B03. Ensembles, applications, relations, groupes

Bernard Le Stum
Université de Rennes 1

Version du 6 janvier 2006

Table des matières

Introduction

On admet les notions d'*ensemble* E et d'*élément* x de cet ensemble comme intuitives. On écrit $x \in E$ et on dit que x *appartient* à E ou que x *est élément de* E. Deux ensembles sont *égaux* s'ils ont les mêmes éléments. Enfin, si x n'appartient pas à E, on écrit $x \notin E$.

1 Calcul propositionnel

1.1 Vérité et mensonge

Définition 1.1.1 *Une* proposition *est un énoncé (mathématique) qui peut être vrai ou faux. On exprime ceci dans une* table de vérité *:*

P
V
F

où V et F désignent les valeurs de vérité*.*

Une proposition peut être a priori ni vraie ni fausse (*indécidable*) ou à la fois vraie et fausse (*contradiction*). Le curieux pourra lire le livre qui rend fou [1] de R. Smullyan. Nous éviterons d'entrer dans ces considérations métamathématique.

Définition 1.1.2 *La* négation *nonP d'une proposition P est la proposition qui est vraie lorsque P est fausse et fausse dans le cas contraire. On résume ceci dans la table de vérité*

P	$nonP$
V	F
F	V

.

Proposition 1.1.3 *La proposition non(nonP) a même vérité que la proposition P.*

1.2 Conjonction et disjonction

Définition 1.2.1 *La* conjonction *de deux propositions P et Q est la proposition $PetQ$ qui est vraie si P et Q sont toutes les deux vraies, et fausse dans le cas contraire. On résume ceci dans la table de vérité*

P	Q	$PetQ$
V	V	V
V	F	F
F	V	F
F	F	F

.

Proposition 1.2.2 *i) La proposition $PetQ$ et la proposition $QetP$ ont même vérité (*commutativité*).*

*ii) La proposition $Pet(QetR)$ et la proposition $(PetQ)etR$ ont même vérité (*associativité*). On écrit alors tout simplement $PetQetR$.*

Définition 1.2.3 *La* disjonction *de deux propositions P et Q est la proposition $PouQ$ qui est fausse si P et Q sont toutes les deux fausses et vraie dans le cas contraire. On résume ceci dans la table de vérité*

P	Q	$PouQ$
V	V	V
V	F	V
F	V	V
F	F	F

.

Proposition 1.2.4 *i) La proposition $non(PouQ)$ et la proposition $(nonP)et(nonQ)$ ont même vérité.*

ii) La proposition $non(PetQ)$ et la proposition $(nonP)ou(nonQ)$ ont même vérité.

Corollaire 1.2.5 *i) La proposition $PouQ$ et la proposition $QouP$ ont même vérité (*commutativité*).*

*ii) La proposition $Pou(QouR)$ et la proposition $(PouQ)ouR$ ont même vérité (*associativité*). On écrit alors tout simplement $PouQouR$.*

Proposition 1.2.6 *i) La proposition $Pet(QouR)$ et la proposition $(PetQ)ou(PetR)$ ont même vérité (*distributivité*).*

*ii) La proposition $Pou(QetR)$ et la proposition $(PouQ)et(PouR)$ ont même vérité (*distributivité*).*

1.3 Implication et équivalence

Définition 1.3.1 *L'* implication *de la proposition P vers la proposition Q est la proposition $P \Rightarrow Q$ qui est fausse lorsque P est vraie alors que Q est fausse. Et vraie dans le cas contraire : P fausse ou Q vraie. On résume ceci dans la table de vérité*

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

.

La contraposée *de l'implication $P \Rightarrow Q$ est l'implication $(nonQ) \Rightarrow (nonP)$.*

Au lieu de « $P \Rightarrow Q$ est vraie », on dit que « P implique Q »ou que « si P, alors Q ». On dit aussi « il suffit que P pour que Q »ou « il faut que Q pour que P ».

Proposition 1.3.2 *i) La proposition $P \Rightarrow Q$ et la proposition $(nonP)ouQ$ ont même vérité.*

ii) La proposition $non(P \Rightarrow Q)$ *et la proposition* $Pet(nonQ)$ *ont même vérité.*

iii) Une implication et sa contraposée ont même vérité (la proposition $P \Rightarrow Q$ *et la proposition* $(nonQ) \Rightarrow (nonP)$*).*

iv) La proposition $P \Rightarrow (QetR)$ *et la proposition* $(P \Rightarrow Q)et(P \Rightarrow R)$ *ont même vérité.*

v) La proposition $(PouQ) \Rightarrow R$ *et la proposition* $(P \Rightarrow R)et(Q \Rightarrow R)$ *ont même vérité.*

Définition 1.3.3 *L'* équivalence *des propositions* P *et* Q *est la proposition* $P \Leftrightarrow Q$ *qui est vraie si* P *et* Q *sont toutes les deux vraies ou toutes les deux fausses. Elle est fausse dans le cas contraire. On résume ceci dans la table de vérité*

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

.

