Applications

Laurent Debize

Mathématiques appliquées à l'informatique

Langage ensembliste

Définition

On appelle **ensemble**, toute collection d'objets, ceux-ci étant appelés **éléments** de l'ensemble.

Exemples

- L'ensemble des entiers naturels impairs
- L'ensemble des entiers qui n'ont que deux diviseurs (nombres premiers)
- L'ensemble des élèves d'une classe

Langage ensembliste

Notation

Un ensemble est noté entre accolades. Exemple : $E = \{0\,;\,1\,;\,2\}$
On note $x \in E$(lire x appartient à E) pour signifier que l'élément x appartient à l'ensemble E.
On note $x \notin E$(lire x n'appartient pas à E) pour signifier que l'élément x n'appartient pas à l'ensemble E.

Remarques

- Chaque élément ne figure qu'une seule fois et l'ordre dans lequel ces éléments sont écrits n'a pas d'importance.
- On appelle **ensemble vide** et on note $\varnothing$ tout ensemble qui ne contient aucun élément.

Deux façons de définir un ensemble

En extension

Définir un ensemble **en extension** signifie donner tous les éléments de cet ensemble.
Exemple : $E = \{0\,;\,2\,;\,4\,;\,5\,;\,12\}$

En compréhension

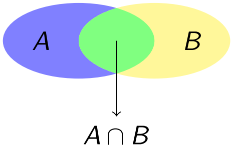
Définir un ensemble **en compréhension** signifie exprimer les éléments de cet ensemble à l'aide d'une proposition.
Exemple : $F = \{x \in \mathbb{N} \,|\, x \leq 10\}$
Le symbole $|$ se lit « tel que »
L'ensemble F se lit « l'ensemble des x dans $\mathbb{N}$ tels que $x \leq 10$ »
En extension, l'ensemble F s'écrit :
$F = \{0\,;\,1\,;\,2\,;\,3\,;\,4\,;\,5\,;\,6\,;\,7\,;\,8\,;\,9\,;\,10\}$

Intersection

Définition

Soient E un ensemble et A et B deux sous-ensembles de E.
L'intersection des deux ensembles A et B est l'ensemble des éléments qui sont communs à A et B.
On la note $A \cap B$.

Remarque :
Lorsque $A \cap B = \varnothing$, on dit que les ensembles A et B sont **disjoints**

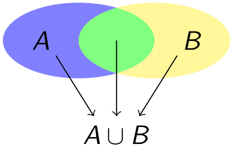


Cette représentation graphique s'appelle un **diagramme de Venn.**
On peut définir $A \cap B$ de la manière suivante (écriture axiomatique) :
$A \cap B = \{x \in E \,|\, x \in A \text{ et } x \in B\}$
Lire « ensemble des éléments x de E qui appartiennent à A **et** à B »

Réunion

Définition

Soient E un ensemble et A et B deux sous-ensembles de E.
La **réunion** des deux ensembles A et B est l'ensemble des éléments qui sont dans A ou dans B.
On la note $A \cup B$.



Écriture axiomatique :
$A \cup B = \{x \in E \,|\, x \in A \text{ ou } x \in B\}$
Lire « ensemble des éléments x de E qui appartiennent à A **ou** à B »

Remarque

Le mot « ou » ici signifie « ou l'un ou l'autre ou les deux » :
$A \cup B$ contient tous les éléments de A et tous les éléments de B.

Réunion

Exemples

Soient A et B les deux ensembles de nombres suivants :
$A = \{0\,;\,1\,;\,2\,;\,3\,;\,4\,;\,5\,;\,6\,;\,7\,;\,8\,;\,9\,;\,10\}$ et
$B = \{2\,;\,3\,;\,5\,;\,7\,;\,11\,;\,13\,;\,17\}$

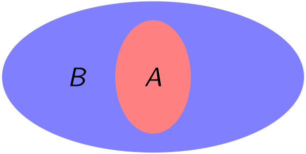
$A \cap B = \{2\,;\,3\,;\,5\,;\,7\}$ (éléments communs à A et à B)
$A \cup B = \{0\,;\,1\,;\,2\,;\,3\,;\,4\,;\,5\,;\,6\,;\,7\,;\,8\,;\,9\,;\,10\,;\,11\,;\,13\,;\,17\}$
Cet ensemble contient tous les éléments de A et tous les éléments de B (on n'écrit qu'une seule fois le même élément).

Inclusion

Définition

On dit que l'ensemble A est **inclus** dans l'ensemble B pour indiquer que tous les éléments de A appartiennent aussi à B.
On note $A \subset B$.

On a toujours, pour n'importe quel ensemble A : $A \subset A$ et $\varnothing \subset A$



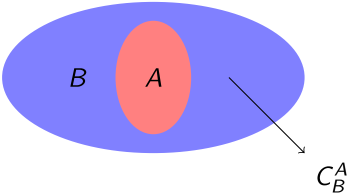
On dit aussi que A est une partie de B ou bien que A est un **sous-ensemble** de B.
Pour dire que A n'est pas inclus dans B, on emploiera la notation : $A \not\subset B$.

