L1S2 Informatique — Université de Tours
Notes de Cours 2018-2019
Emmanuel Chasseigne

Cours Numéro 3 — *Ensembles, applications et lois de composition interne*

(a) Rappels sur les ensembles

- Un ensemble est une collection d'objets distincts ; ces objets s'appellent les éléments de cet ensemble. Si x est un élément de E, on note $x \in E$.
- Ensembles usuels: $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$...
- $A \subset E$ signifie que A est une partie (ou un sous-ensemble) de E, c'est-à-dire que tout élément de A appartient à E.
- On note $\emptyset$ l'ensemble vide.
- L'ensemble $\mathcal{P}(E) = \{A \mid A \subset E\}$ est l'ensemble des parties de E.
- $A \cap B = \{x \mid x \in A \text{ et } x \in B\}$, A et B sont disjoints si $A \cap B = \emptyset$.
- $A \cup B = \{x \mid x \in A \text{ ou } x \in B\}$.
- $A \setminus B = \{x \mid x \in A \text{ et } x \notin B\} = C_A(B)$.
- $A \times B = \{(a, b) \mid a \in A \text{ et } b \in B\}$.

Proposition — Soient A, B, C des parties d'un ensemble E. On a alors plusieurs propriétés:

(i) Commutativité :
$$A \cap B = B \cap A \quad \text{et} \quad A \cup B = B \cup A.$$

(ii) Associativité :
$$\big(A \cap B\big) \cap C = A \cap \big(B \cap C\big) = A \cap B \cap C \quad \text{et} \quad \big(A \cup B\big) \cup C = A \cup \big(B \cup C\big) = A \cup B \cup C.$$

(iii) Distributivité :
$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \quad \text{et} \quad A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

(iv) Lois de Morgan :
$$(A \cup B)^c = A^c \cap B^c \quad \text{et} \quad (A \cap B)^c = A^c \cup B^c.$$

(b) Quantificateurs

- Si E est un ensemble, on appelle prédicat sur E toute proposition $P(x)$ dépendant d'une variable $x \in E$. Ainsi, selon x, $P(x)$ peut être vraie ou fausse.
- A l'aide des quantificateurs $\forall$ (pour tout) et $\exists$ (il existe), on définit les assertions suivantes :

- ($\forall x \in E$, $P(x)$) qui est vraie si et seulement si tous les éléments e de E donnent une assertion $P(e)$ vraie.
- ($\exists x \in E$, $P(x)$) qui est vraie si et seulement si au moins un élément e de E donne une assertion $P(e)$ vraie.

Attention, en présence de plusieurs quantificateurs, l'ordre compte !
Par exemple, les assertions

$$\forall x \in \mathbb{N}, \exists y \in \mathbb{N}, x < y \quad \text{et} \quad \exists y \in \mathbb{N}, \forall x \in \mathbb{N}, x < y$$

ne sont pas équivalentes. La première est vraie tandis que la seconde est fausse.
En revanche, en échangeant deux quantificateurs identiques, on obtient toujours deux assertions équivalentes.

Négations et quantificateurs:

La négation opère de la façon suivante :
NON($\forall x \in E$, $P(x)$) $\Leftrightarrow$ ($\exists x \in E$, NON($P(x)$))
NON($\exists x \in E$, $P(x)$) $\Leftrightarrow$ ($\forall x \in E$, NON($P(x)$))

(c) Rappels sur les applications

- Une application est la donnée d'un triplet (f, E, F) tel qu'à tout élément x de E est associé un unique élément de F, noté $f(x)$. On note $f : E \to F$.

- L'ensemble E s'appelle ensemble de départ de f et l'ensemble F s'appelle ensemble d'arrivée de f. Si $y = f(x)$, l'élément $y \in F$ est appelé image de x par f, l'élément $x \in E$ est appelé antécédent de y par f.

- L'application $Id_E : E \to E$ est définie par $Id_E(x) = x$ pour tout $x \in E$; elle s'appelle identité de E.

