Ensembles

Partie 2 : Théorie des ensembles

Laurent Debize

BTS SIO

Produit cartésien de deux ensembles

Définition

Soient deux ensembles A et B. On appelle produit cartésien de A et B, et l'on note $A \times B$ (lire ≪ A croix B), l'ensemble des couples (x, y) tels que $x \in A$ et $y \in B$, soit encore :

$$A \times B = \{(x, y) \,|\, x \in A \wedge y \in B\}$$

Exemple

Si $A = \{1, 2, 3\}$ et $B = \{a, b\}$,
alors $A \times B = \{(1, a), (1, b), (2, a), (2, b), (3, a), (3, b)\}$

Produit cartésien de deux ensembles

Remarques

- Les éléments de $A \times B$ sont des couples : $(x, y) \neq (y, x)$
  et non des paires : $\{x, y\} = \{y, x\}$
- $A \times B \neq B \times A$
- On note $A \times A = A^2$, $A \times A \times A = A^3$, $A \times A \times \ldots \times A = A^n$ (ici A est présent n fois), ensembles formés respectivement de couples, de triplets, de n-uplets.

Exercice 1

Propriétés des cardinaux d'ensembles

Propriété

Si A et B sont deux **ensembles finis disjoints**, c'est-à-dire tels que $A \cap B = \varnothing$, alors :

$$card(A \cup B) = card(A) + card(B)$$

Si (A_i) est une suite finie d'ensembles finis **deux à deux disjoints**, c'est-à-dire pour lesquels $A_i \cap A_j = \varnothing$ (pour tous indices $i \neq j$), alors :

$$card(\bigcup_{i=1}^{n} A_i) = card(A_1) + card(A_2) + \ldots + card(A_n)$$

Remarque

La somme $card(A_1) + card(A_2) + \ldots + card(A_n)$ est notée $\sum_{i=1}^{n} card(A_i)$

Propriétés des cardinaux d'ensembles

Propriété

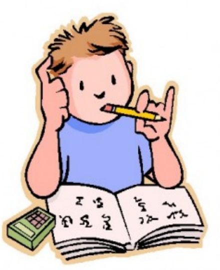
Soit Ω un ensemble. Si A et B sont deux sous-ensembles de Ω, alors :

$$card(A \cup B) = card(A) + card(B) - card(A \cap B)$$

Exemple

Dans une classe, 18 élèves font de l'anglais, 10 de l'espagnol et 7 font les deux langues.
Combien d'élèves sont dans la classe, si tous font au moins une langue ?

Exercices 2 et 3



Propriétés des cardinaux d'ensembles

Propriété

Si A et B sont deux ensembles finis tels que $A \subset B$ alors

$$card(A) \leq card(B)$$

Propriété

Soient Ω un référentiel et A un sous-ensemble de Ω, alors :

$$card(\overline{A}) = card(\Omega) - card(A)$$

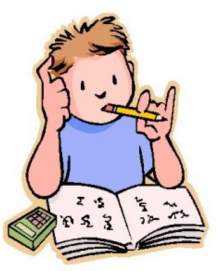
Propriété

Si A et B sont des ensembles finis, alors :

$$card(A \times B) = card(A) \times card(B)$$

Et pour n entier naturel : $card(A^n) = card(A)^n$

Exercice 4



Exercice

On donne l'algorithme suivant :

```
Variables :
i, j, k, S (entiers)
Début
   S <- 0
   Pour i de 1 à 3 Faire
      Pour j de 1 à 50 Faire
         Pour k de 1 à 12 Faire
            S <- S+1
         FinPour
      FinPour
   FinPour
   Afficher S
Fin
```

Quelle valeur affiche l'algorithme ?
Ecrire S comme le cardinal d'un produit d'ensembles à préciser.

Relation binaire

Définition

Soit E un ensemble. On appelle **relation** $\mathcal{R}$ sur E, tout partie de E^2.
L'élément (x, y) de E est alors noté : $x\mathcal{R}y$.

Exemples

- Dans $\mathbb{R}$, l'inégalité est une relation. $x\mathcal{R}y$ est défini par : $x \leqslant y$
- Dans $\mathbb{N}$, la congruence modulo n est une relation. $x\mathcal{R}y$ est défini par : $x \equiv y\,[n]$

Relation d'ordre

Définition

Soit E un ensemble. Soit $\mathcal{R}$ une relation sur E. On dit que $\mathcal{R}$ est une **relation d'ordre** si :

- la relation est **réflexive** : $\forall x \in E, x\mathcal{R}x$
- la relation est **transitive** : $\forall (x, y, z) \in E^3, [x\mathcal{R}y \text{ et } y\mathcal{R}z] \Rightarrow x\mathcal{R}z$
- la relation est **anti-symétrique** :
  $\forall (x, y) \in E^2, [x\mathcal{R}y \text{ et } y\mathcal{R}x] \Rightarrow x = y$

On dit que la relation d'ordre $\mathcal{R}$ est **totale** si tous les éléments de E sont comparables entre eux :

$$\forall (x, y) \in E^2, [x\mathcal{R}y \text{ ou } y\mathcal{R}x]$$

Dans le cas contraire, on dit que la relation d'ordre est **partielle**.

