est une variable muette ; on peut la remplacer par n'importe quelle autre lettre à condition qu'elle ne soit pas utilisée, auparavant, pour désigner un autre objet.*

Propriétés 2.1.8. *on a :*

- $E \cap F \subset E$ *et* $E \cap F \subset F$.
- $E \subset E \cup F$ *et* $F \subset E \cup F$.
- $E \cap F = F \cap E$ *(commutativité de l'intersection).*
- $E \cup F = F \cup E$ *(commutativité de la réunion).*
- $E \cap (F \cap G) = (E \cap F) \cap G$ *(associativité de l'intersection).*
- $E \cup (F \cup G) = (E \cup F) \cup G$ *(associativité de la réunion).*
- $E \cap \emptyset = \emptyset$ *(l'ensemble vide est absorbant pour l'intersection).*
- $E \cup \emptyset = E$ *(l'ensemble vide est neutre pour la réunion).*
- $E \cap E = E$ *et* $E \cup E = E$.
- $A \subset E$ *si, et seulement si,* $A \cap E = A$ *si, et seulement si,* $A \cup E = E$.
- $E \cap (F \cup G) = (E \cap F) \cup (E \cap G)$ *(l'intersection est distributive par rapport à la réunion).*
- $E \cup (F \cap G) = (E \cup F) \cap (E \cup G)$ *(la réunion est distributive par rapport à l'intersection).*

Proposition 2.1.9. *Si A et B sont deux parties de E, alors :*

- $\overline{E} = \emptyset$ *et* $\overline{\emptyset} = E$.
- $\overline{\overline{A}} = A$.
- $\overline{A \cap B} = \overline{A} \cup \overline{B}$.
- $\overline{A \cup B} = \overline{A} \cap \overline{B}$.

Exercice 2.1.10. Soit A et B deux parties de E. On appelle **différence symétrique** de A et B la partie de E notée $A \triangle B$ et définie par $A \triangle B = (A \setminus B) \cup (B \setminus A)$. Vérifier que

1. $A \triangle B = B \triangle A$.
2. $A \triangle \emptyset = A$.
3. $A \triangle A = \emptyset$.
4. $A \triangle B = (A \cup B) \setminus (A \cap B)$.

2.1.2 Produit cartésien

Définition 2.1.11.

- Le **produit cartésien** de deux ensembles E et F est l'ensemble noté $E \times F := \{(x, y)/x \in E$ et $y \in F\}$. Un élément (x, y) de $E \times F$ est appelé **le couple** (x, y).
- Plus généralemet, si $E_1, \ldots, E_n$ sont n ensembles, $E_1 \times E_2 \times \cdots \times E_n = \{(x_1, \ldots, x_n)/\forall i \in \{1, \ldots, n\}, x_i \in E_i\}$. L'ensemble $E_1 \times E_2 \times \cdots \times E_n$ est noté aussi $\prod_{i=1}^{n} E_i$ et $(x_1, \ldots, x_n)$ est appeleé **n-uplet** de $E_1 \times E_2 \times \cdots \times E_n$.
  Si $E_1 = \cdots = E_n$, on note $E_1 \times E_2 \times \cdots \times E_n = E \times E \times \cdots \times E = E^n$.

Exemple 2.1.12. *On considère les deux ensembles suivants :* $E = \{a, b\}$ *et* $F = \{1, 2\}$, *alors* $E \times F = \{(a, 1), (a, 2), (b, 1), (b, 2)\}$ *et* $E^2 = \{(a, a), (a, b), (b, a), (b, b)\}$.

2.2 Applications

2.2.1 Définitions

Définition 2.2.1. On appelle **correspondance** (ou **relation**) de E vers F tout triplet $f = (E, F, \Gamma)$, où Γ est une partie de $E \times F$.
Si (x, y) est un élément de Γ, y est appeleé **une image** de x par f et x est dit **un antécédent** de y par f. On dit aussi que x est en relation avec y.
Γ est appelé le **graphe de** f.