- Soient E, F et G trois ensembles et $f : E \to F$, $g : F \to G$ des applications. L'application $g \circ f : E \to G$ définie par $g \circ f(x) = g(f(x))$ pour tout $x \in E$, s'appelle la composée de g et f.

Définition. Une application $f : E \longrightarrow F$ est dite **injective** si tout élément de F possède au plus un antécedent par f ; c'est-à-dire si pour tout $y \in F$, l'équation $y = f(x)$ possède au plus une solution x dans E.

En langage mathématique,
l'application f est injective si : $\forall x_1 \in E,\ \forall x_2 \in E,\ f(x_1) = f(x_2) \Rightarrow x_1 = x_2$;
l'application f n'est pas injective si : $\exists x_1 \in E,\ \exists x_2 \in E,\ x_1 \neq x_2$ et $f(x_1) = f(x_2)$.

Définition. Une application $f : E \longrightarrow F$ est dite surjective si tout élément de F possède au moins un antécédent par f; c'est-à-dire si pour tout $y \in F$, l'équation $y = f(x)$ possède au moins une solution x dans E.

En langage mathématique,
l'application f est surjective si : $\forall y \in F,\ \exists x \in E,\ f(x) = y$;
l'application f n'est pas surjective si : $\exists y \in F,\ \forall x \in E,\ f(x) \neq y$.

Définition. Une application $f : E \longrightarrow F$ est dite bijective si elle est injective et surjective; c'est-à-dire si tout élément de F possède exactement un antécédent par f; ou encore si pour tout $y \in F$, l'équation $y = f(x)$ possède exactement une solution x dans E.

Si f est une bijection de E sur F, on appelle bijection réciproque de f, l'application $f^{-1} : F \to E$ qui à tout $y \in F$ associe son unique antécédent x de E. On a $f \circ f^{-1} = Id_F$ et $f^{-1} \circ f = Id_E$.

(d) Image directe, image réciproque

- Soit $f : E \to F$ une application. Pour tout $A \subset E$, on note $f(A) = \{f(x) \mid x \in A\}$ l'image de A par f. Pour tout $y \in F$, on a

$$y \in f(A) \Leftrightarrow \exists x \in A,\ f(x) = y.$$

- Pour toute $B \subset F$ on note $f^{-1}(B) = \{x \in E \mid f(x) \in B\}$ l'image réciproque de B par f. Pour tout $x \in E$, on a :

$$x \in f^{-1}(B) \Leftrightarrow f(x) \in B.$$

Proposition — Soient $f : E \to F$ une application de E dans F, A_1 et A_2 deux parties de E et B_1 et B_2 deux parties de F. On a :

$$\begin{array}{rcl}
\text{si } A_1 \subset A_2 \text{ alors } f(A_1) \subset f(A_2) & \text{et} & \text{si } B_1 \subset B_2 \text{ alors } f^{-1}(B_1) \subset f^{-1}(B_2) \\
f(A_1 \cup A_2) = f(A_1) \cup f(A_2) & \text{et} & f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2) \\
f(A_1 \cap A_2) \subset f(A_1) \cap f(A_2) & \text{et} & f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2) \\
A \subset f^{-1}(f(A)) & \text{et} & f(f^{-1}(B)) \subset B.
\end{array}$$

Attention : toutes les inclusions ci-dessus peuvent être strictes.

(e) Loi de composition interne

Définition. Soit E un ensemble. Une lci sur E est la donnée d'une application

$$\star : E \times E \to E\,.$$

Autrement dit, une lci est une "opération" qui, à un couple $(x, y) \in E \times E$ associe un unique $z = x \star y$ dans E. On appelle z le composé de x et y par la loi $\star$.

Exemples immédiats — $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ munis de l'addition ou la multiplication; l'ensemble des fonctions définies sur $\mathbb{R}$ muni de la composition; Les opération $\cap$ et $\cup$ sur les parties d'un ensemble E.

