Cours de mathématiques

En finir avec les « boîtes noires »

2024-05-20

Valentin Moguérou
Lycée Saint-Louis
2024
MP2I

I. Module Logique (2h)

I.1. Contexte

On se place dans le cadre de la logique classique du premier ordre, non définie ici. On rappelle informellement ses enjeux ici.

Définition 1.1.1 : Une suite de symboles mathématiques s'appelle un **assemblage**. Parmi les assemblages qui ont un sens, on distingue les **termes** et les **relations**. Les termes sont des objets mathématiques, et les relations sont des phrases qui font intervenir ces objets mathématiques.

L'application de définitions, vues comme raccourcis de langage, permettent, par l'introduction de symboles ou de mots français, de se dispenser d'écrire une pure suite de symboles.

Example:

Termes	**Relations**	**Ni l'un, ni l'autre**
• $1 + 1$ • $\mathbb{N}$ • $\{n \in \mathbb{Z} \mid \exists p \in \mathbb{Z} : n = 2p + 1\}$	• $1 + 1 = 2$ • Les zéros non triviaux de la fonction ζ se situent tous sur la droite complexe d'équation $\mathfrak{R}(z) = \frac{1}{2}$. • $2 + 2 = 5$	• 1 et 2

Définition 1.1.2 : Les relations font intervenir une ou plusieurs variables. On appelle argument de la relation toute variable non définie présente dans la relation. On appelle arité de la relation son nombre d'arguments.

On dit qu'une relation est un prédicat si elle est d'arité ≥ 1, et que c'est une proposition sinon.

Définition 1.1.3 (Vérité) : On attribue aux propositions une valeur booléenne appelée vérité, qui peut être « vrai » ou « faux » : l'un ou l'autre, toujours l'un, mais jamais les deux à la fois.

Une proposition vraie (resp. fausse) est appelée une tautologie (resp. antilogie).

On note $\top$ (lire « top ») et $\bot$ (lire « bot ») deux propositions telles que $\top$ soit vraie et $\bot$ soit fausse.

I.2. Connecteurs logiques

Définition 1.2.1 (Connecteurs logiques) : Étant donné deux propositions P et Q, on appelle :

- négation de P, notée $\neg P$, la proposition vraie ssi $\neg P$ est fausse ;
- conjonction de P et Q, notée $P \wedge Q$ ou P et Q, la proposition vraie ssi P et Q sont simultanément vraies ;
- disjonction de P et Q, notée $P \vee Q$ ou P ou Q la proposition fausse ssi P et Q sont simultanément fausses

On donne les tables de vérité des connecteurs précédents.

Tableau 1 — Tables de vérités usuelles

P	$\neg P$
V	F
F	V

a) Table de la négation

P	Q	$P \wedge Q$
V	V	V
V	F	F
F	V	F
F	F	F

b) Table de la conjonction

P	Q	$P \vee Q$
V	V	V
V	F	V
F	V	V
F	F	F

c) Table de la disjonction

Définition 1.2.2 (Équivalence au sens de la vérité) : On dit que deux propositions P et Q sont équivalentes au sens de la vérité, et l'on note $P \equiv Q$ ssi elles ont la même valeur de vérité.

Proposition 1.2.1 (Propriétés élémentaires des connecteurs logiques) : Soient P, Q et R trois propositions. On a toujours :

- $P \wedge Q \equiv Q \wedge P$ (commutativité de $\wedge$)
- $P \vee Q \equiv Q \vee P$ (commutativité de $\vee$)
- $(P \wedge Q) \wedge R \equiv P \wedge (Q \wedge R)$ (associativité de $\wedge$)
- $(P \vee Q) \vee R \equiv P \vee (Q \vee R)$ (associativité de $\vee$)
- $\neg\neg P \equiv P$ (double négation)
- $\neg(P \wedge Q) \equiv \neg P \vee \neg Q$ (lois de De Morgan)
- $\neg(P \vee Q) \equiv \neg P \wedge \neg Q$ (lois de De Morgan)
- $(P \wedge Q) \vee R \equiv (P \vee R) \wedge (Q \vee R)$ (distributivité de $\vee$ par rapport à $\wedge$)
- $(P \vee Q) \wedge R \equiv (P \wedge R) \vee (Q \wedge R)$ (distributivité de $\wedge$ par rapport à $\vee$)

Démonstration : Il suffit de dresser les tables de vérité. ■

Remarque (Dualité) : Remarquons que les formules présentées restent vraies si l'on change tous les $\wedge$ par des $\vee$ et inversement.

