Théorie des ensembles

Cours de licence d'informatique
Saint-Etienne — 2002/2003

Bruno Deschamps

Contents

1 Eléments de théorie des ensembles

1.1 Introduction au calcul propositionnel

On note $A, B, C \cdots$ des propositions élémentaires qui prennent la valeur 0 (faux) ou 1 vrai et l'on forme de nouvelles propositions à partir des connecteurs suivants : non, et, ou, implique, équivaut. On leur affecte alors une vérité d'après les tables de vérité ci-après et la valeur prise par les propositions intervenant dans la proposition étudiée.

• Négation.

• Conjonction.

• Disjonction.

• Implication.

• Equivalence.

Définition.— *On appelle tautologie toute proposition qui ne prend que la valeur* 1 *quelle que soit la valeur des propositions élémentaires qu'elle contient.*

Théorème.— *Soit P et Q deux propositions ayants les même propositions élémentaires. Alors P et Q ont même table de vérité ssi $P \Longleftrightarrow Q$ est une tautologie.*

Théorème.— *Toute proposition du calcul propositionnel équivaut à une conjonction de disjonctions (et à une disjonction de conjonctions) de propositions élémentaires.*

1.2 Ensembles

1.2.1 Généralités

• On appelle *ensemble* une collection d'objets assujétie à certaines contraintes que nous n'énoncerons pas ici. Les objets de cette collection s'appelle les éléments de l'ensemble. Si E est un ensemble et si $\cdots$ sont ses éléments, on note alors $E = \{\cdots\}$ ou alors on représente E par une patate (ce qui est plus visuel, car l'ordre d'énumération des éléments d'un ensemble n'a aucune importance).

• L'ensemble qui ne contient aucun élément est appellé *l'ensemble vide* et est noté $\emptyset$ ou parfois $\{\}$. On remarquera bien que $E = \{\emptyset\}$ n'est pas l'ensemble vide puisqu'il contient un élément.

• Si E est un ensemble et si x est un objet, on écrira $x \in E$ pour symboliser le fait que x est élément de E, et on écrira $x \notin E$ pour symboliser le fait que x n'est pas élément de E.

• Si E est un ensemble et si P désigne une propriété pourtant sur les éléments de l'ensemble E, on écrira

$$\forall x \in E \ P(x)$$

pour dire "pour tout x la propriété $P(x)$" de même, on écrira

$$\exists x \in E \ P(x)$$

pour dire "il existe x tel que la propriété $P(x)$".

Définition.— *Soit A et B deux ensembles. Si tout élément de A est un élément de B, on dit que A est un sous-ensemble de B et l'on note $A \subset B$.*

$$i.e. \ A \subset B \Longleftrightarrow \forall x \in A, \ x \in B$$

On dit que deux ensembles A et B sont égaux et l'on note $A = B$ si $A \subset B$ et $B \subset A$.
Si $A \subset B$ et $A \neq B$ on parle d'inclusion stricte et l'on note ???

Exemple: Soit $E = \{x, y, \{x, y\}\}$ et $A = \{x, y\}$. On a alors à la fois $x \in A$ et $X \subset A$.

Définition.— *Soient A et B deux ensembles. On appelle réunion de A et de B l'ensemble, noté $A \cup B$, constitué des éléments appartenant à A ou à B*

$$i.e.\ x \in A \cup B \Longleftrightarrow x \in A \text{ ou } x \in B$$

De même, On appelle intersection de A et de B l'ensemble, noté $A \cap B$, constitué des éléments appartenant à A et à B

$$i.e.\ x \in A \cap B \Longleftrightarrow x \in A \text{ et } x \in B$$

Proposition.— *Soit A, B, C trois ensembles. On a*

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

et

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

Définition.— *Soit E un ensemble et A un sous-ensemble de E. On appelle complémentaire de A dans E l'ensemble, noté $\mathcal{C}_E A$, constitué des éléments de E qui n'appartiennent pas à A.*

Proposition.— *Soit E un ensemble et A, B des sous-ensembles de E. On a:*

- $\mathcal{C}_E(\mathcal{C}_E A) = A$,
- *si* $A \subset B$ *alors* $\mathcal{C}_E B \subset \mathcal{C}_E A$,
- $\mathcal{C}_E(A \cup B) = (\mathcal{C}_E A) \cap (\mathcal{C}_E A)$,
- $\mathcal{C}_E(A \cap B) = (\mathcal{C}_E A) \cup (\mathcal{C}_E A)$.

Définition.— *Soient E et F deux ensembles. on appelle différence de E par F l'ensemble, noté $E - F$, constitué des éléments de E qui ne sont pas éléments de F.*

Exemple: Soient $5\mathbb{N} = \{0, 5, 10, \cdots\}$ l'ensemble des entiers multiples de 5 et $3\mathbb{N} = \{0, 3, 6, \cdots\}$ l'ensemble des entiers multiples de 3. L'ensemble $5\mathbb{N} - 3\mathbb{N}$ est donc constitué des entiers multiples de 5 qui ne sont pas multiples de 3. Or, les entiers multiples de 5 et multiples de 3 sont exactement les entiers multiples de 15. On en déduit donc que :

$$5\mathbb{N} - 3\mathbb{N} = \mathcal{C}_{5\mathbb{N}} 15\mathbb{N} = \{5, 10, 20, 25, 35, \cdots\}$$

Proposition.— *Soient E, F, G trois ensembles. On a*

- $E - F = \mathcal{C}_E E \cap F = \mathcal{C}_{E \cup F} F$,
- $E - (F \cup G) = ((E \cup G) - F) \cap ((E \cup F) - G)$,
- $E - (F \cup G) = (E - F) \cap (E - G)$,
- $E - (F \cap G) = (E - F) \cup (E - G)$.