Complémentaire

Définition

Supposons que l'ensemble A est inclus dans l'ensemble B. On appelle le complémentaire de A dans B et on note C_B^A ou $\overline{A}$ l'ensemble des éléments de B qui n'appartiennent pas à A. Autrement dit :

$$x \in C_B^A \Leftrightarrow x \in B \text{ et } x \notin A$$



Remarque

On dit que B constitue le référentiel (l'ensemble auquel on se réfère pour prendre le complémentaire).

Fonctions

Définition

Soient E et F deux ensembles. Si à tout élément x de E est associé **au plus un élément** y de F par une relation f alors on dit que f est une **fonction** de E vers F.

Remarque : « au plus » signifie un ou aucun.

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

- f est le nom de la fonction
- E est l'ensemble de départ
- F est l'ensemble d'arrivée
- $x \mapsto f(x)$ donne la correspondance entre x et son image $f(x)$

La notation globale se lit « la fonction f de E dans F qui à x associe $f(x)$ ».

Fonctions

Image - antécédent : définitions

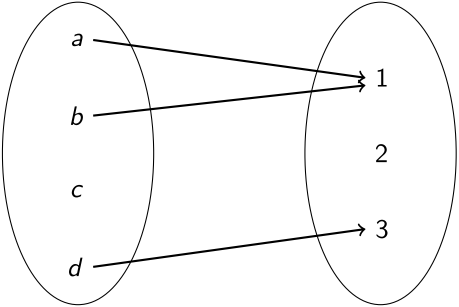
L'élément $f(x)$ est appelé **image** de x par la fonction f.

Pour tout y dans F, tout élément x de E vérifiant $f(x) = y$ est appelé **antécédent** de y par la fonction f.

Fonctions

Une fonction de E vers F peut également être définie par une **représentation sagittale**.

Exemple



$$f(a) = f(b) = 1\,;\ f(d) = 3$$

Fonctions

Définition

L'ensemble noté D_f des x qui ont une image par f est appelé **ensemble (ou domaine) de définition** de f.

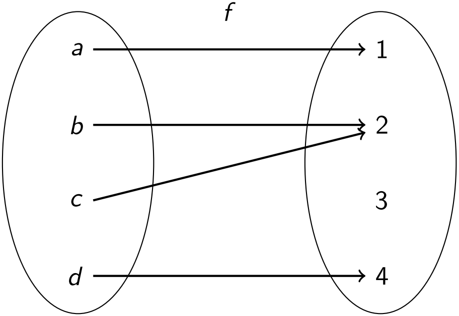
Dans l'exemple précédent, l'élément c n'ayant pas d'image : $D_f = \{a, b, d\}$.

Applications

Définition

Soient E et F deux ensembles. Si **à tout élément** x de E est associé un élément y de F par la fonction f alors on dit que f est une **application** de E vers F.

Exemple



f est une application de $E = \{a, b, c, d\}$ vers $F = \{1, 2, 3, 4\}$.

Applications

Remarque

Soient f une fonction de E vers F et D_f son ensemble de définition. Si $E = D_f$ alors f est une application de E vers F.

Pour qu'une fonction devienne une application, il suffit de réduire son ensemble de départ à son ensemble de définition.

Dans l'exemple précédent $E = \{a, b, c, d\} = D_f$.

Image - Image réciproque

Définition

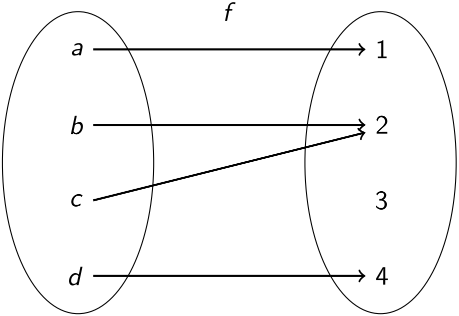
Soient E et F deux ensembles, A un sous-ensemble de E et B un sous-ensemble de F.

L'ensemble des images des éléments de A par f est appelé **image de** A **par** f. On le note $f(A)$.

L'ensemble des antécédents des éléments de B par f est appelé **image réciproque de** B. On le note $f^{-1}(B)$.

Image - Image réciproque

Exemple



$$f(\{a, c\}) = \{1, 2\}$$
$$f^{-1}(\{2, 3, 4\}) = \{b, c, d\}$$

Exercice 1

On considère la fonction f de $E = \{a, b, c, d\}$ vers $F = \{1, 2, 3, 4, 5\}$ définie par : $f(a) = 2$; $f(b) = 3$; $f(c) = 5$; $f(d) = 3$.

1. Donner la représentation sagittale de f.
2. Quel est le domaine de définition D_f de f ? Est-ce que f est une application ?
3. Quelle est l'image de $A = \{a, b, d\}$ par f ?
4. Quelle est l'image réciproque de $B = \{1, 2, 5\}$ par f ?