I.3. Implication et équivalence

Définition 1.3.1 (Implication) : Étant données deux propositions P et Q, on appelle implication de P envers Q, et l'on note $P \Rightarrow Q$, la proposition $\neg P \vee Q$.

Tableau 2 — Table de vérité de l'implication

P	Q	$P \Rightarrow Q$
V	V	V
V	F	F
F	V	V
F	F	V

Définition 1.3.2 : Soient P et Q deux propositions. On appelle **contraposée** de l'implication $P \Rightarrow Q$ l'implication $\neg Q \Rightarrow \neg P$, et **réciproque** de $P \Rightarrow Q$ l'implication $Q \Rightarrow P$.

Proposition 1.3.1 : Une implication et sa contraposée sont équivalentes au sens de la vérité.

Démonstration : Soient P et Q deux propositions. On a :

$$\begin{aligned} P \Rightarrow Q &\equiv \neg P \lor Q \\ &\equiv Q \lor \neg P \quad \text{(commutativité)} \\ &\equiv \neg\neg Q \lor \neg P \quad \text{(double négation)} \\ &\equiv \neg Q \Rightarrow \neg P \end{aligned}$$

■

Définition 1.3.3 : On appelle équivalence de P et Q, notée $P \Leftrightarrow Q$, la proposition

$$(P \Rightarrow Q) \land (Q \Rightarrow P)$$

Tableau 3 — Table de vérité de l'équivalence

P	Q	$P \Leftrightarrow Q$
V	V	V
V	F	F
F	V	F
F	F	V

Proposition 1.3.2 : Soient P et Q deux propositions. Alors on a $P \equiv Q$ si, et seulement si la proposition $P \Leftrightarrow Q$ est vraie.

Démonstration :
- Mq $\Longrightarrow$. Supposons $P \equiv Q$. Alors P et Q ont la même valeur de vérité, donc on a :
  - Soit P est vraie et Q est vraie, donc $P \Leftrightarrow Q$ est vraie
  - Soit P est fausse et Q est fausse, donc $P \Leftrightarrow Q$ est fausse
- Mq $\Longleftarrow$. Supposons que $P \Leftrightarrow Q$ soit vraie. Alors d'après la table de vérité de l'équivalence, on a soit P vraie et Q vraie, soit P fausse et Q fausse. Dans les deux cas, P et Q ont la même valeur de vérité donc $P \equiv Q$.

■

I.4. Raisonnements

Règle 1.4.1 : Pour montrer qu'une proposition de la forme $P \Rightarrow Q$ est vraie, on écrit :

« Supposons que P, montrons Q. », puis on démontre Q.

Formellement, on dit que l'on démontre Q dans la théorie obtenue en adjoignant P aux axiomes de la théorie ambiante.

Proposition 1.4.1 (*Modus ponens*): Soient P et Q deux propositions, alors

$$P \land (P \Rightarrow Q) \Rightarrow Q$$

est une tautologie.

Démonstration: On a d'abord

$$\begin{aligned} P \land (P \Rightarrow Q) &\equiv P \land (\neg P \lor Q) \\ &\equiv (P \land \neg P) \lor (P \land Q) \\ &\equiv P \land Q, \end{aligned}$$

puis $P \land Q \Rightarrow Q$, car

$$P \land Q \Rightarrow Q \equiv \neg(P \land Q) \lor Q \equiv \neg P \lor \underbrace{\neg Q \lor Q}_{\equiv \top} \equiv \top.$$

■

I.5. Quantification

Jusqu'ici nous avons travaillé à l'ordre zéro, c'est-à-dire que nous n'avons travaillé qu'avec des propositions, des relations d'arité zéro. Nous introduisons donc des notions de calcul des prédicats, essentielles.