1.2.2 Ensemble des parties

Définition.— *Soient E un ensemble. On appelle ensemble des parties de E l'ensemble, noté $\mathcal{P}(E)$ constitué des sous-ensembles de E.*

On remarquera bien que les éléments de $\mathcal{P}(E)$ sont des ensembles.

Exemples: Si $E = \{x, y\}$ alors

$$\mathcal{P}(E) = \{\emptyset, \{x\}, \{y\}, E\}$$

On a

$$\mathcal{P}(\emptyset) = \{\emptyset\}$$

de même,

$$\mathcal{P}(\mathcal{P}(\emptyset)) = \{\emptyset, \{\emptyset\}\}$$

1.2.3 Produit cartésien

Définition.— *Soit A et B deux ensembles, on appelle couple (ou paire ordonnée) d'élément de A et de B tout ensemble de la forme $\{a, \{a, b\}\}$ avec $a \in A$ et $b \in B$. Un tel ensemble se note alors (a, b). L'ensemble constitué des couples d'éléments de A et de B s'appelle le produit cartésien de A par B et se note $A \times B$.*

Il faut bien remarquer que $(a, b) \neq (b, a)$ le plus souvent. En fait :

Proposition.— *Soient A et B deux ensembles et (a, b) et (c, d) deux éléments de $A \times B$. Les propositions suivantes sont équivalentes:*

i) $(a, b) = (c, d)$,

ii) $a = c$ *et* $b = d$.

Proposition.— *Soit A, B, C trois ensembles. On a:*

- $A \times (B \cup C) = A \times B \cup A \times C$,
- $A \times (B \cap C) = A \times B \cap A \times C$.

Remarque: Si $E_1, \cdots, E_n$ sont des ensembles, on définit par récurrence le produit cartésien $E_1 \times \cdots \times E_n$ des ensembles $E_1, \cdots, E_n$, par la relation

$$E_1 \times \cdots \times E_n = (E_1 \times \cdots \times E_{n-1}) \times E_n$$

Les éléments de $E_1 \times \cdots \times E_n$ sont alors appellés des n-uplets et notés $(x_1, \cdots, x_n)$ avec $x_i \in E_i$ pour tout $i = 1, \cdots, n$. On a alors

Proposition.— *Soient $E_1, \cdots, E_n$ des ensembles et $(x_1, \cdots, x_n)$ et $(y_1, \cdots, y_n)$ deux éléments de $E_1 \times \cdots \times E_n$. Les propositions suivantes sont équivalentes:*

i) $(x_1, \cdots, x_n) = (y_1, \cdots, y_n)$,

ii) $x_i = y_i$ *pour tout* $i = 1, \cdots n$.

1.3 Applications

1.3.1 Généralités

Définition.— *Soit E et F deux ensembles. On appelle graphe (ou graphe fonctionnel) de $E \times F$ toute partie $X \subset E \times F$ vérifiant :*

$$\forall (a, b) \in X,\ \forall (a^{'}, b^{'}) \in X,\ a = a^{'} \Longrightarrow b = b^{'}$$

Exemple: Pour $E = F$,

• $X = \emptyset$,

• $X = \{(a, a)/\ a \in E\}$

Définition.— *On appelle fonction la donnée d'un triplet (E, X, F) où E et F sont des ensembles et X un graphe de $E \times F$. On note $f = (E, X, F)$ ou plus classiquement $f : E \to F$ une fonction. L'ensemble E s'appelle l'ensemble de départ de f, l'ensemble F s'appelle l'ensemble d'arrivé de f, et X s'appelle de graphe de f. On dit alors que f est une fonction de E dans F de graphe X.*

Si $(x, y) \in X$, on note alors $y = f(x)$.

Si $f = (E, X, F)$ est une fonction, on appelle ensemble de définition de f le sous-ensemble A de E constitué des éléments $a \in E$ tel qu'il existe $b \in F$ vérifiant $(a, b) \in X$.

On dit qu'une fonction $f = (E, X, F)$ est totale et on parle alors d'application, si le domaine de définition de f est E.

Lemme.— *Soit E et F deux ensembles et X un graphe fonctionnel de $E \times F$. Soit $U \subset E$. L'ensemble*

$$X_U = \{(a, b) \in X/\ a \in U\}$$

est un graphe fonctionnel de $U \times F$.

Définition.— *Soit $f : E \longrightarrow F$ une fonction, X sont graphe et $U \subset E$. La fonction de U dans F de graphe X_U s'appelle la restricion de f à U et se note $f_{|U}$ (c'est une fonction). En particulier, si A est le domaine de définition de f, alors $f_{|A}$ est une application.*

Notation : Si E et F sont deux ensembles, on note $\mathcal{F}(E, F)$ l'ensemble des applications de E dans F.

Exemples: • Si E est un ensemble et $X = \{(a, a) \in E \times E,\ a \in E\}$, l'application $f = (E, X, E)$ s'appelle l'*application identité de E* et se note Id_E.

• Si $E \subset F$ sont deux ensembles et $X = \{(a, a) \in E \times F,\ a \in E\}$, l'application $f = (E, X, F)$ s'appelle l'*injection canonique de E dans F*. Dans le cas où $E = F$ il s'agit alors de Id_E.