Au lieu de « $P \Leftrightarrow Q$ est vraie », on dit que « P est équivalente à Q »ou que « P si et seulement si Q », ou encore que que « P est une condition nécessaire et suffisante pour que Q ». Cela signifie que P et Q ont même vérité. Dans la suite, on utilisera ce vocabulaire.

Proposition 1.3.4 *i) La proposition* $P \Leftrightarrow Q$ *et la proposition* $Q \Leftrightarrow P$ *sont équivalentes (*commutativité*).*

ii) La proposition $P \Leftrightarrow Q$ *et la proposition* $nonP \Leftrightarrow nonQ$ *sont équivalentes.*

iii) La proposition $P \Leftrightarrow Q$ *et la proposition* $(P \Rightarrow Q)et(Q \Rightarrow P)$ *sont équivalentes.*

1.4 Quantificateurs

Définition 1.4.1 *Soit* $P(x)$ *une proposition qui dépend d'une variable* x*. La proposition* $\forall x, P(x)$ *est vraie si* $P(x)$ *est vraie pour toute valeur de* x*. On dit que* $\forall$ *est le* quantificateur universel.

On écrira $\forall x \in E, P(x)$ au lieu de $\forall x, (x \in E \Rightarrow P(x))$.

Proposition 1.4.2 *i) Si* $P(x)$ *et* $Q(x)$ *sont deux propositions qui dépendent de* x*, les propositions* $\forall x, (P(x)etQ(x))$ *et* $(\forall x, P(x))et(\forall x, Q(x))$ *sont équivalentes. On écrira* $\forall x, P(x)etQ(x)$*.*

ii) Si $P(x, y)$ *est une proposition qui dépend de deux variables* x, y*, les propositions* $\forall x, \forall y, P(x, y)$ *et* $\forall y, \forall x, P(x, y)$ *sont équivalentes. On écrira* $\forall x, y, P(x, y)$*.*

Si $P(x)$ et $Q(x)$ sont deux propositions qui dépendent de x, les propositions $\forall x, (P(x) ou Q(x))$ et $(\forall x, P(x)) ou (\forall x, Q(x))$ ne sont pas équivalentes. Il se passe le même phénomène avec la conjonction et le quantificateur existentiel défini ci-dessous.

Définition 1.4.3 *Soit $P(x)$ une proposition qui dépend d'une variable x. La proposition $\exists x, P(x)$ est vraie si $P(x)$ est vraie pour au moins une valeur de x. On dit que $\exists$ est le* quantificateur existentiel. *S'il existe exactement un x qui satisfait $P(x)$, on écrit parfois $\exists! x, P(x)$.*

On écrira $\exists x \in E, P(x)$ au lieu de $\exists x, (x \in E et P(x))$.

Proposition 1.4.4 *Soit $P(x)$ une proposition qui dépend d'une variable x.*

i) Les propositions $non(\forall x, P(x))$ et $\exists x, non P(x)$ sont équivalentes.

ii) Les propositions $non(\exists x, P(x))$ et $\forall x, non P(x)$ sont équivalentes.

Proposition 1.4.5 *i) Si $P(x)$ et $Q(x)$ sont deux propositions qui dépendent de x, les propositions $\exists x, (P(x) ou Q(x))$ et $(\exists x, P(x)) ou (\exists x, Q(x))$ sont équivalentes. On écrira $\exists x, P(x) ou Q(x)$.*

ii) Si $P(x, y)$ est une proposition qui dépend de deux variables x, y, les propositions $\exists x, \exists y, P(x, y))$ et $\exists y, \exists x, P(x, y)$ sont équivalentes. On écrira $\exists x, y, P(x, y)$.

Attention, les propositions $\forall x, \exists y, P(x, y))$ et $\exists y, \forall x, P(x, y)$ ne sont pas équivalentes.

2 Ensembles

2.1 Ensemble et élément

Définition 2.1.1 *Si $E := \{a, b, \ldots\}$ est l'ensemble dont les éléments sont a, b, ..., on dit que E est défini en* extension. *Si $E := \{x, P(x)\}$ est l'ensemble des x qui satisfont la proposition P, on dit que E est défini en* compréhension.

Attention, la collection de tous les éléments satisfaisant une propriété donnée ne forme pas ncessairement un ensemble. Par exemple, le *paradoxe de Russell* consiste à considérer la proposition $x \notin x$ pour un ensemble x.

Définition 2.1.2 *On note $\emptyset$ l'*ensemble vide *qui ne contient aucun élément. Un ensemble à un élément est un* singleton. *Un ensemble à deux éléments (distincts) est une* paire.