Motivation

Si l'on considère $P_1, ..., P_n$ n propositions. On peut se demander s'il existe un k entre 1 et n tel que P_k soit vraie, et on peut se demander si toutes les propositions P_k sont vraies.

En écrivant

$$D = P_1 \lor ... \lor P_n = \bigvee_{i=1}^{n} P_i \quad \text{et} \quad C = P_1 \land ... \land P_n = \bigwedge_{i=1}^{n} P_i,$$

le problème se ramène à la vérité de D ou de C. Maintenant on souhaite généraliser. On considère un prédicat unaire $P(x)$, d'unique argument x. On veut savoir s'il existe un x tel que $P(x)$ ou si pour tout x, on ait $P(x)$. Cependant, on ne peut pas énumérer tous les termes x pour les tester. On est donc limité par nos symboles actuels. On en introduit donc deux autres.

Définition 1.5.1.1 (Quantificateurs): Soit $P(x)$ un prédicat unaire d'argument x.

On note :
- $\exists x P(x)$ la proposition (il s'agit bien d'une proposition) vraie si, et seulement si il existe un terme x tel que $P(x)$.
- $\forall x P(x)$ la proposition vraie ssi pour tout terme x, $P(x)$ soit vraie

Proposition 1.5.1.1 (Négation d'une quantification) : Soit $P(x)$ un prédicat. On a :

- $\neg(\exists x \ P(x)) \equiv \forall x \ \neg P(x)$
- $\neg(\forall x \ P(x)) \equiv \exists x \ \neg P(x)$

Remarque : C'est une généralisation des lois de De Morgan.

Démonstration :

- Supposons $\neg(\exists x \ P(x))$. Montrons que $\forall x \ \neg P(x)$.

  Soit x un terme, montrons que $P(x)$. Supposons par l'absurde $P(x)$, alors $P(x)$ serait exemplifiée par x, donc $\exists x \ P(x)$ ce qui contredit l'hypothèse.
- Supposons $\forall x \ \neg P(x)$. Montrons que $\neg(\exists x \ P(x))$. Supposons par l'absurde qu'il existe un x tel que $P(x)$. Alors en applicant l'hypothèse à x, on aurait $\neg P(x)$, ce qui est absurde.
- Pour le deuxième point, on utilise le premier. On a

$$\neg(\forall x \ P(x)) \equiv \neg\neg(\exists x \ P(x)) \equiv \exists x \ P(x).$$

■

Proposition 1.5.1.2 (Compatibilité des quantificateurs avec les connecteurs idoines) : Soient $P(x)$ et $Q(x)$ deux prédicats unaires. On a

- $\exists x \ (P(x) \vee Q(x)) \equiv (\exists x \ P(x)) \vee (\exists x \ Q(x))$
- $\forall x \ (P(x) \wedge Q(x)) \equiv (\forall x \ P(x)) \wedge (\forall x \ Q(x))$

Remarque : C'est une généralisation de l'associativité de $\vee$ et $\wedge$.

Démonstration : Triviale, laissée en exercice de rédaction au lecteur. ■

II. Module Ensembles, relations et applications (2h)

II.1. Vocabulaire ensembliste

Note historique 2.1.1 : La théorie des ensembles s'est formalisée à la fin du XIX^e^ siècle avec l'appui de mathématiciens tels que Georg Cantor (1845-1918), David Hilbert (1862-1943). WIP

Définition 2.1.1 (Ensemble) : On appelle ensemble tout terme.

Remarque : Cette définition paraît décevante au premier regard. On vous avait peut-être vendu précédemment une notion de « collection d'objets mathématiques », ou bien de « collection désordonnée d'objets mathématiques ». Mais ces définitions n'en sont pas vraiment, elles utilisent elles-mêmes des mots non définis.