Définition.— *Soit E, F, G trois ensembles, X_1 un graphe fonctionnel de $E \times F$ et X_2 un graphe fonctionnel de $F \times G$. On appelle graphe composé de X_1 et X_2 l'ensemble*

$$X = \{(a, b) \in E \times G/\ \exists c \in F,\ (a, c) \in X_1 \text{ et } (c, b) \in X_2\}$$

(C'est un graphe fonctionnel de $E \times G$)

Proposition.— *Si $f : E \to F$ est une application de E dans F de graphe X_1 et $g : F \to G$ est une application de F dans G de graphe X_2, le graphe composé de X_1 et X_2 est le graphe X d'une application de E dans G.*

Définition.— *Avec les notation précédente, l'application (E, X, G) s'appelle la composée de f et g et se note $g \circ f$.*

Proposition.— *Soient $f : E \to F$, $g : F \to G$, $h : G \to H$ sont trois applications. Les deux applications $(h \circ g) \circ f$ et $h \circ (g \circ f)$ sont identique (i.e. ont même graphe).*

Remarque: La loi $\circ$ est donc associative. Dans $\mathcal{F}(E, F)$ elle est rarement associative. Par exemple si $f, g : \mathbb{R} \to \mathbb{R}$ sont définie par, $f(x) = x + 1$ et $g(x) = x^2$; on a alors $f \circ g(x) = x^2 + 1$ et $g \circ f(x) = (x + 1)^2$.

1.3.2 Image directe et réciproque

Définition.— *Soit $f : E \to F$ une application. Pour toute partie $A \subset E$, on appelle image directe de A par f l'ensemble*

$$f(A) = \{y \in F/\ \exists x \in A,\ f(x) = y\}$$

et pour tout partie B de F, on appelle image réciproque de B par f l'ensemble

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

Exemple: Soit $f : \mathbb{R} \to \mathbb{R}$ définie par $f(x) = x^2$. Soit $B = [1, 2]$, on a alors

$$f^{-1}(B) = [-\sqrt{2}, -1] \cup [1, \sqrt{2}]$$

Soit maintenant $A = [1, \sqrt{2}]$, on a $f(A) = [1, 2] = B$. On remarqu'alors $f^{-1}(f(A)) \neq A$.

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

1/ $\forall A, B \subset F$, $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$ et $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$.

2/ $\forall A, B \subset E$, $f(A \cap B) \subset f(A) \cap f(B)$ et $f(A \cup B) = f(A) \cup f(B)$.

3/ $\forall B \subset F$, $f(f^{-1}(B)) \subset B$.

4/ $\forall A \subset E$, $A \subset f^{-1}(f(A))$.

5/ $\forall B \subset F$, $f^{-1}(\mathcal{C}_F B) = \mathcal{C}_E f^{-1}(B)$.

Remarque: Si $A \subset E$ alors $f(\mathcal{C}_E A)$ et $\mathcal{C}_F f(A)$ sont des ensembles incomparables.

1.3.3 Injectivité, surjectivité, bijectivité

Définition.— *Soit $f : E \to F$ une application. On dit que f est :*

- *injective si $\forall x, y \in E$, $f(x) = f(y) \Rightarrow x = y$,*
- *surjective si $\forall y \in F$, $\exists x \in E$, $f(x) = y$,*
- *bijective si $\forall y \in F$, $\exists! x \in E$, $f(x) = y$.*

Lemme.— *Soit $f : E \to F$ une application. Les propositions suivantes sont équivalentes:*

i) f est bijective,

ii) f est injective et surjective.

Proposition.— *Soit $f : E \to F$ et $g : F \to G$ deux applications. On a alors*

$$g \circ f \text{ injective} \Longrightarrow f \text{ injective}$$

et

$$g \circ f \text{ surjective} \Longrightarrow g \text{ surjective}$$

Proposition.— *Soient $f : E \to F$ et $g : F \to G$ deux applications. Si f et g sont injectives (resp. surjectives) alors $g \circ f$ est injective (resp. surjective).*

Proposition.— *Soit $f : E \to F$ une application. Si f est bijective, alors il existe une unique application $g : F \to E$ telle que*

$$g \circ f = Id_E \text{ et } f \circ g = Id_F$$

Cette application s'appelle la réciproque (ou l'inverse) de f et se note f^{-1}. On a alors:

1/ f^{-1} est bijective,

2/ $(f^{-1})^{-1} = f$.

Remarque: Il ne faut pas confondre f^{-1} "application réciproque" et f^{-1} "image inverse".

Proposition.— *Soient $f : E \to F$ et $g : F \to E$ deux applications telles que $g \circ f = Id_E$ et $f \circ g = Id_F$. Les applications f et g sont bijectives et $f^{-1} = g$ et $g^{-1} = f$.*

Remarque: Si seulement une seule des égalités $g \circ f = Id_E$ et $f \circ g = Id_F$ est vérifiée, on ne peux rien dire. En effet, soit $f, g : \mathbb{N} \to \mathbb{N}$ définies par, $f(n) = 2n$ et $g(n) = E(n/2)$. On a alors $g \circ f = Id_{\mathbb{N}}$ et pourtant, f n'est pas surjective et g n'est pas injective.

Proposition.— *Soient $f : E \to F$ et $g : F \to G$ deux applications. Si f et g sont bijectives alors $g \circ f$ est bijective et $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.*

Définition.— *Soit $f : E \to E$ une application. On dit que f est une involution de E si $f \circ f = Id_E$.*

Définition.— *Soit $f : E \to E$ une application. Les proposition suivantes sont équivalentes :*

i) f est involutive,

ii) f est bijective et $f^{-1} = f$.

1.3.4 Caractérisation de l'injectivité et de la surjectivité

Proposition.— *Soit $f : E \to F$ une application. Les propositions suivantes sont équivalentes :*

i) f est injective,

ii) $\forall A, B \subset E$, $f(A \cap B) = f(A) \cap f(B)$,

iii) $\forall A \subset E$, $f^{-1}(f(A)) = A$.

Proposition.— *Soit $f : E \to F$ une application. Les propositions suivantes sont équivalentes :*

i) f est surjective,

ii) $\forall B \subset F$, $f(f^{-1}(B)) = B$.