2.2 Inclusion et complémentaire

Définition 2.2.1 *On dit que F est* contenu, *est une* partie, *est un* sous-ensemble *ou est* inclus *dans E et on écrit $F \subset E$ si tout élément de F est élément de E. Sinon, on écrit $F \not\subset E$. Enfin, l'ensemble de toutes les parties de E se note $\mathcal{P}(E)$.*

Proposition 2.2.2 *On a toujours*

i) $E \subset E$ *(*réflexivité*)*

ii) Si $F \subset E$ *et* $G \subset F$ *alors* $G \subset E$ *(*transitivité*)*

iii) $(E = F) \Leftrightarrow [(E \subset F)$ *et* $(F \subset E)]$ *(*antisymétrie*)*

Définition 2.2.3 *Si $F \subset E$, le* complémentaire *de F dans E est l'ensemble $\complement_E F$, aussi noté F^c lorsque le rôle de E est clair, des $x \in E$ tels que $x \notin F$.*

Proposition 2.2.4 *On a toujours*

i) $(F^c)^c = F$

ii) $F \subset G \Leftrightarrow G^c \subset F^c$

Le complémentaire d'un ensemble n'existe que relativement à un autre ensemble. En effet, la collection de tous les éléments qui n'appartiennent pas à un ensemble donné ne forment pas un ensemble. En fait, il résulte du paradoxe de Russell qu'il n'existe pas d'ensemble assez gros pour contenir tous les éléments qui existent.

2.3 Intersection, union et différence

Définition 2.3.1 *L'*intersection *de deux ensembles E et F est l'ensemble $E \cap F$ des éléments x qui sont à la fois dans E et dans F. On dit que deux ensembles E et F sont* disjoints *si $E \cap F = \emptyset$.*

Proposition 2.3.2 *On a toujours*

i) $E \cap F = F \cap E$ *(*commutativité*)*

ii) $E \cap (F \cap G) = (E \cap F) \cap G$ *(*associativité*). On écrit alors $E \cap F \cap G$.*

iii) $(E \subset F \cap G) \Leftrightarrow [(E \subset F)$ *et* $(E \subset G)]$

Définition 2.3.3 *L'*union *de de deux ensembles E et F est l'ensemble $E \cup F$ des éléments x qui sont dans E, dans F ou dans les deux à la fois.*

Proposition 2.3.4 *On a toujours*

i) $(F \cap G)^c = F^c \cup G^c$

ii) $(F \cup G)^c = F^c \cap G^c$

Corollaire 2.3.5 *On a toujours*

i) $E \cup F = F \cup E$ *(*commutativité*)*

ii) $E \cup (F \cup G) = (E \cup F) \cup G$ *(*associativité*). On écrit alors* $E \cup F \cup G$.

iii) $(E \cup F \subset G) \Leftrightarrow [(E \subset G)$ *et* $(F \subset G)]$.

Proposition 2.3.6 *On a toujours*

i) $E \cap (F \cup G) = (E \cap F) \cup (E \cap G)$ *(*distributivité*)*

ii) $E \cup (F \cap G) = (E \cup F) \cap (E \cup G)$ *(*distributivité*)*

Définition 2.3.7 *Si* E *et* F *sont deux ensembles, la* différence $E \setminus F$ *entre* E *et* F *est l'ensemble des éléments de* E *qui ne sont pas dans* F. *La* différence symétrique $E\Delta F$ *de* E *et* F *est* $(E \cup F) \setminus (E \cap F)$.

Proposition 2.3.8 *On a toujours*

i) $F \setminus G = F \cap G^c$.

ii) $E\Delta F = (E \setminus F) \cup (F \setminus E)$.

2.4 Partition et produit

Définition 2.4.1 *Une* partition P *d'un ensemble* E *est un ensemble de parties de* E *telles que*

1. $\forall p \in P, p \neq \emptyset$
2. $\forall p, q \in P, p \cap q = \emptyset$ *ou* $p = q$
3. $\forall x \in E, \exists p \in P, x \in p$

Définition 2.4.2 *Le couple* couple (a, b) *est l'ensemble* $\{\{a, b\}, a\}$.

Un couple est donc déterminé par ses éléments et leur ordre. Un couple est donc une suite de deux éléments (distincts ou non). En d'autres termes, il s'agit d'une « paire ordonnée ».

On peut définir de même un *triplet*, etc.

Définition 2.4.3 *Le* produit cartésien *de deux ensembles* E *et* F *est l'ensemble*

$$E \times F := \{(x, y), x \in E \text{ et } y \in F\}.$$

La diagonale *d'un ensemble* E *est*

$$\Delta := \{(x, x), x \in E\} \subset E \times E.$$

3 Relations

3.1 Généralités sur les relations

Définition 3.1.1 *Une* relation *ou* correspondance $\mathcal{R}$ *d'un ensemble* E *vers un ensemble* F *est un triplet*

$$\mathcal{R} := (E, F, \Gamma)$$

où Γ *est un sous ensemble de* $E \times F$*. On dit que* E *est la* source *ou l'*ensemble de départ*. On dit que* F *est le* but *ou l'*ensemble de d'arrivée*. Et enfin, on dit que* Γ *le* graphe *de* $\mathcal{R}$*. Si* $F = E$*, on dit que* $\mathcal{R}$ *est une relation dans* E*.*

