L3I COMBINATOIRE — 1 : ENSEMBLES

Christian RONSE, ICube, Département d'Informatique de l'Université de Strasbourg

Un ensemble est une structure mathématique définie par ses éléments. On écrit $x \in A$ pour dire que *x est un élément de A*, ou que x *appartient à* A (la négation de $x \in A$ s'écrit $x \notin A$). Un ensemble peut être défini soit comme combinaison d'autres ensembles (voir plus bas), soit en spécifiant ses éléments. Dans ce cas il peut être décrit *par extension*, en donnant la liste explicite de ses éléments entre accolades { }, par exemple

$$X = \{3, 4, 5, 6, 7\} \ ,$$

ou *par intension*, en caractérisant mathématiquement ses éléments, ce qui donne pour l'exemple ci-dessus :

$$X = \{x \mid x \in \mathbb{N},\ x \geq 3,\ x \leq 7\} \ .$$

D'une manière générale, la description par intension d'un ensemble prendra la forme

$$\{\mathit{expression} \mid \mathit{conditions}\} \ ,$$

avec la convention qu'une virgule entre des conditions doit être considérée comme une conjonction : les différentes conditions séparées par des virgules doivent être satisfaites simultanément. On adopte généralement la convention d'écrire

$$\{x \in \mathit{ensemble} \mid \mathit{conditions}\} \qquad \text{pour} \qquad \{x \mid x \in \mathit{ensemble},\ \mathit{conditions}\} \ .$$

Paradoxes de la conception naïve des ensembles

La conception "naïve" de la théorie des ensembles considère que n'importe quelle condition mathématique suffit à définir un ensemble, mais cela conduit rapidement à des "paradoxes" (en fait, des contradictions), le plus connu étant dû à Bertrand Russel. Définissons

$$A = \{x \mid x \notin x\} \ .$$

A-t-on $A \in A$? On voit que $A \in A$ ssi A est un x tel que $x \notin x$, donc ssi $A \notin A$. Cette contradiction est semblable au "paradoxe du barbier" :

Le barbier rase tous les hommes qui ne se rasent pas eux-mêmes, et uniquement ceux-ci.

A la question : "le barbier se rase-t-il lui-même ?", la reponse est :

Le barbier se rase lui-même si et seulement s'il ne se rase pas lui-même.

La conclusion est alors que le barbier n'est pas un homme, qu'il n'est pas sujet à être rasé. De même, on conclura que l'objet mathématique A défini plus haut n'est pas sujet à la relation d'appartenance, donc la relation $A \in X$ (ou $A \notin X$) pour un ensemble X n'est pas définie. On dira ainsi que A est une *collection*, et on réservera le mot ensemble pour une structure qui peut elle-même appartenir à un ensemble.

Théorie des ensembles

La théorie mathématique des ensembles considère que tous les objets mathématiques sont des ensembles, et que la relation d'appartenance $\in$ est définie entre les ensembles. Elle ne dit pas quelles propriétés mathématiques permettent ou non de définir un ensemble, ni s'il y a tel ou tel type d'ensemble, mais elle donne des axiomes sur les ensembles, et des règles permettant de construire des ensembles à partir d'autres ensembles.

Un ensemble est défini par ses éléments, donc deux ensembles ayant les mêmes éléments doivent être égaux :

$$A = B \quad \Longleftrightarrow \quad \big[\forall x,\ (x \in A \ \Leftrightarrow\ x \in B)\big] \ .$$

Ensuite on a l'ensemble vide $\emptyset$ (caractérisé par $\forall x,\ x \notin \emptyset$), pour tout objet a on a le singleton $\{a\}$ (caractérisé par $\forall x,\ [x \in \{a\} \ \Leftrightarrow\ x = a]$), et pour deux objets a, b distincts ($a \neq b$), on a la paire $\{a, b\}$ (caractérisée par $\forall x,\ [x \in \{a, b\} \ \Leftrightarrow\ (x = a \text{ ou } x = b)]$).

On définit une *partie* ou un *sous-ensemble* d'un ensemble A comme un ensemble B dont tous les éléments appartiennent à A, et on écrit $B \subseteq A$ (ou $A \supseteq B$) ; on dit aussi que B *est inclus dans* A. Ainsi :

$$B \subseteq A \iff \big[\forall x,\ (x \in B \ \Rightarrow\ x \in A)\big] \ .$$

Donc $B = A$ ssi $B \subseteq A$ et $A \subseteq B$. On dit que B est une *partie propre* de A, ou que B *est strictement inclus dans* A si $B \subseteq A$ mais $B \neq A$; on écrit alors $B \subset A$ (ou $A \supset B$). Certains auteurs (notamment ceux suivant la tradition de Bourbaki) écrivent $B \subset A$ pour $B \subseteq A$, et $B \underset{\neq}{\subset} A$ pour $B \subset A$.

Les parties d'un ensemble A forment un ensemble, noté $\mathcal{P}(A)$. Donc

$$\mathcal{P}(A) = \{B \mid B \subseteq A\} \ .$$

Par exemple $\mathcal{P}(\emptyset) = \{\emptyset\}$, $\mathcal{P}(\{a\}) = \big\{\emptyset, \{a\}\big\}$ et $\mathcal{P}(\{a, b\}) = \big\{\emptyset, \{a\}, \{b\}, \{a, b\}\big\}$.