1.4 Relations binaires

1.4.1 Généralités

Définition.— *Soient A et B deux ensembles. On appelle relation binaire de A vers B toute partie de $A \times B$. Si $\mathcal{R}$ est une relation binaire de A vers B et si $(a, b) \in \mathcal{R}$, on note alors $a\mathcal{R}b$ ou $\mathcal{R}(a, b)$. On appelle relation binaire sur un ensemble E, toute relation binaire de E dans E.*

Exemples: •

• $E = \mathbb{R}$ et $x\mathcal{R}y \iff x \leq y$.

• E ensemble et $\mathcal{R} = \emptyset$.

• E et F deux ensembles et $f : E \to F$. Le graphe de f est une relation binaire, on a alors $x\mathcal{R}y \iff y = f(x)$. Réciproquement,...

Graphe d'une relation binaire sur un ensemble:

Notations: • La relation binaire sur un ensemble E $\{(x,x),\ x \in E$ se note Id_E.

• Si $\mathcal{R}$ est une relation binaire sur un ensemble E, on note

• $\overline{\mathcal{R}} = \{(x,y) \in E \times E/\ (x,y) \notin \mathcal{R}\}$ (i.e. $\overline{\mathcal{R}} = \mathcal{C}_{E\times E}\mathcal{R}$),

• $\mathcal{R}^{-1} = \{(y,x) \in E \times E/\ (x,y) \in \mathcal{R}\}$

• $\mathcal{R}^0 = Id_E$, $\mathcal{R}^1 = \mathcal{R}$.

Définition.— *Soit $\mathcal{R}$ et $\mathcal{T}$ deux relations binaires sur un ensemble E. On note:*

$$\mathcal{R} \circ \mathcal{T} = \{(x,y) \in E \times E/\ existez \in E,\ x\mathcal{R}z \text{ et } z\mathcal{T}y\}$$

Définition.— *Soit e un ensemble et $\mathcal{R}$ une relation binaire sur E. On dit que $\mathcal{R}$ est :*

• *reflexive si $\forall a \in E$, $a\mathcal{R}a$ (i.e. $Id_E \subset \mathcal{R}$,*

• *symétrique si $\forall a, b \in E$, $a\mathcal{R}b \Rightarrow b\mathcal{R}a$ (i.e. $\mathcal{R} = \mathcal{R}^{-1}$),*

• *antisymétrique si $\forall a, b \in E$, $a\mathcal{R}b$ et $b\mathcal{R}a \Rightarrow a = b$ (i.e. $\mathcal{R} \cap \mathcal{R}^{-1} = \emptyset$),*

• *antireflexive si $\forall a \in E$, $(a,a) \notin \mathcal{R}$ (i.e. $\mathcal{R} \cap Id_E = \emptyset$),*

• *transitive si $\forall a, b, c \in E$, $a\mathcal{R}b$ et $b\mathcal{R}c \Rightarrow a\mathcal{R}c$.*

Exemples: 1/ E ensemble, $\mathcal{R} = \emptyset$.

2/ E ensemble, $\mathcal{R} = Id_E$.

3/ Sur $\mathcal{P}(E)$, $A\mathcal{R}B \Leftrightarrow A \subset B$.

4/ Sur $\mathbb{R}$, $a\mathcal{R}b \Leftrightarrow a < b$.

5/ Sur E ensemble, $a\mathcal{R}b \Leftrightarrow a \neq b$.

6/ Ω ensemble à au moins deux éléments. Sur $\mathcal{P}(\Omega)$, $A\mathcal{R}B$ ssi il existe une bijection $f : A \to B$.

1.4.2 Relations d'équivalence

Définition.— *Soit E un ensemble et $\mathcal{R}$ un relation binaire sur E. On dit que $\mathcal{R}$ est une relation d'équivalence si $\mathcal{R}$ est reflexive, symétrique et transitive.*

Exemple: Congruence sur $\mathbb{Z}$.

Notation: Si $\mathcal{R}$ est une relation d'équivalence sur un ensemble E, pour tout $x \in E$, on note

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

Cet ensemble s'appelle *la classe d'équivalence de x modulo $\mathcal{R}$.*

Proposition.— *Soit E un ensemble et $\mathcal{R}$ une relation d'équivalence sur E.*

a) Si $x, y \in E$ sont tels que $\overline{x} \neq \overline{y}$, alors $\overline{x} \cap \overline{y} = \emptyset$.

b) Les propositions suivantes sont équivalantes:

i) $x\mathcal{R}y$,

ii) $\overline{x} = \overline{y}$.

Définition.— *Soit E un ensemble et $\mathcal{R}$ un relation d'équivalence sur E. On appelle ensemble quotient de E par $\mathcal{R}$ l'ensemble des classes d'équivalences des éléments de E modulo $\mathcal{R}$. On note cet ensemble $E/\mathcal{R}$ (c'est un sous-ensemble de $\mathcal{P}(E)$.*

Exemple: $\mathbb{Z}/n\mathbb{Z}$.

Proposition.— *Soit E un ensemble, $\mathcal{R}$ et $\mathcal{T}$ deux relations d'équivalences sur E. Les propositions suivantes sont équivalentes:*

i) $\mathcal{R} = \mathcal{T}$,

ii) $E/\mathcal{R} = E/\mathcal{T}$.

1.4.3 Partitions et relations d'équivalences

Définition.— *Soit E un ensemble. On appelle partition de E toute partie $\{E_i\}_{i\in I}$ de $\mathcal{P}(E)$ telle que :*

- $\forall i \in I,\ E_i \neq \emptyset$,
- $\forall i \neq j,\ E_i \cap E_j = \emptyset$,
- $\bigcup_i E_i = E$.

Proposition.— *Soit E un ensemble et $\mathcal{R}$ une relation d'équivalence sur E. L'ensemble $E/\mathcal{R} \subset \mathcal{P}(E)$ est une partition de E.*

Réciproquement, si $\{E_i\}_{i\in I} \subset \mathcal{P}(E)$ est une partition de E, alors il existe une unique relation d'équivalence $\mathcal{R}$ sur E telle que $E/\mathcal{R} = \{E_i\}_{i\in I}$.