Définition 3.1.2 *Soit* $\mathcal{R}$ *une relation de* E *vers* F *de graphe* Γ*. Si* $(x, y) \in \Gamma$*, on écrit* $x\mathcal{R}y$*. On dit que* y *est une* image *de* x *et que* x *est un* antécédent *de* y*. Le* domaine de définition *de* $\mathcal{R}$ *est l'ensemble* $\mathcal{D}_\mathcal{R}$ *de tous les antécédents. L'*image *de* $\mathcal{R}$ *est l'ensemble* $\operatorname{Im}\mathcal{R}$ *de toutes les images.*

Définition 3.1.3 *Soient* $\mathcal{R}$ *une relation de* E *vers* F *de graphe* Γ *et* $\mathcal{R}'$ *une relation de* E' *ves* F' *de graphe* Γ'*. Si* $E' \subset E$*,* $F' \subset F$ *et* $\Gamma \subset \Gamma'$*, on dit que* $\mathcal{R}'$ *est une* restriction *de* $\mathcal{R}$ *ou que* $\mathcal{R}$ *est un* prolongement *de* $\mathcal{R}'$*.*

Lorsque

$$\Gamma' = \Gamma \cap (E' \times F'),$$

on dit que $\mathcal{R}'$ *est la relation* induite *par* $\mathcal{R}$*. On dit aussi que c'est* la *restriction de* $\mathcal{R}$ *en une relation de* E' *vers* F'*. Dans ce cas, on a donc :*

$$\forall x \in E', y \in F', x\mathcal{R}'y \Leftrightarrow x\mathcal{R}y.$$

3.2 Composition, relation réciproque

Définition 3.2.1 *L'*identité *dans* E *est la relation*

$$x \ \mathrm{Id}_E \ y \Leftrightarrow x = y.$$

La relation réciproque *ou* inverse *de* $\mathcal{R}$ *est la relation* $\mathcal{R}^{-1}$ *de* F *vers* E *définie par*

$$y\mathcal{R}^{-1}x \Leftrightarrow x\mathcal{R}y.$$

Proposition 3.2.2 *1. On a toujours* $\left(\mathcal{R}^{-1}\right)^{-1} = \mathcal{R}$*.*

2. D'autre part, $ImR = \mathcal{D}_{\mathcal{R}^{-1}}$ *et* $\mathcal{D}_\mathcal{R} = ImR^{-1}$

Définition 3.2.3 *Si* $\mathcal{R}$ *est une relation de* E *vers* F *et* $\mathcal{S}$ *une relation de* F *vers* G*, la relation* composée $\mathcal{S} \circ \mathcal{R}$ *est définie par*

$$x(\mathcal{S} \circ \mathcal{R})z \Leftrightarrow \exists y \in F, x\mathcal{R}y \text{ et } y\mathcal{S}z.$$

Proposition 3.2.4 *On a toujours*

$$(\mathcal{T} \circ \mathcal{S}) \circ \mathcal{R} = \mathcal{T} \circ (\mathcal{S} \circ \mathcal{R}) \quad (\text{associativité})$$

et

$$(\mathcal{S} \circ \mathcal{R})^{-1} = \mathcal{R}^{-1} \circ \mathcal{S}^{-1}.$$

On n'a pas nécéssairement $\mathcal{R}^{-1} \circ \mathcal{R} = \mathrm{id}_E$ ni $\mathcal{R} \circ \mathcal{R}^{-1} = \mathrm{id}_F$.

3.3 Relation entre parties

Définition 3.3.1 *Soit $\mathcal{R}$ une relation de E vers F. Si $A \subset E$, alors*

$$\mathcal{R}(A) = \{y \in F, \exists x \in E, x\mathcal{R}y\} \subset F$$

*est l'*image *de A par R. On obtient ainsi une fonction*

$$\begin{array}{rccc} \mathcal{R}: & \mathcal{P}(E) & \to & \mathcal{P}(F) \\ & A & \mapsto & \mathcal{R}(A) \end{array}.$$

Au lieu d'« image par la relation inverse », on dit plus simplement image inverse *ou* image réciproque.

Proposition 3.3.2 *On a toujours*

1. *Si $A \subset B \subset E$, alors $\mathcal{R}(A) \subset \mathcal{R}(B)$.*
2. *Si $A, B \subset E$, alors*

$$\mathcal{R}(A \cup B) = \mathcal{R}(A) \cup \mathcal{R}(B)$$

et

$$\mathcal{R}(A \cap B) \subset \mathcal{R}(A) \cap \mathcal{R}(B).$$

On a pas toujours

$$\mathcal{R}(A \cap B) = \mathcal{R}(A) \cap \mathcal{R}(B).$$

Ni $\mathcal{R}^{-1}(\mathcal{R}(A)) \subset A$ ou $A \subset \mathcal{R}^{-1}(\mathcal{R}(A))$ d'ailleurs.