Ces tentatives de définitions qui plaisent à l'intuition cachent le fait que le concept d'ensemble est une **notion primitive** de la théorie des ensembles. C'est un concept qui n'est pas défini car c'est une brique de base de la théorie.

Notation 2.1.2 : Soit $\mathcal{R}$ une relation binaire. Quels que soient les termes x et y, on note $x\mathcal{R}y$ la proposition $\mathcal{R}(x, y)$.

Définition 2.1.3 (Appartenance) : On considère sur la théorie des ensembles un prédicat binaire noté $\in$. Pour tous termes x, y, on note $x \in y$ au lieu de $\in(x, y)$ et l'on dit x appartient à y.

Notation 2.1.4 (Quantification restreinte ou typique) : Soit $P(x)$ un prédicat et E un ensemble.

On note :
- $\exists x \in E \quad P(x)$ au lieu de $\exists x \quad x \in E \wedge P(x)$;
- $\forall x \in E \quad P(x)$ au lieu de $\forall x \quad x \in E \Rightarrow P(x)$.

Remarque : En particulier, **quel que soit** le prédicat P,
- $\exists x \in \varnothing \quad P(x)$ est une antilogie
- $\forall x \in \varnothing \quad P(x)$ est une tautologie

Définition 2.1.5 (Égalité) : On définit une relation binaire notée $=$, et l'on note $x = y$ au lieu de $=(x, y)$ et l'on dit que x égale y ou que x et y.

Règle 2.1.1 (Critères de substitution) : Soit $P(x)$ un prédicat unaire, et $U(x), V(x)$ deux termes à un argument.

Alors :
- $\forall x \forall y \quad x = y \Rightarrow (P(x) \Leftrightarrow P(y))$;
- $\forall x \quad x = y \Rightarrow U(x) = V(y)$.

II.2. Axiomes de la théorie des ensembles

Axiome 2.2.1 (Existence d'un ensemble vide) : Il existe un ensemble vide, c.-à-d. :

$$\exists E \ \forall x \quad x \notin E$$

Définition 2.2.1 : Soient E et F deux ensembles. On dit que E est inclus dans F et l'on note $E \subset F$ si, et seulement si $\forall x \quad x \in E \Rightarrow x \in F$.

Axiome 2.2.2 (Axiome d'extensionnalité) : Les ensembles sont entièrement caractérisés par leurs éléments, c'est-à-dire :

$$\forall E \forall F \quad E = F \Leftrightarrow (\forall x \quad x \in E \Leftrightarrow x \in F),$$

ce qui est équivalent à

$$\forall E \forall F \quad E = F \Leftrightarrow (E \subset F \land F \subset E)$$

Définition 2.2.2 : On dit qu'une relation binaire est :
- réflexive ssi $\forall x \quad x \mathcal{R} x$
- symétrique ssi $\forall x \forall y \quad x \mathcal{R} y \Rightarrow y \mathcal{R} x$
- transitive ssi $\forall x \forall y \forall z \quad x \mathcal{R} y \land y \mathcal{R} z \Rightarrow x \mathcal{R} z$
- antisymétrique ssi $\forall x \forall y \quad x \mathcal{R} y \land y \mathcal{R} x \Rightarrow x = y$.

Définition 2.2.3 (Relation d'équivalence) : On dit qu'une relation binaire $\mathcal{R}$ est une relation d'équivalence ssi elle est réflexive, symétrique et transitive.

Définition 2.2.4 (Relation d'ordre): On dit qu'une relation binaire $\mathcal{R}$ est une relation d'ordre ssi elle est réflexive, transitive et antisymétrique.

Proposition 2.2.1: L'égalité est une relation d'équivalence.