La table de Cayley d'une lci est la table qui récapitule la valeur de $x \star y$ en fonction de x et y, placés en ligne/colonne. Par exemple, si $E = \{a, b, c\}$, la table suivante détermine une lci:

$\star$	a	b	c
a	c	b	b
b	a	c	a
c	b	a	c

(f) Propriétés des lci

Définition. La lci $\star$ est associative si pour tout $(x, y, z) \in E^3$, $x \star (y \star z) = (x \star y) \star z$, ce qu'on notera $x \star y \star z$. La loi est dite commutative si pour tout $(x, y) \in E^2$, $x \star y = y \star x$.

Exemple: la table précédente donn-t-elle une loi associative? commutative? qu'en est-il pour les lois $+$ et $\times$ sur $\mathbb{R}$?

Définition. Un élément neutre (pour $\star$) est un élément $e \in E$ tel que $e \star x = x \star e = x$ pour tout $x \in E$.

Exemple: pour l'addition dans $\mathbb{N}$, $e = 0$ est un élément neutre. De même, 1 est l'élément neutre pour la multiplication dans $\mathbb{Q}$. NB: si l'élément neutre existe, il est unique (exercice).

Définition. Soit $(E, \star)$ possédant un élément neutre e. On dit que $x \in E$ est symétrisable s'il existe un élément $x' \in E$ tel que $x \star x' = x' \star x = e$.

Exemple évident: l'élément neutre lui-même est symétrisable.

Si on considère $(\mathbb{Z}, \times)$, alors les seuls éléments symétrisables sont -1 et $+1$. Dans $(\mathbb{Q}, \times)$, l'ensemble des symétrisables est $\mathbb{Q}_* = \mathbb{Q} \setminus \{0\}$.

NB: Lorsque la loi est associative, le symétrique est unique (s'il existe). Dans le cas de la notation additive, on note le symétrique $x' = -x$, et dans le cas de la notation multiplicative, on le note x^{-1}.

Définition. Soit $(E, \star, \perp)$ un ensemble muni de deux lci. On dit que $\star$ est distributive (à gauche) par rapport à $\perp$ si pour tout $(x, y, z) \in E$, on a

$$x * (y \perp z) = (x * y) \perp (x * z) \,.$$

On définit de même la distributivité à droite, et on parle de distributivité si les deux ont lieu.

Exemple: $(\mathbb{N}, +, \times)$: la loi $\times$ est distributive par rapport à la loi $+$ (attention, l'inverse n'est pas vrai).

Exercice — Soit E un ensemble. Vérifier que $\cap$ et $\cup$ sont deux lci sur $\mathcal{P}(E)$, associatives, commutatives et distributives l'une par rapport à l'autre.

(g) Morphismes

La notion de morphisme est essentielle, elle permet de mettre en relation des ensembles a priori différents, mais dans lesquels les mécanismes de calculs sont relativement identiques.

Définition. Soient $(E, \star)$ et $(F, \perp)$ deux ensembles munis chacun d'une lci. On dit que $f : E \to F$ est un morphisme si pour tout $(x, y) \in E$,

$$f(x \star y) = f(x) \perp f(y)\,.$$

On dit qu'on a un isomorphisme si f est de plus bijectif, et on parle d'automorphisme quand on a un morphisme bijectif de $(E, \star)$ dans $(E, \star)$.

Un exemple typique est celui de la fonction exponentielle, en tant qu'application de $(\mathbb{R}, +)$ dans $(\mathbb{R}, \times)$ puisque

$$\exp(x + y) = \exp(x) \times \exp(y)\,.$$

Si on se restreint de la façon suivante: $\exp : \mathbb{R} \to]0, \infty[$, alors on a un isomorphisme.

Exercice: démontrer que la fonction $f(x) = 2x$ est un automorphisme de $(\mathbb{R}, +)$, de même que $f(x) = \sqrt{x}$.