3.4 Relation dans un ensemble

Définition 3.4.1 *Une relation dans E est* réflexive *si,*

$$\forall x \in E, x\mathcal{R}x.$$

Elle est symétrique *si*

$$\forall x, y \in E, x\mathcal{R}y \Rightarrow y\mathcal{R}x.$$

Elle est antisymétrique *si*

$$\forall x, y \in E, (x\mathcal{R}y \text{ et } y\mathcal{R}x) \Rightarrow y = x.$$

Elle est transitive *si*

$$\forall x, y, z \in E, x\mathcal{R}y \text{ et } y\mathcal{R}x \Rightarrow x\mathcal{R}z.$$

Proposition 3.4.2 *1. Une relation $\mathcal{R}$ possède une de ces propriétés si et seulement si son inverse $\mathcal{R}^{-1}$ vérifie cette même propriété. En fait, $\mathcal{R}$ est symétrique si et seulement si $\mathcal{R}^{-1} = \mathcal{R}$.*

2. Si une relation $\mathcal{R}$ sur un ensemble E possède une de ces propriétés, la relation $\mathcal{R}'$ induite sur un sous ensemble E' vérifie la même propriété.

3.5 Relation d'équivalence

Définition 3.5.1 *Une relation d'*équivalence *est une relation réflexive, symétrique et transitive.*

Proposition 3.5.2 *1. Si $\mathcal{R}$ est une relation est une relation d'équivalence, alors $\mathcal{R}^{-1} = \mathcal{R}$.*

2. Si $\mathcal{R}$ est une relation d'équivalence, la restriction de $\mathcal{R}$ à un sous ensemble E' est aussi une relation d'équivalence.

Définition 3.5.3 *Si $\mathcal{R}$ est une relation d'équivalence dans E, la* classe *de $x \in E$ est l'ensemble*

$$\overline{x} = \{y \in E, x\mathcal{R}y\}.$$

On note $E/\mathcal{R}$ et on appelle ensemble quotient *de E par $\mathcal{R}$ l'ensemble des classes d'équivalence de $\mathcal{R}$.*

Lemme 3.5.4 *Soit $\mathcal{R}$ une relation d'équivalence dans un ensemble E. Alors*

1. $\forall x, y \in E, x\mathcal{R}y \Leftrightarrow \bar{x} = \bar{y}$
2. $\forall x \in E, \forall p \in E/\mathcal{R}, \quad x \in p \Leftrightarrow p = \bar{x}$.

Proposition 3.5.5 *Si $\mathcal{R}$ est une relation d'équivalence dans E, l'ensemble quotient $E/\mathcal{R}$ est une partition de E. Réciproquement, si P est une partition de E, la relation*

$$x\mathcal{R}y \Leftrightarrow \exists p \in P, x \in p \text{ et } y \in P$$

est une relation d'équivalence sur E et $E/\mathcal{R} = P$.

3.6 Relation d'ordre

Définition 3.6.1 *Une relation d'*ordre *est une relation réflexive, antisymétrique et transitive.*

Définition 3.6.2 *Une relation d'*ordre total *est une relation d'ordre $\mathcal{R}$ qui satisfait*

$$\forall x, y \in E, x\mathcal{R}y \text{ ou } y\mathcal{R}x.$$

Sinon, on dit ordre partiel.

Proposition 3.6.3 *1. Si $\mathcal{R}$ est une relation est une relation d'ordre (total), la relation inverse $\mathcal{R}^{-1}$ est aussi une relation d'ordre (total).*

2. Si $\mathcal{R}$ est une relation d'ordre (total), la restriction de $\mathcal{R}$ à un sous ensemble E' est aussi une relation d'ordre (total).

Définition 3.6.4 *Soit E un ensemble muni d'une relation d'ordre (partiel) $\mathcal{R}$. On dit que $M \in E$ est un* majorant *d'une partie F de E si*

$$\forall x \in F, x\mathcal{R}M.$$

On dit minorant *si cette proposition est satisfaite par la relation inverse.*

Proposition 3.6.5 *S'il existe dans E un majorant (resp. minorant) x de E tout entier, il est unique.*

Définition 3.6.6 *On dit alors que x est le* plus grand élément *(resp.* plus petit élément*) de E. Si F est une partie de E, on dit que $M \in E$ la* borne supérieure *(resp.* borne inférieure*) pour F si c'est le plus petit (resp. grand) des majorants (resp. minorants) de F dans E.*

4 Fonctions, applications

4.1 Fonctions

Définition 4.1.1 *Une relation f de E vers F est dite* fonctionelle *si tout $x \in E$ a au plus une image y dans F. On dit aussi que f est une* fonction *et on écrit alors $y = f(x)$ au lieu de xfy. On écrit aussi*

$$\begin{array}{rccc} f: & E & \to & F \\ & x & \mapsto & f(x) \end{array}.$$

Proposition 4.1.2 *Si $f : E \to F$ est une fonction et A une partie de E, l'image de A par f est*

$$f(A) = \{f(x), x \in A\}.$$

De même, si B est une partie de F, l'image réciproque de B par f est

$$f^{-1}(B) = \{x \in E, f(x) \in B\}.$$

Proposition 4.1.3 *1. La composée de la fonction $f : E \to F$ et de la fonction $g : F \to G$ est la fonction*

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

2. Toute restriction d'une fonction reste une fonction.

4.2 Applications

Définition 4.2.1 *Une fonction f est une* application *si tout élément de E à (au moins et donc exactement) une image dans F. On note F^E ou $\mathcal{F}(E,F)$ l'ensemble de toutes les applications de E dans F.*

Une fonction f est une application si et seulement si son domaine de définition est E tout entier.