Injection – Surjection – Bijection

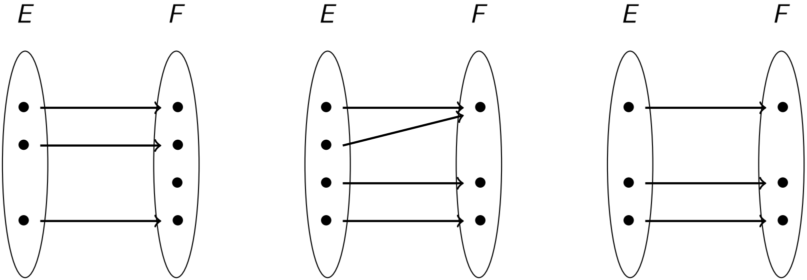
Définition

Soient E et F deux ensembles, et f est une application de E dans F. On dira que :

- f est une **injection** de E dans F si tout élément y de F admet **au plus** un antécédent x de E.
- f est une **surjection** de E sur F si tout élément y de F admet **au moins** un antécédent x de E.
- f est une **bijection** de E sur F si tout élément y de F admet **un et un seul** antécédent x de E.

Injection – Surjection – Bijection

Exemple



Injection   surjection   bijection

Injection – Surjection – Bijection

Pour déterminer si l'application f de E dans F est une injection, une surjection ou une bijection, on remarquera que pour a élément donné de F :

- si l'équation $f(x) = a$ admet **au plus** une solution x dans E alors f est une **injection** ;
- si l'équation $f(x) = a$ admet **au moins** une solution x dans E alors f est une **surjection** ;
- si l'équation $f(x) = a$ admet **une et une seule** solution x dans E alors f est une **bijection**.

Exercice 2

On considère la fonction f de $E = \{a, b, c, d\}$ vers $F = \{1, 2, 3, 4, 5\}$ définie par : $f(a) = 2$; $f(b) = 3$; $f(c) = 5$; $f(d) = 3$.

1. Résoudre dans E les équations d'inconnue x : $f(x) = 3$ et $f(x) = 1$.
2. Est-ce que f est injective ? Surjective ? Bijective ?

Injection – Surjection – Bijection

Exemple : le bit de parité

Etant donné un nombre représenté en base 2 par $A = a_n a_{n-1} \ldots a_2 a_1$, le bit de parité est défini comme :

$$\beta = \sum_{i=1}^{n} a_i \quad (mod\, 2)$$

Autrement dit, le bit de parité vaut 0 si le nombre de 1 est pair, et il vaut 1 si le nombre de 1 est impair.

Exercice 3

Intégrité d'une adresse IPv4

Prenons par exemple le cas d'une adresse IPv4 de 32 bits que l'on découpe en 4 mots de 8 bits :
255.245.26.53 s'écrit en binaire
11111111 11110101 00011010 00110101
sur lequel nous calculons une clé de contrôle de la forme $abcd$ où a, b, c et d sont les bits de parités de chaque mot de 8 bits.
Nous avons ainsi une application p de l'ensemble des mots des adresses IPv4 exprimées en binaire vers l'ensemble des mots de 4 bits.
Nous appellerons E l'ensemble des mots des adresses IPv4 exprimées en binaire et F l'ensemble des mots de 4 bits

1. Déterminer la clé de contrôle du nombre ci-dessus
2. Décrire l'ensemble F, en citant tous ses éléments.
3. Cette application p est-elle injective ? Justifier.
4. Cette application p est-elle surjective ? Justifier.
5. Cette application p est-elle bijective ? Justifier

Exercice 4

Pour s'échanger des messages codés, Alice et Bob utilisent leur clavier téléphonique. Le chiffre 2 sert à coder les lettres A, B, C ; le chiffre 3 sert à coder les lettres D, E, F, etc.

1. Quel nombre Alice va-t-elle envoyer à Bob pour lui dire BRAVO ?
2. Bob est-il sûr de comprendre ?
3. Quelle propriété de l'application : lettre $\mapsto$ chiffre n'est pas respectée, qui permettrait de décoder le message de façon certaine ?
4. Proposer une adaptation de la méthode permettant d'avoir un décodage unique.

Exercice 5

1. Pour un certain type de codage, on a besoin de coder les lettres A, B, C, D. On commence par attribuer un nombre à chaque lettre : A $=0$, B $=1$, C $=2$, D $=3$. Puis on multiplie par 2 le nombre et on ajoute 3. On cherche ensuite le reste de la division euclidienne par 4. A ce reste correspond alors une lettre qui est la lettre cryptée.
   Comment seront cryptées les lettres A, B, C, D ? Ce type de codage est-il acceptable ?
2. On décide de modifier le procédé. On multiplie par 3 le nombre et on ajoute 2. Et on cherche encore le reste de la division euclidienne par 4. Vérifier que l'on a un codage bijectif.