Il y a donc une correspondance bijective entre les partitions d'un ensemble E et les relations d'équivalence sur E.

Définition.— *Soit E un ensemble. Soient P_1 et P_2 deux partitions de E. On dit que P_1 est plus fine que P_2 si*

$$\forall A \in P_1,\ \exists B \in P_2,\ A \subset B$$

Si $\mathcal{R}$ et $\mathcal{T}$ sont deux relations d'équivalence sur E, on dit que $\mathcal{R}$ est plus fine que $\mathcal{T}$ si $E/\mathcal{R}$ est une partition de E plus fine que $E/\mathcal{T}$.

Proposition.— *Soit E un ensemble et Ω l'ensemble des relations d'équivalence sur E. La relation binaire sur Ω "être plus fine que" est une relation d'ordre (i.e. est réflexive, antisymétrique et transitive).*

Lemme.— *Si $\mathcal{R}$ et $\mathcal{T}$ sont deux relations d'équivalence sur E, la relation binaire $\mathcal{S} = \mathcal{R} \cap \mathcal{T}$ est une relation d'équivalence. De plus, $\mathcal{S}$ est plus fine que $\mathcal{R}$ et que $\mathcal{T}$.*

1.4.4 Représentation matricielle d'une relation binaire

Définition.— *On appelle matrice booléenne d'ordre n, toute matrice nxn à coefficients dans $\{0,1\}$. Dans l'ensemble des matrices booléenne d'ordre n, on définit deux lois de composition $+$ et $.$ définie, pour $A = (a_{i,j})_{1\leq i,j\leq n}$ et $B = (b_{i,j})_{1\leq i,j\leq n}$, par*

$$A + B = (c_{i,j})_{1\leq i,j\leq n} \text{ avec } c_{i,j} = Max(a_{i,j}, b_{i,j})$$

et

$$A.B = (d_{i,j})_{1\leq i,j\leq n} \text{ avec } d_{i,j} = Max_{k=1,\cdots,n}(a_{i,k}b_{k,j})$$

Définition.— *Soit $E = \{x_1, \cdots, x_n\}$ un ensemble fini et $\mathcal{R}$ une relation binaire sur E. On appelle matrice booléenne associée à $\mathcal{R}$ la matrice $M_{\mathcal{R}} = (a_{i,j})_{1\leq i,j\leq n}$ définie par:*

$$\forall 1 \leq i,j \leq n \begin{cases} a_{i,j} = 1 & si\ x_i\mathcal{R}x_j \\ a_{i,j} = 0 & sinon \end{cases}$$

Proposition.— *Dans cette situation, on a:*

• $\mathcal{R}$ *est reflexive si et seulement si* $M_{\mathcal{R}}$ *ne possède que des* 1 *sur sa diagonale.*

• $\mathcal{R}$ *est symétrique si et seulement si* ${}^tM_{\mathcal{R}} = M_{\mathcal{R}}$.

Proposition.— *Soit* E *un ensemble fini et* $\mathcal{R}$ *et* $\mathcal{T}$ *deux relations binaire sur* E *de matrice booléenne respective* $M_{\mathcal{R}}$ *et* $M_{\mathcal{T}}$. *La matrice booléenne de* $\mathcal{R} \cup \mathcal{T}$ *vaut*

$$M_{\mathcal{R}\cup\mathcal{T}} = M_{\mathcal{R}} + M_{\mathcal{T}}$$

et celle de $\mathcal{R} \circ \mathcal{T}$ *est*

$$M_{\mathcal{R}\circ\mathcal{T}} = M_{\mathcal{R}}.M_{\mathcal{T}}$$

1.5 Dénombrement

1.5.1 Principe de récurrence

Théorème.— (Principe de récurrence) *Soit* $A \subset \mathbb{N}$ *telle que :*

• $0 \in A$,

• $\forall n \in \mathbb{N},\ n \in A \Rightarrow n+1 \in A$.

Alors $A = \mathbb{N}$.

Corollaire.— (Démonstration par récurrence) *Soit* $\mathcal{P}_n$ *une famille de propositions indexées par* $\mathbb{N}$. *Si :*

• $\mathcal{P}_0$ *est vraie,*

• $\forall n \in \mathbb{N}$, $\mathcal{P}_n$ *vraie* $\Rightarrow \mathcal{P}_{n+1}$ *vraie.*

Alors $\mathcal{P}_n$ *est vraie pour tout* $n \in \mathbb{N}$.

Exemples.— • $\forall n \in \mathbb{N}, \displaystyle\sum_{p=0}^{n} p = \frac{p(p+1)}{2}$.

• Paradoxe de Tarski : *Si dans une population de* n *personnes il y a au moins une femme, alors il n'y a que des femmes.*

1.5.2 Ensembles finis

Définition.— *On dit qu'un ensemble non vide* E *est fini, s'il existe un entier* $n \geq 1$ *et une bijection de* E *sur* $\{1, \cdots, n\}$. *L'entier* n *s'appelle alors le cardinal de* E *et se note au choix,* $card(E)$, $\sharp E$ *ou* $|E|$.

On décrète que $\emptyset$ est un ensemble fini et que son cardinal est 0.

Théorème.— *Un ensemble fini possède un unique cardinal.*

Proposition.— *Soit* E *et* F *deux ensembles finis. Les propositions suivantes sont équivalentes.*

i) $card(E) = card(F)$,

ii) Il existe une bijection de E *sur* F.