Proposition 4.2.2 *1. La composée de deux applications est une application.*

2. Si $f : E \to F$ est une fonction et $E' \subset \mathcal{D}_f$, la fonction induite par f sur E' est une application.

On peut alors faire les remarques suivantes :

1. La réciproque d'une application n'est pas une application en général, ce n'est même pas une fonction.
2. Par contre, toute relation $\mathcal{R}$ d'un ensemble E vers un ensemble F fournit une application
$$\begin{array}{rccc} \mathcal{R}: & \mathcal{P}(E) & \to & \mathcal{P}(F) \\ & A & \mapsto & \mathcal{R}(A) \end{array}.$$
Cela s'applique en particulier à une application $f : E \to F$ qui va fournir
$$\begin{array}{rccc} f: & \mathcal{P}(E) & \to & \mathcal{P}(F) \\ & A & \mapsto & f(A) \end{array} \quad \text{et} \quad \begin{array}{rccc} f^{-1}: & \mathcal{P}(F) & \to & \mathcal{P}(E) \\ & B & \mapsto & f^{-1}(B) \end{array}.$$

Proposition 4.2.3 *Soit $f : E \to F$ une application.*

1. Soient A et B deux parties de E. Alors,

(a) Si $A \subset B$, on a $f(A) \subset f(B)$

(b) On a toujours
$$f(A \cup B) = f(A) \cup f(B)$$

(c) On a toujours
$$f(A \cap B) \subset f(A) \cap f(B.)$$

2. Soient A et B deux parties de F. Alors,

(a) Si $A \subset B$, alors $f^{-1}(A) \subset f^{-1}(B)$.

(b) On a toujours
$$f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$$

(c) On a toujours
$$f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B).$$

3. (a) Si A est une partie de E, on a $A \subset f^{-1}(f(A))$.

(b) Si B est une partie de f, on a $f(f^{-1}(B)) \subset B$.

Définition 4.2.4 *Une* famille *d'éléments d'un ensemble E indexée par un ensemble I est une application*

$$\begin{array}{ccc} I & \to & E \\ i & \mapsto & x_i \end{array} .$$

On la note $(x_i)_{i\in I}$.

Enfin, une suite *est une famille indexée par* $\mathbf{N}$.

On peut définir l'*intersection* $\cap_{i\in I} E_i$ d'une famille d'ensembles ou leur l'*union* $\cup_{i\in I} E_i$. On peut aussi définir leur *produit* $\prod_{i\in I} E_i$.

4.3 Application injective, surjective, bijective

Définition 4.3.1 *Une application $f : E \to F$ est* injective *si tout élément de F a au plus un antécédent :*

$$\forall x, y \in E, f(x) = f(y) \Rightarrow x = y$$

Elle est surjective *si tout élément de F à au moins un antécédent dans E :*

$$\forall y \in F, \exists x \in E, f(x) = y$$

Elle est bijective *si elle est à la fois injective et surjective (tout élément de F a exactement un antécédent dans E).*

On peut faire les remarques suivantes :

1. Une application est injective si et seulement si la relation réciproque est une fonction.
2. Une application est surjective si et seulement si son image est son ensemble d'arrivée.
3. Une application est bijective si et seulement si la relation réciproque est une application.

Proposition 4.3.2 *1. Si $f : E \to F$ et $g : F \to G$ sont deux applications injectives, surjectives ou bijectives, alors $g \circ f : E \to G$ l'est aussi.*

2. Une application $f : E \to F$ est bijective si et seulement s'il existe une application $g : F \to E$ telle que $g \circ f = \mathrm{Id}_E$ et $f \circ g = \mathrm{Id}_E$. On a alors $g = f^{-1}$.

Si $f : E \to F$ et $g : F \to G$ sont deux applications avec $g \circ f : E \to G$ injective, alors f est aussi injective. De même, si $g \circ f$ est surjective, alors g est surjective.

4.4 Projections et quotient

Définition 4.4.1 *Si E et F sont deux ensemblers, les applications*

$$E \times F \to E, (x, y) \longmapsto x$$

et

$$E \times F \to F, (x, y) \longmapsto y$$

sont respectivement la première et la seconde projection.