La *réunion* de deux ensembles A et B est l'ensemble

$$A \cup B = \{x \mid x \in A \text{ ou } x \in B\} \ .$$

Cette opération est *commutative*, $A \cup B = B \cup A$, et *associative*, $A \cup (B \cup C) = (A \cup B) \cup C$. On peut donc écrire la réunion d'un nombre fini d'ensembles par une succession de réunions binaires, sans mettes de parenthèses, par exemple pour 4 ensembles A, B, C, D, $A \cup B \cup C \cup D$ désigne

$$\big((A \cup B) \cup C\big) \cup D = \big(A \cup (B \cup C)\big) \cup D = A \cup \big((B \cup C) \cup D\big) = A \cup \big(B \cup (C \cup D)\big) = (A \cup B) \cup (C \cup D) \ .$$

Etant donnés n ensembles $B_1, \ldots, B_n$, leur réunion $B_1 \cup \cdots \cup B_n$ peut s'écrire

$$\bigcup_{i=1}^{n} B_i = \big\{x \mid \exists i \in \{1, \ldots, n\},\ x \in B_i\big\} \ .$$

On peut aussi définir la réunion d'un ensemble $\mathcal{F}$ quelconque d'ensembles (même s'il y en a une infinité), cela donne l'ensemble $\bigcup \mathcal{F}$:

$$\bigcup \mathcal{F} = \big\{x \mid \exists B \in \mathcal{F},\ x \in B\big\} \ .$$

Par exemple prenons $\mathcal{F} \subset \mathcal{P}(\mathbb{N})$ donné par extension : $\mathcal{F} = \big\{\{0, 2, 4\}, \{1, 4, 5\}, \{2, 6, 8\}\big\}$, on aura $\bigcup \mathcal{F} = \{0, 1, 2, 4, 5, 6, 8\}$. Souvent on prend un ensemble $\mathcal{F}$ de la forme $\{B_i \mid i \in I\}$, sa réunion s'écrit alors

$$\bigcup_{i \in I} B_i = \big\{x \mid \exists i \in I,\ x \in B_i\big\} \ .$$

L'*intersection* de deux ensembles A et B est l'ensemble

$$A \cap B = \{x \in A \mid x \in B\} \ .$$

Cette opération est commutative et associative, $A \cap B = B \cap A$ et $A \cap (B \cap C) = (A \cap B) \cap C$, on peut donc écrire l'intersection d'un nombre fini d'ensembles par une succession d'intersections binaires, sans mettes de parenthèses. Etant donnés n ensembles $B_1, \ldots, B_n$, leur intersection $B_1 \cap \cdots \cap B_n$ peut s'écrire

$$\bigcap_{i=1}^{n} B_i = \big\{x \mid \forall i \in \{1, \ldots, n\},\ x \in B_i\big\} \ .$$

On définit aussi l'intersection d'un ensemble $\mathcal{F}$ quelconque d'ensembles, cela donne l'ensemble $\bigcap \mathcal{F}$:

$$\bigcap \mathcal{F} = \big\{x \mid \forall B \in \mathcal{F},\ x \in B\big\} \ .$$

Par exemple prenons $\mathcal{F} \subset \mathcal{P}(\mathbb{N})$ donné par $\mathcal{F} = \big\{\{0,2,4\}, \{0,1,4,5\}, \{0,2,6,8\}\big\}$, on aura $\bigcap \mathcal{F} = \{0\}$. Si on prend $\mathcal{F}$ de la forme $\{B_i \mid i \in I\}$, son intersection s'écrit alors

$$\bigcap_{i \in I} B_i = \big\{x \mid \forall i \in I,\ x \in B_i\big\} \ .$$

L'union et l'intersection satisfont la propriété de *distributivité* :

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \qquad \text{et} \qquad A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \ .$$

La distributivité est une propriété bien connue dans l'algèbre des nombres réels, où la multiplication distribue l'addition : $x \cdot (y+z) = (x \cdot y) + (x \cdot z)$; mais ici chacune de l'intersection et de la réunion distribue l'autre, alors que dans les réels l'addition ne distribue pas la multiplication : $x + (y \cdot z) \neq (x+y) \cdot (x+z)$. En fait, l'union et l'intersection satisfont une règle plus générale, la *distributivité infinie* : pour un ensemble $\{B_i \mid i \in I\}$, on a

$$A \cup \Big(\bigcap_{i \in I} B_i\Big) = \bigcap_{i \in I} (A \cup B_i) \qquad \text{et} \qquad A \cap \Big(\bigcup_{i \in I} B_i\Big) = \bigcup_{i \in I} (A \cap B_i) \ .$$

La *différence* de deux ensembles A et B est

$$A \setminus B = \{x \in A \mid x \notin B\} \ ,$$

et la *différence symétrique* de A et B, qui comprend tous les objets appartenant à un et un seul des ensembles A et B, s'écrit :

$$A \bigtriangleup B = (A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B) \ .$$