Démonstration: Elle coïncide avec la relation binaire $\mathcal{R}$ définie pour tous ensembles E, F par $E\mathcal{R}F \Leftrightarrow (\forall x \quad x \in E \Leftrightarrow x \in F)$ qui est évidemment une relation d'équivalence.
■

Proposition 2.2.2: L'inclusion est une relation d'ordre.

Démonstration:
- La réflexivité et la transitivité découlent des propriétés de l'implication ;
- L'antisymétrie est l'axiome d'extensionnalité.

■

Proposition 2.2.3: Il existe un unique ensemble vide. On le note $\varnothing$.

Démonstration:
- Existence : par axiome
- Unicité : Soient E et F deux ensembles tels que $\forall x \ (x \notin E \wedge x \notin F)$. On a alors $E \subset F$ et $F \subset E$, donc par l'axiome d'extensionnalité $E = F$.

■

Définition 2.2.5 (Quantification existentielle avec unicité): Soit $P(x)$ un prédicat. On note

$$\exists! x \quad P(x)$$

la proposition

$$(\exists x \quad P(x)) \wedge (\forall x \forall y \ P(x) \wedge P(y) \Rightarrow x = y)$$

Définition 2.2.6: On dit qu'un prédicat P de variable x est collectivisant en x si, et seulement si

$$\exists E \ \forall x \quad (x \in E \Leftrightarrow P(x)).$$

Proposition 2.2.4: Dans ce cas, si un ensemble E vérifie

$$\forall x \quad x \in E \Leftrightarrow P(x),$$

alors il est unique et on le note $\{x \mid P(x)\}$.

Démonstration: Soient E et F deux ensembles, dont l'appartenance équivaut à vérifier P. Alors, pour tout x, $x \in E \Leftrightarrow P(x) \Leftrightarrow x \in F$ donc par l'axiome d'extensionnalité, $E = F$. ∎

Axiome 2.2.3 (Schéma d'axiomes de compréhension): Soit P un prédicat unaire et E un ensemble. Alors la relation $x \in E \wedge P(x)$ est collectivisante en x.

Notation 2.2.7: On note $\{x \in E \mid P(x)\} = \{x \mid x \in E \wedge P(x)\}$

Proposition 2.2.5 (Intersection binaire): Soient A et B deux ensembles. Alors la relation $x \in A \wedge x \in B$ est collectivisante en x. L'ensemble associé est noté $A \cap B$.

Démonstration: Il suffit de poser $A \cap B = \{x \in A \mid x \in B\}$. ∎

Proposition 2.2.6 (Intersection quelconque): Soit E un ensemble **non vide**. Alors la relation $\forall F \in E, x \in F$ est collectivisante en x. L'ensemble associé se note alors $\bigcap E$ ou encore $\bigcap\limits_{F \in E} E$.

Démonstration: Comme E est non vide, il possède un élément F_0. On pose alors

$$I = \{x \in F_0 \mid \forall F \in E, x \in F\}.$$

On a alors, pour tout x :

$$\begin{aligned} x \in I &\Leftrightarrow x \in F_0 \wedge \forall F \in E \quad x \in F \\ &\Leftrightarrow \forall F \in E \quad x \in F \quad \text{car } F_0 \in E \end{aligned}$$

■

Proposition 2.2.7 (Différence ensembliste): Soient A et B deux ensembles. Alors la relation $x \in A \wedge \neg(x \in B)$ est collectivisante en x. L'ensemble associé est noté $A \setminus B$.

Démonstration: Il suffit de poser $A \setminus B = \{x \in A \mid x \notin B\}$. ■

Définition 2.2.8 (Complémentaire): En particulier, quand B est une partie de A, on note $\complement_A B$ ou $\overline{B}^A$, ou $\overline{B}$ lorsqu'il n'y a pas d'ambiguïté sur la valeur de A, l'ensemble $A \setminus B$, et on l'appelle le complémentaire de B dans A.

Axiome 2.2.4 (Axiome de la paire): Soient a et b deux termes (non nécessairement différents). Alors la relation $x = a \vee x = b$ est collectivisante en x. L'ensemble associé se note $\{a; b\}$.