3.7 L'anneau $\mathbb{Z}/n\mathbb{Z}$

On définit dans $\mathbb{Z}/n\mathbb{Z}$ deux lois de composition : une additivement et l'autre multiplicativement :
— **Addition :** Soit $\overline{x}, \overline{y} \in \mathbb{Z}/n\mathbb{Z}$, on définit $\overline{x} + \overline{y} := \overline{x+y}$.
— **Multiplication :** Soit $\overline{x}, \overline{y} \in \mathbb{Z}/n\mathbb{Z}$, on définit $\overline{x}.\overline{y} := \overline{xy}$.

Théorème 3.7.1. *L'addition et la multiplication dans $\mathbb{Z}/n\mathbb{Z}$ munissent cet ensemble d'une structure d'anneau commutatif non trivial. Cet anneau admet $\overline{0}$ pour élément nul et $\overline{1}$ pour unité.*

Théorème 3.7.2. *La correspondance $f : \{0, 1, \ldots, n-1\} \to \mathbb{Z}/n\mathbb{Z}$, $x \mapsto \overline{x}$ et une bijection et ainsi $\mathbb{Z}/n\mathbb{Z}$ est un ensemble fini ayant n éléments.*

Théorème 3.7.3. *$\mathbb{Z}/n\mathbb{Z}$ est un corps si, et seulement si, n est premier.*

Théorème 3.7.4. ***(Petit théorème de Fermat)*** *Soit $a \in \mathbb{Z}$ et p un nombre premier. Si p ne divise pas a, alors $a^{p-1} \equiv 1 (\mod p)$.*

Corollaire 3.7.5. *Si p est un nombre premier, alors pour tout $a \in \mathbb{Z}$, $a^p \equiv a (\mod p)$.*

Exercice 3.7.6. Soit $n > 1$ un entier, $a, b, c \in \mathbb{Z}$.

1. Montrer que si $a \equiv b (\mod n)$, alors $a^k \equiv b^k (\mod n)$, pour tout entier $k > 0$.
2. On suppose que a, b et c sont non nuls. Montrer que si $ac \equiv bc (\mod n)$, alors $a \equiv b (\mod \frac{n}{d})$, où $d = c \wedge n$.

3.8 Fonction indicatrice d'Euler

Définition 3.8.1. Pour tout entier $n \geq 1$, on note $\varphi(n)$ le nombre des entiers $k \in \{0, 1, \ldots, n-1\}$ tels que $k \wedge n = 1$, i.e., $\varphi(n) = card\{k \in \{0, 1, \ldots, n-1\} / k \wedge n = 1\}$. L'application φ est appelée la **fonction indicatrice d'Euler** ou **l'indicateur d'Euler** et $\varphi(n)$ est l'indicateur d'Euler de n.

Exemple 3.8.2. *On a $\varphi(1) = 1, \varphi(2) = 1, \varphi(10) = 4$.*

Théorème 3.8.3. *Si p est un nombre premier et $k > 0$ est un entier, alors $\varphi(p^k) = p^k - p^{k-1}$.*

Lemme 3.8.4. *Soit $a, b, c \in \mathbb{N}$. $a \wedge bc = 1$ si, et seulement si, $a \wedge b = 1$ et $a \wedge c = 1$.*

Théorème 3.8.5. *Soit $m, n \in \mathbb{N} - \{0, 1\}$. Si m et n sont premiers entre eux, alors $\varphi(mn) = \varphi(m)\varphi(n)$.*

Théorème 3.8.6. *Soit $n > 1$ un entier et $n = p_1^{k_1} \ldots p_r^{k_r}$, avec $p_1, \ldots, p_r$ des nombres premiers et $k_1, \ldots, k_r$ des entiers > 0, alors $\varphi(n) = (p_1^{k_1} - p_1^{k_1-1}) \ldots (p_r^{k_r} - p_r^{k_r-1}) = n(1 - \frac{1}{p_1}) \ldots (1 - \frac{1}{p_r})$.*

Exemple 3.8.7. *on a $1800 = 2^3 3^2 5^2$, alors $\varphi(1300) = 480$.*