Notons enfin qu'on peut construire une partie d'un ensemble en restreignant ses éléments à ceux satisfaisant certaines conditions :

$$B = \{x \in A \mid \textit{conditions}\} \ ,$$

où chacune des conditions peut se réduire à une combinaison logique de propriétés ensemblistes. On peut aussi, à partir d'une fonction construite par combinaison logique d'énoncés ensemblistes, définir l'ensemble image d'un ensemble par cette fonction :

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

Etant donné un ensemble E, on définit sur $\mathcal{P}(E)$ l'opération de *complémentation*, qui associe à tout $X \in \mathcal{P}(E)$ son *complémentaire* $X^c \in \mathcal{P}(E)$, défini par $X^c = E \setminus X$; certains auteurs l'écrivent $\overline{X}$. Notons que $(X^c)^c = X$. Par ailleurs l'intersection et l'union sont des opérations internes sur $\mathcal{P}(E)$ (une union ou une intersection de parties de E donne une partie de E), on peut donc exprimer diverses opérations sur $\mathcal{P}(E)$ par des combinaisons d'union, d'intersection et de complémentation. Par exemple $A \setminus B = A \cap B^c$ et $A \bigtriangleup B = (A \cap B^c) \cup (A^c \cap B)$. Les lois de *De Morgan* établissent une *dualité par complémentation* entre l'union et l'intersection :

$$(A \cup B)^c = A^c \cap B^c \qquad \text{et} \qquad (A \cap B)^c = A^c \cup B^c \ .$$

Elles permettent ainsi de mettre toute formule construite par les opérations d'union et intersection finies, et de complémentation, sous *forme normale disjonctive*, c.-à-d. comme une union de termes, chaque terme étant une intersection d'atomes, chaque atome étant un ensemble ou son complémentaire. Par exemple :

$$(A \setminus B) \setminus C = A \setminus (B \cup C) = A \cap B^c \cap C^c \ ,$$
$$(A \triangle B) \triangle C = A \triangle (B \triangle C) = (A \cap B \cap C) \cup (A \cap B^c \cap C^c) \cup (A^c \cap B \cap C^c) \cup (A^c \cap B^c \cap C) \ .$$

Un *couple* (a, b) est un objet formé de a et de b (qui peuvent être égaux ou distincts), en tenant compte de l'ordre entre eux ; donc $(a, b) = (a', b')$ ssi $a = a'$ et $b = b'$. Un couple (a, b) se distingue de la paire $\{a, b\}$ de deux façons : d'une part on peut avoir $a = b$ et considérer le couple (a, a), d'autre part pour $a \neq b$ on a $(a, b) \neq (b, a)$, alors que $\{a, b\} = \{b, a\}$. Formellement, on peut poser $(a, b) = \big\{\{a\}, \{a, b\}\big\}$. Etant donnés deux ensembles A et B, on définit le *produit cartésien*

$$A \times B = \{(a, b) \mid a \in A, b \in B\} \ .$$

Le terme "cartésien" provient de l'idé de Descartes, à la base de la géométrie analytique, de représenter un point du plan euclidien comme un couple de réels (ses coordonées selon deux axes orthogonaux). Notons que le produit cartésien distribue l'union et l'intersection, même infinies :

$$A \times \Big(\bigcup_{i \in I} B_i\Big) = \bigcup_{i \in I}(A \times B_i) \qquad \text{et} \qquad \Big(\bigcup_{i \in I} A_i\Big) \times B = \bigcup_{i \in I}(A_i \times B) \ ,$$
$$A \times \Big(\bigcap_{i \in I} B_i\Big) = \bigcap_{i \in I}(A \times B_i) \qquad \text{et} \qquad \Big(\bigcap_{i \in I} A_i\Big) \times B = \bigcap_{i \in I}(A_i \times B) \ .$$

On peut faire un produit cartésien de 3 ensembles par composition de produits de 2 :

$$(A \times B) \times C = \big\{\big((a, b), c\big) \mid a \in A, b \in B, c \in C\big\}$$
$$\text{et} \qquad A \times (B \times C) = \big\{\big(a, (b, c)\big) \mid a \in A, b \in B, c \in C\big\} \ .$$

On peut identifier les couples composés $\big((a, b), c\big)$ et $\big(a, (b, c)\big)$, ils contiennent la même information (les objets a, b et c, et leur ordre), ce qui donne le *triplet* (a, b, c), et on écrira

$$A \times B \times C = \big\{(a, b, c) \mid a \in A, b \in B, c \in C\big\} \ .$$

Plus généralement, pour un entier $n > 2$ on peut considérer un *n-uple* $(a_1, \ldots, a_n)$, et le produit cartésien de n ensembles :

$$A_1 \times \cdots \times A_n = \big\{(a_1, \ldots, a_n) \mid a_1 \in A_1, \ldots, a_n \in A_n\big\} \ .$$

Pour un ensemble E, on posera $E^2 = E \times E$, et pour un entier $n > 2$, $E^n = E \times \cdots \times E$ (n facteurs).