Remarque: En particulier, cet axiome assure que pour tout a, le singleton $\{a\}$ existe. On a donc par définition

$$\forall x \quad x \in \{a\} \Leftrightarrow x = a.$$

Axiome 2.2.5 (Axiome de l'union): Soit E un ensemble (comprendre ensemble d'ensembles). Alors la relation

$$\exists F \in E \quad x \in F$$

est collectivisante en x. L'ensemble associé se note $\bigcup E$ ou $\bigcup\limits_{F \in E} F$.

Proposition 2.2.8 (Union binaire): Soient A et B deux ensembles. La relation $x \in A \vee x \in B$ est collectivisante en x et l'on note $A \cup B$ l'ensemble associé.

Démonstration: Il suffit de poser $A \cup B = \bigcup\{A; B\}$. ■

Proposition 2.2.9 (Traductions ensemblistes) : Soit

Axiome 2.2.6 (Axiome des parties) : Soit E un ensemble. Alors la relation $F \subset E$ est collectivisante en F. L'ensemble associé se note $\mathcal{P}(F)$ ou $\mathfrak{P}(F)$.

Axiome 2.2.7 (Axiome de fondation) : Soit E un ensemble non vide. Alors il possède un élément x tel que $x \cap E = \varnothing$.

Proposition 2.2.10 (Irréflexivité de l'appartenance) : Soit E un ensemble. Alors $E \notin E$.

Démonstration : Soit E un ensemble. Supposons par l'absurde $E \in E$. On a donc $\{E\} \subset E$. Comme $\{E\}$ est non vide, il possède un élément x tel que $x \cap E = \varnothing$. Or $x \in \{E\}$ donc $x = E$, puis $E \cap E = \varnothing$, donc $E = \varnothing$, ce qui contredit le fait qu'il possède un élément. ■

II.3. Couples

Définition 2.3.1 (Couples au sens de Kuratowski) : Soient x et y deux termes. On appelle couple formé de x et y l'ensemble $\{\{x\}; \{x; y\}\}$. On le note $(x; y)$.

Proposition 2.3.1 (Unicité des couples) : Soient a, b, c, d quatre termes. On a :

$$(a; b) = (c; d) \Leftrightarrow \begin{cases} a = c \\ b = d \end{cases}$$

Démonstration : Par double implication.

L'implication $\Longleftarrow$ est évidente. Montrons $\Longrightarrow$.

Supposons $(a, b) = (c, d)$. Montrons $a = c$ et $b = d$.

On a donc $\{\{a\}; \{a; b\}\} = \{\{c\}; \{c; d\}\}$,

donc

- Ou bien $\{a\} = \{c; d\}$ et $\{a; b\} = \{c\}$, ce qui implique $a = b$ et $c = d$, puis $a = c$ et $a = d$

- Ou bien $\{a\} = \{c\}$ et $\{b\} = \{d\}$, donc $a = c$ et $b = d$.

■

Définition 2.3.2: Pour tout couple (a, b), on note $\mathrm{pr}_1((a, b)) = a$ et $\mathrm{pr}_2((a, b)) = b$.

Ces deux opérateurs sont bien définis par la propriété précédente.

Notation 2.3.3: Si $P(x, y)$ est un prédicat binaire, au lieu de $\forall x \forall y \quad P(x, y)$ on peut noter $\forall (x; y) \quad P(x; y)$.

Définition 2.3.4: Soit $\mathcal{R}$ une relation binaire. On dit que $\mathcal{R}$ est collectivisante si, et seulement si la relation « x est un couple de la forme (a, b) et $\mathcal{R}(a; b)$ » est collectivisante en x.

Dans le cas où $\mathcal{R}$ est collectivisante, l'ensemble associé s'appelle **graphe** de $\mathcal{R}$.

Proposition 2.3.2 (Produit cartésien): Soient E et F deux ensembles.

La relation $x \in E \land y \in F$ est collectivisante en (x, y).