Relation d'ordre

Exemple

Dans $\mathbb{R}$, la relation $\leqslant$ est une relation d'ordre
Cette relation d'ordre est totale.

Relation d'équivalence

Définition

Soit E un ensemble. Soit $\mathcal{R}$ une relation sur E. On dit que $\mathcal{R}$ est une **relation d'équivalence** si :

- la relation est **réflexive** : $\forall x \in E, x\mathcal{R}x$
- la relation est **transitive** : $\forall (x, y, z) \in E^3, [x\mathcal{R}y \text{ et } y\mathcal{R}z] \Rightarrow x\mathcal{R}z$
- la relation est **symétrique** : $\forall (x, y) \in E^2, x\mathcal{R}y \Rightarrow y\mathcal{R}x$

Relation d'équivalence

Exemple

- Dans $\mathbb{N}$, la relation de congruence modulo n :

$$x\mathcal{R}y \Leftrightarrow x \equiv y\,[n]$$

est une relation d'équivalence.

Exercices

Pour les différentes relations $\mathcal{R}$ ci-dessous, déterminer si $\mathcal{R}$ est réflexive, transitive, symétrique ou anti-symétrique. En déduire quelles relations sont des relations d'ordre ou d'équivalence. Déterminer ensuite si ce sont des relations totales ou partielles.

- Dans $\mathbb{R}$, $x\mathcal{R}y \Leftrightarrow x < y$
- Dans $\mathbb{N}$, $x\mathcal{R}y \Leftrightarrow x$ est un diviseur de y
- Dans $\mathbb{N}$, $x\mathcal{R}y \Leftrightarrow x + y$ est un multiple de 2
- Soit E un ensemble contenant au moins deux éléments. Dans $\mathcal{P}(E)$, $A\mathcal{R}B \Leftrightarrow A \subset B$
- Sur $\mathbb{R}^2$ la relation définie par

$$(x, y) \preceq (x', y') \Leftrightarrow \begin{cases} x < x' \\ \text{ou} \\ x = x' \text{ et } y \leqslant y' \end{cases}$$

Propriétés des opérations définies sur les ensembles

Les propriétés des opérations $\cup$, $\cap$ et $\overline{A}$ définies sur $\mathcal{P}(E)$ correspondent aux propriétés des opérations logiques $\vee$, $\wedge$ et $\neg$. Ces propriétés sont donc identiques.
Elles peuvent être aisément représentées à l'aide de diagrammes de Venn.

Propriété de l'inclusion

- Pour tout ensemble A, $A \subset A$ (réflexivité)
- Si A, B et C sont trois ensembles tels que $A \subset B$ et $B \subset C$, alors $A \subset C$ (transivité)
- Si $A \subset B$ et $B \subset A$ alors $A = B$ (antisymétrie)

Propriétés des opérations définies sur les ensembles

Propriété du complémentaire

- Si Ω est le référentiel, alors $\overline{\Omega} = \varnothing$ et $\overline{\varnothing} = \Omega$
- $\overline{\overline{A}} = A$
- Si $A \subset B$ alors $\overline{B} \subset \overline{A}$

Propriétés des opérations définies sur les ensembles

Propriété de la réunion

- Idempotence : $A \cup A = A$
- Commutativité : $A \cup B = B \cup A$
- Associativité : $(A \cup B) \cup C = A \cup (B \cup C)$ que l'on peut noter $A \cup B \cup C$
- Si A et B sont inclus dans C, alors $A \cup B$ est inclus dans C :

$$(A \subset C) \wedge (B \subset C) \Rightarrow A \cup B \subset C$$

- Si $A \subset B$, alors $A \cup B = B$
- $A \cup \varnothing = A$ et $A \cup \Omega = \Omega$ (Ω étant le référentiel)

Propriétés des opérations définies sur les ensembles

Propriété de l'intersection

- Idempotence : $A \cap A = A$
- Commutativité : $A \cap B = B \cap A$
- Associativité : $(A \cap B) \cap C = A \cap (B \cap C)$ que l'on peut noter $A \cap B \cap C$
- Si A et B sont inclus dans C, alors $A \cap B$ est inclus dans C :

$$(A \subset C) \wedge (B \subset C) \Rightarrow A \cap B \subset C$$

- Si $A \subset B$, alors $A \cap B = A$
- $A \cap \varnothing = \varnothing$ et $A \cap \Omega = A$ (Ω étant le référentiel)

Propriétés des opérations définies sur les ensembles

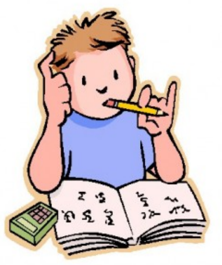
Distributivité

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

Lois de De Morgan

- $\overline{A \cup B} = \overline{A} \cap \overline{B}$
- $\overline{A \cap B} = \overline{A} \cup \overline{B}$

Exercice 5



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

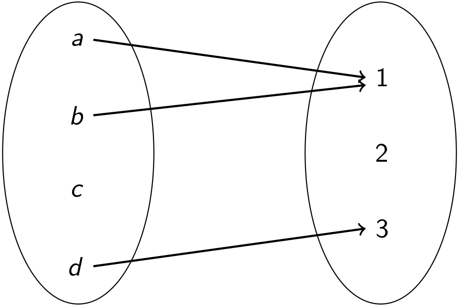
L'élément $f(x)$ est appelé **image** de x par la fonction f.