Proposition.— *Soit* E *et* F *deux ensembles finis de même cardinal et* $f : E \to F$ *une application. Les propositions suivantes sont équivalentes.*

i) f *est bijective,*

ii) f *est injective,*

iii) f *est surjective.*

1.5.3 Analyse combinatoire

Proposition.— *Soit E et F deux ensembles finis. Alors $E \cup F$ et $E \cap F$ sont finis et*

$$\sharp(E \cup F) = \sharp E + \sharp F - \sharp(E \cap F)$$

Proposition.— *Soit E et F deux ensembles finis. L'ensemble $\mathcal{F}(E, F)$ est fini et*

$$\sharp\mathcal{F}(E, F) = (\sharp F)^{\sharp E}$$

Notation: C'est pourquoi, on note plus souvent F^E au lieu de $\mathcal{F}(E, F)$.

Proposition.— *Soit E et F deux ensembles de cardinal respectif p et n. Le sous-ensemble de $\mathcal{F}(E, F)$ constitué des applications injectives à un cardinal qui vaut :*

- 0 *si* $p > n$,
- $\dfrac{n!}{(n-p)!}$ *si* $p \leq n$.

Notation: On note A_n^p ce cardinal, c'est le nombre d'"arrangements" de p éléments dans un ensemble à n éléments.

Proposition.— *Soit E un ensemble de cardinal n. Le sous-ensemble de $\mathcal{P}(E)$ constitué des sous-ensemble de de E de cardinal p est un ensemble fini de cardinal :*

- 0 *si* $p > n$,
- $\dfrac{n!}{p!(n-p)!}$ *si* $p \leq n$.

Notation: On note C_n^p ce cardinal, c'est le nombre de "combinaisons" de p éléments dans un ensemble à n éléments.

Théorème.— (Formule du binôme de Newton) *Soit $(A, +, .)$ un anneau commutatif, $a, b \in A$ et $n \in \mathbb{N}$. On a :*

$$(a + b)^n = \sum_{p=0}^{n} C_n^p a^p b^{n-p}$$

Principe des nids de pigeons: Soit n pigeons dans p nids. Si $n > p$, alors il existe un nid contenant au moins 2 pigeons.

Généralisation: Soit n pigeons dans p nids. Si $n > pk$ (pour un entier $k \neq 0$ donné), alors il existe un nid contenant au moins $k + 1$ pigeons.

Interprétation.— *Soit $f : E \to F$ une application entre deux ensembles finis vérifiant $\sharp E > \sharp F$. Il existe un élément $y \in F$ tel que $\sharp f^{-1}(\{y\}) \geq 2$.*

1.6 Ensembles infinis

1.6.1 Cardinalité

Définition.— *On dit qu'un ensemble E est infini, s'il n'est pas fini. Soient E et F deux ensembles. On dit que E et F sont équipotent s'il existe une bijection entre ces deux ensembles. On dit alors qu'ils ont même cardinal et l'on note $card(E) = card(F)$.*

S'il existe une injection de E dans F, on note $card(E) \leq card(F)$ et s'il existe une surjection de E dans F, on note $card(E) \geq card(F)$.

Proposition.— *Soit E et F deux ensembles.*

- *si $card(E) \leq card(F)$ et si E est infini alors F est infini.*
- *si $card(E) \leq card(F)$ et $card(F) \leq card(E)$ alors $card(E) = card(F)$.*
- *si $card(E) \leq card(F)$ alors $card(F) \geq card(E)$*

La réciproque de la dernière propriété n'est pas décidable. En fait, elle dépend de l'axiome suivant :

Axiome du choix. Soit E un ensemble non vide. Il existe une fonction (dite fonction de choix sur E) $f : \mathcal{P}(E) \to E$ vérifiant :

$$\forall A \in \mathcal{P}(E),\ A \neq \emptyset \Rightarrow f(A) \in A$$

On a alors :

Théorème.— *L'axiome du choix équivaut à la propriété suivantes : si E et F sont des ensembles tels que $card(E) \geq card(F)$, alors $card(F) \leq card(E)$.*

Théorème.— *Soit E un ensemble. Les ensembles E et $\mathcal{P}(E)$ ne sont jamais équipotents.*

1.6.2 Ensembles dénombrables

Proposition.— *Toute partie infinie de $\mathbb{N}$ est équipotente à $\mathbb{N}$.*

Définition.— *Un ensemble E est dit dénombrable s'il est fini ou équipotent à $\mathbb{N}$ (ce qui revient à dire qu'il existe une injection de E dans $\mathbb{N}$).*

Exemples: • $\mathbb{N}$ est dénombrable.

• $\mathbb{Z}$ est dénombrable. L'application $\varphi : \mathbb{Z} \to \mathbb{N}$ qui à $n \geq 0$ associe $2n$ et à $n < 0$ associe $-2n - 1$, est bijective.

• $\mathbb{N} \times \mathbb{N}$ est dénombrable. L'application $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ qui à (a, b) associe $2^a 3^b$ est injective. De manière générale, $\mathbb{N}^n$ est dénombrable. L'application $f : \mathbb{N}^n$ qui à $(a_1, \cdots, a_n)$ associe $2^{a_1} 3^{a_2} \cdots p_n^{a_n}$ (où $(p_k)_k$ désigne la suite des nombres premiers) est injective.

• $\mathbb{Q}$ est dénombrable. Si $r \in \mathbb{Q}$, il existe un unique couple d'entiers (p, q) avec $p \in \mathbb{Z}$ et $q \in \mathbb{N}$ tel que $r = p/q$. Si on pose $f(r) = (\varphi(p), q) \in \mathbb{N} \times \mathbb{N}$, alors f est une application injective.