On appelle produit cartésien de E et F, noté $E \times F$ et lu « E croix F » l'ensemble associé.

Démonstration: On cherche à trouver un surensemble de l'ensemble que l'on essaie de construire, pour en prendre une partie.

Soit $x \in E$ et $y \in F$. On a $(x, y) = \{\{x\}, \{x, y\}\} = \{\{x\}\} \cup \{\{x, y\}\}$.

Or $x \in E$ et $y \in F$ donc $\{x, y\} \subset E \cup F$ puis $\{x, y\} \in \mathcal{P}(E \cup F)$. De même $\{x\} \in \mathcal{P}(E \cup F)$, puis $\{\{x\}, \{x, y\}\} \in \mathcal{P}(\mathcal{P}(E \cup F))$.

Pour tout a, notons $P(a)$ la proposition « a est un couple de la forme (x, y) et $x \in E \land y \in F)$ ».

On a montré $\forall a \quad P(a) \Rightarrow a \in \mathcal{P}(\mathcal{P}(E \cup F))$.

Notons $G = \{a \in \mathcal{P}(\mathcal{P}(E \cup F)) \mid P(a)\}$.

On a toujours $\forall a \quad P(a) \Rightarrow a \in G$ mais on a en plus $\forall a \quad a \in G \Rightarrow P(a)$, donc la relation $P(a)$ est collectivisante en a d'ensemble associé G. ■

II.4. Correspondances et applications

Définition 2.4.1 (Correspondance) : Soient E et F deux ensembles, et $\Gamma \subset E \times F$. On appelle correspondance entre E et F le terme $f = (\Gamma, (E, F))$.

On note $\mathrm{Cor}(E, F)$ l'ensemble des correspondances de E vers F. Il s'agit bien d'un ensemble car il s'identifie naturellement à $\mathcal{P}(E \times F)$.

On note $x \mapsto y$ la relation $(x, y) \in \Gamma$.

On dit que E est l'ensemble de départ de f et que F est l'ensemble d'arrivée de f.

Pour tout $(x, y) \in E \times F$, si $x \mapsto y$ on dit que y est une image de x et que x est un antécédent de x.

Définition 2.4.2 (Fonction) : Soit E, F deux ensembles et f une correspondance de E vers F. On dit que f est une fonction de E dans F si, et seulement si

$$\forall x \in E \ \forall (y, y') \in F^2 \quad (x \mapsto y \land x \mapsto y') \Rightarrow y = y'$$

Cela revient à dire que si un élément x de E possède une image, alors elle est unique. On la note alors $f(x)$.

Définition 2.4.3 (Application) : Soit E, F deux ensembles et f une correspondance de E vers F. On dit que f est une application de E dans F si, et seulement si

$$\forall x \in E \ \exists! y \in F \quad x \mapsto y.$$

Cela revient à dire que tout élément de E possède une image et qu'elle est unique. On la note alors $f(x)$. L'ensemble des applications de E dans F se note F^E (ou plus rarement $\mathcal{F}(E, F)$).

Définition 2.4.4 (Injectivité, surjectivité, bijectivité) : Soit f une application de E dans F. On dit qu'elle est :

- injective ssi $\forall (x, x') \in E^2 \quad f(x) = f(x') \Rightarrow x = x'$
- surjective ssi $\forall y \in F \ \exists x \in E \quad f(x) = y$
- bijective ssi elle est injective et surjective

Proposition 2.4.1 (Caractérisation des bijections) : Soit f une application de E dans F. Elle est bijective si, et seulement si

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

Définition 2.4.5 (Permutation) : Soit E un ensemble. Une bijection de E dans E s'appelle une permutation. L'ensemble des permutations de E se note $S(E)$ ou $\mathfrak{S}(E)$

Définition 2.4.6 (Identité) : Pour tout ensemble E, on note id_E l'application

$$\begin{aligned} \mathrm{id}_E : E &\to E \\ x &\mapsto x \end{aligned}$$

Définition 2.4.7 (Composition) : Soient E, F, G trois ensembles et $f : E \to F$, $g : F \to G$ deux applications. On note

$$\begin{aligned} g \circ f : E &\to G \\ x &\mapsto g(f(x)). \end{aligned}$$

Attention, c'est la fonction f qui est évaluée en premier.