Définition 4.4.2 *Si E est un ensemble muni d'une relation d'équivalence $\sim$, alors l'application*

$$\begin{array}{rccc} \pi : & E & \to & E/\sim \\ & x & \mapsto & \bar{x} \end{array}$$

*est l'*application quotient.

Proposition 4.4.3 *Soit E ensemble muni d'une relation d'équivalence $\sim$ et $\pi : E \to E/\sim$ l'application quotient. On a alors pour $x, y \in E$,*

$$x \sim y \Leftrightarrow \pi(x) = \pi(y).$$

Réciproquement, si $f : E \to F$ est une application quelconque, on a une relation d'équivalence sur E définie par

$$x \sim y \Leftrightarrow f(x) = f(y).$$

4.5 Cardinaux

Définition 4.5.1 *S'il existe une bijection entre deux ensembles, on dit qu'ils ont même* cardinal *ou qu'ils sont* équipotents. *On dit qu'un ensemble est* fini à n éléments, *s'il est équipotent à $\{1, 2, \ldots, n\}$. Sinon, on dit qu'il est infini. Un ensemble est* dénombrable *s'il est équipotent à $\mathbf{N}$. Un ensemble a la* puissance du continu *s'il s'il est équipotent à $\mathbf{R}$.*

Par convention, $\{1, 2, \ldots, n\} = \emptyset$ pour $n = 0$.

Théorème 4.5.2 *(Cantor) Si E est un ensemble, alors E et $\mathcal{P}(E)$ ne sont pas équipotents.*

Corollaire 4.5.3 *Un ensemble qui a la puissance du continu n'est pas dénombrable.*

5 Lois de composition

5.1 Associativité, commutativité

Définition 5.1.1 *Une* loi de composition *est une application*

$$E \times F \to G, (x, y) \longmapsto x * y$$

Si $E = F = G$, on dit que c'est une loi de composition interne *dans E. Une loi de composition se note souvent multiplicativement $(x, y) \mapsto xy$.*

Définition 5.1.2 *Une loi de composition interne sur un ensemble E est* associative *si*

$$\forall x, y, z \in E, \quad (x * y) * z = x * (y * z)$$

et on écrit alors $x * y * z$.

Définition 5.1.3 *Une loi de composition interne sur un ensemble E est* commutative *si*

$$\forall x, y \in E, \quad x * y = y * x.$$

5.2 Élément neutre, symétrique

Définition 5.2.1 *Soit E un ensemble muni d'une loi de composition interne. On dit que $e \in E$ est un* élément neutre *si*

$$\forall x \in E, \quad e * x = x * e = x.$$

On parle d' unité*, et on écrit* 1*, lorsque la loi est notée multiplicativement. On parle de* zéro*, et on écrit* 0*, lorsque la loi est commutative et notée additivement.*

Proposition 5.2.2 *Un élément neutre s'il existe est unique.*

Proposition 5.2.3 *Soit E un ensemble muni d'une loi de composition interne avec élément neutre e. On dit que $x' \in E$ est un* symétrique *pour $x \in E$ si $x * x' = x' * x = e$.*

*Lorsque la loi est notée multiplicativement, on parle d'*inverse x^{-1} *de x. Lorsque la loi est commutative et notée additivement on parle d'*opposé $-x$ *de x.*

Proposition 5.2.4 *L'élément x' s'il existe, est alors unique.*

Proposition 5.2.5 *Soit E un ensemble muni d'une loi de composition interne avec élément neutre e.*

1. *Si $x \in E$ possède un symétrique x', alors x' possède aussi un symétrique et c'est x.*
2. *Si $x, y \in E$ possèdent tous deux des symétriques x' et y', alors $x * y$ possède aussi un symétrique et c'est $(y' * x')$.*

Définition 5.2.6 *Soit E un ensemble muni d'une loi de composition interne commutative, associative et unitaire notée multiplicativement. Si y est inversible on définit le* quotient $x/y := xy^{-1}$. *Lorsque la loi est commutative et notée additivement, on parle de la* différence *et on écrit $x - y := x + (-y)$.*

5.3 Itéré d'un élément

Définition 5.3.1 *Soit E un ensemble muni d'une loi de composition interne associative et avec élément neutre e. Le n-ème* itéré *de x est définie par récurrence par*

$$x^{*0} = e \quad et \quad x^{*n} = x^{*(n-1)} * x.$$

Si $x \in E$ est inversible et si $n \in \mathbf{N}$, on pose $x^{*(-n)} = (x')^{*n}$.

Si la loi est notée multiplicativement, on parle de puissance x^n *de x. Si la loi est commutative et notée additivement, on parle de* multiple nx *de x.*

Proposition 5.3.2 *Soit E un ensemble muni d'une loi de composition interne associative et avec élément neutre. Si $m, n \in \mathbf{N}$ et $x \in E$, alors*

$$x^{*(m+n)} = x^{*m} x^{*n}$$

et

$$x^{*mn} = (x^{*m})^{*n}.$$

Si $m, n \in \mathbf{Z}$ et $x \in E$ est inversible, les mêmes égalités sont toujours vraies.