Proposition.— *Si A et B sont deux ensembles dénombrables, alors $A \times B$ l'est aussi*

Proposition.— *Si $(E_n)_{n \in \mathbb{N}}$ est une famille d'ensembles dénombrables, $\bigcup_n E_n$ est dénombrable.*

Proposition.— *$\mathbb{R}$ n'est pas dénombrable.*

2 Ordres

2.1 Généralités

2.1.1 Ensembles ordonnés

Définition.— *Soit E un ensemble et $\mathcal{R}$ une relation binaire sur E. On dit que $\mathcal{R}$ est :*

- *un pré-ordre sur E, si $\mathcal{R}$ est réflexive et transitive,*

• *un ordre sur E, si $\mathcal{R}$ est réflexive, transitive et antisymétrique,*

• *un ordre stricte sur E, si $\mathcal{R}$ est antiréflexive, antisymétrique et transitive.*

Si $\leq$ est un ordre sur E, on dit que $(E, \leq)$ est un ensemble ordonné.

Exemples: • $(\mathbb{N}, \leq)$ est un ordre.

• $(\mathbb{R}, <)$ est un ordre stricte.

• $(\mathcal{P}(E), \subset)$ est un ordre.

• $(\mathbb{N}^*, \leq)$ avec $a \leq b \iff a$ divise b est un ordre.

• $(\mathbb{Z}^*, \leq)$ avec $a \leq b \iff a$ divise b n'est pas un ordre, mais est un pré-ordre.

• $(\mathcal{P}(E), \leq)$ avec $A \leq B \iff \sharp A \leq \sharp B$ n'est pas un ordre, mais est un pré-ordre.

Proposition.— *Soit $(E_1, \leq_1)$ et $(E_2, \leq_2)$ deux ensembles ordonnés. Sur $E = E_1 \times E_2$, la relation $\leq$ définie par :*

$$(e_1, e_2) \leq (f_1, f_2) \iff e_1 \leq_1 f_1 \textit{ et } e_2 \leq_2 f_2$$

est un ordre. On appelle cet ordre, "l'ordre produit".

Proposition.— *Soit $(E_1, \leq_1)$ et $(E_2, \leq_2)$ deux ensembles ordonnés. Sur $E = E_1 \times E_2$, la relation $\leq_{lex}$ définie par :*

$$(e_1, e_2) \leq_{lex} (f_1, f_2) \iff \begin{cases} e_1 \leq_1 f_1 & \textit{et} \quad e_1 \neq f_1 \\ & \textit{ou} \\ e_1 = f_1 & \textit{et} \quad e_2 \leq f_2 \end{cases}$$

est un ordre. On appelle cet ordre, "l'ordre lexicographique".

Définition.— *Soit $(E, \leq)$ un ensemble ordonné. On dit que $\leq$ est total si pour tout $x, y \in E$, on a $x \leq y$ ou $y \leq x$. Si $\leq$ n'est pas total, on dit que $\leq$ est partiel.*

Proposition.— *Soit $(E_1, \leq_1)$ et $(E_2, \leq_2)$ deux ensembles totalement ordonnés. L'ordre lexicographique $\leq_{lex}$ sur $E = E_1 \times E_2$ est total.*

Définition.— *Soit $(E, \leq)$ un ensemble ordonné et A une partie de E. On appelle ordre induit par E sur A, la relation $\leq_A = \leq \cap (A \times A)$. C'est un ordre sur A; s'il n'y a pas d'ambiguité, on continue à le noté $\leq$.*

2.1.2 Eléments remarquables

Définition.— *Soit $(E, \leq)$ un ensemble ordonné, $A \subset E$ et $\alpha \in E$. On dit que α est :*

• *un majorant (resp. minorant) de A si*

$$\forall x \in A,\ x \leq \alpha \ (\textit{resp. } \alpha \leq x)$$

• *un élément maximal (resp. minimal) de A, si $\alpha \in A$ et si*

$$\forall x \in A,\ \alpha \leq x \Rightarrow x = \alpha \ (\textit{resp. } x \leq \alpha \Rightarrow x = \alpha)$$

• *un plus grand élément (resp. plus petit élément) de A, si $\alpha \in A$ et si*

$$\forall x \in A,\ x \leq \alpha \ (\textit{resp. } \alpha \leq x)$$

• *une borne supérieure (resp. inférieure) de A, si α est le plus petit des majorants (resp. le plus grand des minorants).*

Proposition.— *Soit* $(E, \leq)$ *un ensemble ordonné,* $A \subset E$ *et* $\alpha \in E$*. On a :*

1/ α *plus grand élément* $\Rightarrow$ α *élément maximal.*

2/ α *plus grand élément* $\Rightarrow$ α *borne supérieure.*

3/ α *borne supérieure* $\Rightarrow$ α *majorant.*

Exemples: • Majorant qui n'est pas une borne supérieure :

• Borne supérieure qui n'est pas un plus grand élément :

• Elément maximal qui n'est pas un plus grand élément :

• Elément maximal qui n'est pas un majorant :

• Majorant qui n'est pas un élément maximal :

Remarques : • Si α est un plus grand élément, il est unique. De même si α est une borne supérieure.

• Si α est l'unique élément maximal de A, il se peut quand même que α ne soit pas le plus grand élément de A. Par contre, si $\leq$ est total, il y a au maximum un élément maximal dans A et si ce dernier existe, c'est un plus grand élément.

Notation: Si A admet une borne supérieure (resp. inférieure), on note celle-ci $Sup(A)$ (resp. $Inf(A)$).

Proposition.— *Soit* $(E, \leq)$ *ordonné et* X *une partie de* E*.*

• *Si* X *admet une borne supérieure et inférieure, alors* $Inf(X) \leq Sup(X)$*.*

• *Si* $X = \emptyset$ *alors* X *admet une borne supérieure (resp. inférieure) ssi* E *possède un plus petit élément (resp. un plus grand élément). Dans ces condition, on a* $Sup(\emptyset) \leq Inf(\emptyset)$*.*

Définition.— *Soient* $(E_1, \leq_1)$ *et* $(E_2, \leq_2)$ *deux ensembles ordonnés et* $f : E_1 \to E_2$ *une application. On dit que* f *est croissante si*

$$\forall x, y \in E_1,\ x \leq_1 y \Rightarrow f(x) \leq_2 f(y)$$

Exemple.— Soit $f : E \to F$ une application. On ordonne $\mathcal{P}(E)$ et $\mathcal{P}(F)$ par l'inclusion. L'application $g : \mathcal{P}(E) \to \mathcal{P}(F)$ définie par

$$\forall A \in \mathcal{P}(E),\ g(A) = f(A)$$

est croissante.