Attention, la proposition suivante est réservée pour une seconde lecture et fait appel à des notions encore non abordées.

Proposition 2.4.2 (Structure de S_E) : Soit E un ensemble. $(S_E, \circ)$ est un groupe.

Définition 2.4.8 (Image directe) : Soit E, F deux ensembles, f une application de E dans F et A une partie de E. On appelle image directe de A par f, notée $f(A)$ l'ensemble

$$\{y \in F \mid \exists x \in E\ f(x) = y\}$$

Proposition 2.4.3: Soit E, F deux ensembles, f une application de E dans F et A, B deux parties de E. On a :

- $f(A \cup B) \subset f(A) \cup f(B)$
- $f(A \cap B) \subset f(A) \cap f(B)$
- $\overline{f(A)} \subset f\left(\overline{A}\right)$

Notation 2.4.9: On le note aussi $\{f(x) : x \in E\}$. Cette dernière notation permet de ne pas expliciter l'application f mais seulement son comportement.

Définition 2.4.10 (Image réciproque): Soit E, F deux ensembles, f une application de E dans F et B une partie de F. On appelle image réciproque de B par f, notée $f^{-1}(B)$ l'ensemble

$$\{x \in E \mid f(x) \in B\}.$$

II.5. Entiers naturels

Définition 2.5.1 (Opérateur « successeur »): Pour tout ensemble E, on appelle successeur de E, noté $s(E)$ l'ensemble $E \cup \{E\}$.

Définition 2.5.2: On note : $0 := \varnothing$, $1 := s(\varnothing)$, $2 := s(s(\varnothing))$, $3 := s(s(s(\varnothing)))$, …

Proposition 2.5.1: On a toujours $E \subset s(E)$.

Démonstration: Triviale. ■

Proposition 2.5.2: Soit E un ensemble. L'union $E \cup \{E\}$ est disjointe.

Démonstration: Soit E un ensemble. Supposons par l'absurde $E \cup \{E\} \neq \varnothing$. Il existe donc $x \in E \cup \{E\}$ puis $x = E$ donc $E \in E$, ce qui est absurde. ■

Proposition 2.5.3 (Fondation) : L'ensemble vide n'a pas de prédecesseur.

Démonstration : Supposons qu'il existe un ensemble E tel que $s(E) = \varnothing$. Alors $E \subset \varnothing$ donc $E = \varnothing$. ■

Définition 2.5.3 : On dit qu'un ensemble E est héréditaire si, et seulement si

$$\forall x \in E \quad s(x) \in E.$$

Définition 2.5.4 : Soit E un ensemble héréditaire. On appelle support de E, noté $\operatorname{Supp}(E)$ l'ensemble

$$\{y \in E \mid \forall x \in E \; s(x) \neq y\}.$$

C'est le sous-ensemble des éléments de E qui n'ont pas de prédecesseur.

Proposition 2.5.4 (Source d'un élément) : Soit E un ensemble héréditaire, et $x \in E$.

Axiome 2.5.1 (De l'infini) : Il existe un ensemble héréditaire qui possède $\varnothing$.

Attention, un tel ensemble n'a pas de raison d'être unique ! En effet, on pourrait très bien imaginer un ensemble constitué de deux chaînes distinctes :

$$E_{\text{hyp}} = \{\varnothing, s(\varnothing), s^2(\varnothing), ..., \alpha, s(\alpha), ...\}$$

On voudrait donc bien disposer d'un ensemble unique, qui ne possède qu'une seule chaîne !

Proposition 2.5.5 (Ensemble des entiers naturels) : Il existe un unique ensemble héréditaire de support $\{\varnothing\}$. On le note $\mathbb{N}$.