Proposition 5.3.3 *Si E est un ensemble muni d'une loi de composition interne commutative, associative et unitaire, on a*

$$\forall x, y \in E, n \in \mathbf{N}, \quad (xy)^{*n} = x^{*n} y^{*n}.$$

Dans le cas ou x et y sont inversibles, ces égalités sont toujours valides pour $n \in \mathbf{Z}$.

6 Groupes

6.1 Groupes et sous-groupes

Définition 6.1.1 *Un* groupe *est un ensemble G muni d'une loi interne associative $*$ possédant un élément neutre e_G et telle que tout élément possède un symétrique.*

Un groupe dont la loi est commutative est un groupe commutatif *ou* abélien.

Proposition 6.1.2 *Dans un groupe $(G, *)$, on a*

$$\forall x, y, z \in G, \quad x * y = x * z \Rightarrow y = z$$

et

$$\forall x, y, z \in G, \quad x * z = y * z \Rightarrow x = y$$

Définition 6.1.3 *Un* sous groupe *d'un groupe $(G, *)$ est un sous ensemble H de G tel que*

1. $\forall x, y \in H, \quad x * y \in H$
2. $e_G \in H$
3. $\forall x \in H, \quad x' \in H$

Proposition 6.1.4 *Soit $(G, *)$ un groupe.*

1. *Pour qu'une partie non vide H d'un groupe G soit un sous-groupe, il faut et suffit que*
$$\forall x, y \in H, \quad x * y' \in H$$
2. *Si H est un sous groupe du G, la loi de G induit sur H une structure de groupe.*
3. *Un sous groupe d'un groupe commutatif est commutatif.*

6.2 Sous-groupe engendré

Proposition 6.2.1 *Toute intersection de sous-groupes est un sous-groupe.*

Corollaire 6.2.2 *Il existe un plus petit sous groupe H contenant une partie donnée S d'un groupe G, c'est l'intersection de tous les sous-groupes de G contenant S.*

Définition 6.2.3 *On dit alors que H est le* sous-groupe engendré *par S ou que S est un* ensemble de générateurs *de H.*

Définition 6.2.4 *Un groupe est* cyclique *(ou* monogène*) s'il est engendré par un seul élément.*

Proposition 6.2.5 *Un groupe $(G, *)$ est cylcique engendré par x si et seulement si G est l'ensemble des itérés de x. Plus précisément, G est infini si et seulement si tous les itérés de x sont distincts. Dans le cas contraire, si G a n éléments, alors*

$$G = \{e, x, x^{*2}, \ldots, x^{*(n-1)}\}.$$

et $x^{*n} = e$.

Définition 6.2.6 *L'ordre d'un groupe est nombre d'éléments (fini ou infini) de ce groupe. L'ordre d'un élément d'un groupe est l'ordre du sous-groupe engendré.*

6.3 Permutations

Proposition 6.3.1 *Si E est un ensemble, l'ensemble $\mathcal{S}(E)$ des bijections de E vers E est un groupe pour $\circ$.*

Définition 6.3.2 *On dit que $\mathcal{S}_n := \mathcal{S}(\{1,\dots,n\})$ est le* groupe symétrique *ou groupe des* permutations. *Le* support *de $\sigma \in \mathcal{S}_n$ est $\{i, \sigma(i) \neq i\}$. Étant donnés $i_1,\dots,i_k \in \{1,\dots,n\}$ tous distincts, on définit le* cycle $(i_1 \cdots i_k)$ *comme la permutation σ de support $\{i_1,\dots,i_k\}$ définie par*

$$\begin{cases} \sigma(i_1) & = & i_2 \\ \sigma(i_2) & = & i_3 \\ \vdots & = & \vdots \\ \sigma(i_{k-1}) & = & i_k \\ \sigma(i_k) & = & i_1 \end{cases}$$

On dit que k est la longueur *du cycle. Un cycle de longueur 2 est une* transposition. *On dit que 2 cycles sont* disjoints *si leurs supports le sont.*

Proposition 6.3.3 *Toute permutation s'écrit de manière unique comme produit de cycles disjoints.*

Corollaire 6.3.4 *$\mathcal{S}_n$ est engendré par les transpositions.*

6.4 Quotient de groupes

Proposition 6.4.1 *Si H est un sous-groupe de G, alors la relation*

$$x \sim y \Leftrightarrow \exists z \in H, y = xz$$

est une relation d'équivalence sur G.

Définition 6.4.2 *La classe de $x \in G$ pour cette relation se note xH et s'appelle la* classe (à gauche) de x modulo H. *L'ensemble quotient se note G/H.*

Théorème 6.4.3 *(de Lagrange) L'ordre d'un sous-groupe divise l'ordre du groupe. En particulier, l'ordre d'un élément divise l'ordre du groupe.*

Index

Références

[1] Raymond Smullyan. *Le livre qui rend fou.* Dunod, 1984.