Définition.— *Soit* $(E, \leq)$ *un ensemble ordonné.*

• *On appelle chaine de* E *tout partie* X *totalement ordonnée (i.e.* $(X, \leq_X)$ *est totalement ordonné).*

• *On appelle antichaine de* E *tout partie* X *telle que* $(X \times X) \cap \leq = Id_X$ *(i.e.* $\forall x, y \in X,\ x \leq y \Rightarrow x = y$*).*

Si X *est une chaine (resp. une antichaine), on dit que* X *est maximale si pour toute chaine (resp. antichaine)* Y *de* E*,*

$$X \subset Y \Rightarrow X = Y$$

Exemple : Soit $E = \mathcal{P}(\{a, b, c\})$, muni de l'inclusion.

• $X = \{\emptyset, \{a\}, \{a, b\}, \{a, b, c\}\}$ est une chaine maximale.

• $X = \{\{a\}, \{a, b\}, \{a, b, c\}\}$ est une chaine non maximale.

• $X = \{\{a\}\}$ est une antichaine non maximale.

Définition.— *Soit* $(E, \leq)$ *un ensemble ordonné fini. On appelle*

• *largeur de* E*, le cardinal maximal des antichaines de* E*,*

• *hauteur de* E*, le cardinal maximal des chaines de* E*.*

Définition.— *Soit* $(E, \leq)$ *un ensemble ordonné et* $a, b \in E$ *tels que* $a \leq b$*. On appelle intervalle d'extrémité* a, b *l'ensemble*

$$[a, b] = \{c \in E / \ a \leq c \leq b\}$$

Exemples : Sur $(\mathcal{P}(\{a, b, c\}), \subset)$ on a :

• $[\emptyset, \{a, b, c\}] = \mathcal{P}(\{a, b, c\}$,

• $[\emptyset, \{a, b\}] = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$,

• $[\{a\}, \{b\}]$ n'a pas de sens.

Définition.— *Soit* $(E, \leq)$ *un ensemble ordonné. On dit que* E *est inductif si toute chaine* $X \subset E$ *admet un majorant.*

Lemme (Axiome) de Zorn.— *Tout ensemble inductif admet un élément maximal.*

En fait, le lemme de Zorn équivaut à l'axiome du choix.

Définition.— *Soit* $(E, \leq)$ *un ensemble ordonné. On appelle extension linéaire de* $\leq$*, tout ordre total* $\leq_0$ *tel que* $\leq \subset \leq_0$*.*

Théorème.— *Tout ensemble ordonné* $(E, \leq)$ *admet des extensions linéaires et*

$$\leq = \bigcap_{ext.\ lin.} \leq_0$$

2.2 Treillis

2.2.1 Ensembles réticulés

Définition.— *On dit qu'un ensemble ordonné* $(E, \leq)$ *est filtrant à droite (resp. filtrant à gauche, resp. filtrant) si pour tout couple* $(a, b) \in E^2$*, la partie* $\{a, b\}$ *admet un majorant (resp. un minorant, resp. un majorant et un minorant).*

Définition.— *On dit qu'un ensemble ordonné* $(E, \leq)$ *est réticulé à droitre (ou est un semi-treillis supérieur) (resp. réticulé à gauche (ou est un semi-treillis inférieur), resp. réticulé (ou est un treillis)) si pour tout couple* $(a, b) \in E^2$*, la partie* $\{a, b\}$ *admet une borne supérieure (resp. une borne inférieure, resp. une borne supérieure et inférieure).*

Notation.— Si $(E, \leq)$ est un treillis et si $a, b \in E$, on note:

• $a \cup b = Sup(\{a, b\})$,

• $a \cap b = Inf(\{a, b\})$,

Proposition.— *Soit* $(E, \leq)$ *un treillis et* $X \subset E$ *une partie finie non vide.* X *admet une borne supérieure et inférieure.*

Corollaire.— *Si* $(E, \leq)$ *un treillis fini, alors* E *admet un plus grand et un plus petit élément.*

Proposition.— *Soit* $(E, \leq)$ *un treillis.*

- $\forall x \in E,\ \left.\begin{array}{rcl} x \cup x & = & x \\ x \cap x & = & x \end{array}\right\}$ *Idempotence*
- $\forall x, y \in E,\ \left.\begin{array}{rcl} x \cup y & = & y \cup x \\ x \cap y & = & y \cap x \end{array}\right\}$ *Commutativité*
- $\forall x, y, z \in E,\ \left.\begin{array}{rcl} (x \cup y) \cup z & = & x \cup (y \cup z) \\ (x \cap y) \cap z & = & x \cap (y \cap z) \end{array}\right\}$ *Associativité*
- $\forall x, y \in E,\ \left.\begin{array}{rcl} (x \cup y) \cap x & = & x \\ (x \cap y) \cup x & = & x \end{array}\right\}$ *Absorption*

Définition.— *On dit qu'un treillis $(E, \leq)$ est distributif si pour tout $x, y, z \in E$,*

- $x \cup (y \cap z) = (x \cup y) \cap (x \cup z)$,
- $x \cap (y \cup z) = (x \cap y) \cup (x \cap z)$.

2.3 Ensembles complets et bien fondés

2.3.1 Généralités

2.3.2 Principe d'induction Noethérienne

2.3.3 Les théorèmes de Knäster et Tarski