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.

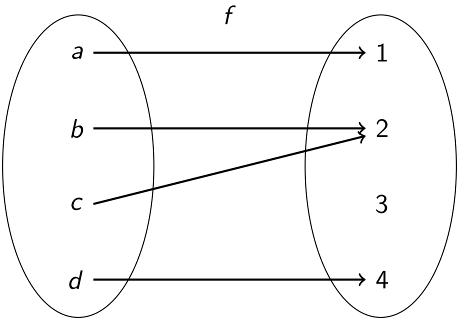
Dans l'exemple précédent, l'élément c n'ayant pas d'image :
$D_f = \{a, b, d\}$.

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

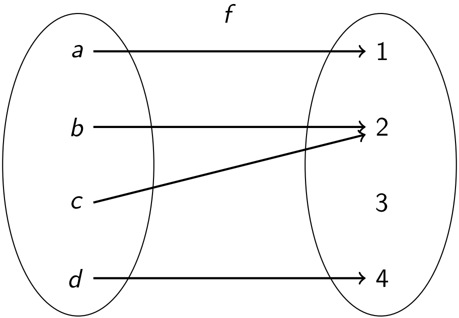
Soient E et F deux ensembles, A un sous-ensemble de E et B un sous-ensemble de F.

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 6

Injection – Surjection – Bijection

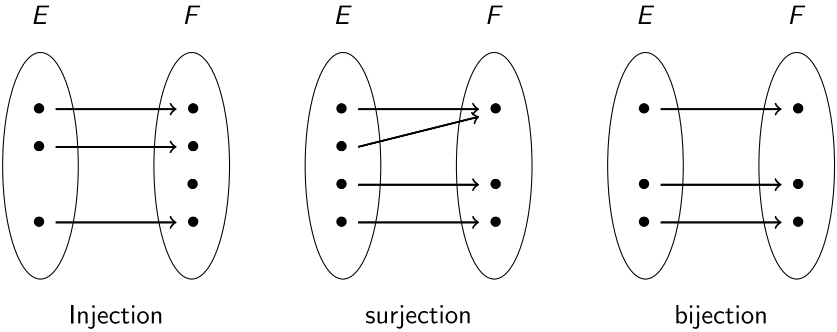
Définition

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

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 7

Injection – Surjection – Bijection

Exemple : le bit de parité

Etant donné un nombre représenté en base 2 par $A = a_n a_{n-1} \dots a_2 a_1$, 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.

Injection – Surjection – Bijection

Exemples : 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
6. Que représente $p^{-1}(\{1101\})$?
7. Quel est le cardinal de $p^{-1}(\{1101\})$?
8. Soit b l'application de F vers G où $G = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15\}$ qui à tout mot de 4 bits associe sa valeur en base 10. Réaliser un diagramme sagittal de cette application b. L'application b est-elle une bijective ? Justifier.

Composition d'applications

Définition

Soient f une application de E dans F et g une application de F dans G.
On appelle application composée de f par g l'application notée $g \circ f$ définie de E vers G par : $g \circ f(x) = g[f(x)]$.
$g \circ f$ se lit « g rond f ».

Exemple

1. Calculer $b \circ p(11111111\,10101010\,00001111\,10111010)$
2. Que dire de $p \circ b(11111111\,10101010\,00001111\,10111010)$?

Composition d'applications

Propriété

La composition des applications n'est pas commutative, c'est-à-dire que si f et g sont deux applications alors $f \circ g$ n'est pas toujours égale à $g \circ f$.

Propriété

Soient $f : E \to F$, $g : F \to G$ et $h : G \to H$ trois applications.
Alors $(h \circ g) \circ f = h \circ (g \circ f)$.
La composition des applications est donc associative, et l'on peut noter :

$$h \circ g \circ f = (h \circ g) \circ f = h \circ (g \circ f)$$

Composition d'applications

1. L'application $b \circ p$ est-elle injective ? Justifier.
2. L'application $b \circ p$ est-elle surjective ? Justifier

Composition d'applications

Propriété

Soient $f : E \to F$ et $g : F \to G$ deux applications.

1. Si f et g sont injectives, alors $g \circ f$ aussi
2. Si f et g sont surjectives, alors $g \circ f$ aussi
3. Si f et g sont bijectives, alors $g \circ f$ aussi

Exercices

Exercice 1

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.

Exercices

Exercice 2

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.