Chapitre 1. Ensembles et applications.

Table des matières

1. Ensembles: introduction

2. Ensembles finis

1. Ensembles: introduction

Définition

On appelle *ensemble* une collection des objets. Ces objets sont appelés *les éléments* de l'ensemble.

Exemples

1) $\mathbb{N} =$ l'ensemble de tous les nombres entiers positifs.
2) $\mathbb{Z} =$ l'ensemble de tous les nombres entiers relatifs.
3) $\mathbb{Q} =$ l'ensemble des nombres rationnels $\frac{m}{n}$, $m, n \in \mathbb{Z}$, $n \neq 0$.
4) $\mathbb{R} =$ l'ensemble des nombres réels.
5) $\mathbb{R}_+ =$ l'ensemble des nombres réels positifs.
6) $\mathbb{R}_* =$ l'ensemble des nombres réels non nuls.

Terminologie de la théorie des ensembles

Si x est un élément d'un ensemble A, on ecrit $x \in A$. Si non, on écrit $x \notin A$. Par exemple $2 \in \mathbb{N}$, $\frac{2}{3} \notin \mathbb{N}$.

On peut définir un ensemble par la liste de ses éléments. Par exemple, l'ensemble contenant le seul élément 0 est noté $\{0\}$. L'ensemble contenant trois éléments $1, 2, 3$ est noté par $\{1, 2, 3\}$.
Une autre façon de définir un ensemble c'est d'indiquer la propriété à laquelle vérifient tous les éléments de cet ensemble et seulement ces éléments. L'ensemble de tous les éléments vérifiant propriété P est noté $\{x \mid P\}$.

Exemple

l'ensemble de tous les nombres naturels strictement supérieurs à 2 est noté

$$\{x \in \mathbb{N} \mid x > 2\}.$$

Définition

L'ensemble ne contenant aucun élément est appelé *l'ensemble vide* et noté $\varnothing$.

Définition

Soit E, F des ensembles. Si chaque élément de E est aussi un élément de F, on dit que E est *une partie (ou sous-ensemble)* de F et on écrit $E \subset F$. Si $E \subset F$ et $E \neq F$ alors on dit que E est un *sous-ensemble propre* de E et on écrit $E \subsetneqq F$.

Exemples

1) $\mathbb{N} \subset \mathbb{Z}$.
2) $\mathbb{Z} \subset \mathbb{Q}$.
3) quel que soit un ensemble E on a: $\varnothing \subset E$ et $E \subset E$.

Pour un ensemble A, l'ensemble de tous les sous-ensembles de A est noté 2^A ou $P(A)$.

Exemple

Soit $A = \{0, 1\}$. Les sous-ensembles de A sont $\varnothing$, A, $\{0\}$, $\{1\}$ donc $P(A) = \big\{\varnothing, \{0, 1\}, \{0\}, \{1\}\big\}$.

Définition

Soit A, B des ensembles. L'ensemble qui contient tous les éléments qui appartiennent à la fois à A et à B est appelé *l'intersection de* A, B et noté $A \cap B$.

Autrement dit $(x \in A \cap B) \iff ((x \in A)$ et $(x \in B))$.

Exemple

$\{0, 1\} \cap \{2, 1\} = \{1\}$

Définition

Soit A, B des ensembles. L'ensemble des éléments x tels que $x \in A$ ou $x \in B$ est appellé *la réunion de* A *et* B et noté $A \cup B$.

Exemple

On note par $\mathbb{Z}_-$ l'ensemble de tous les nombres entiers négatifs (y compris 0). On a alors $\mathbb{N} \cup \mathbb{Z}_- = \mathbb{Z}$ et $\mathbb{N} \cap \mathbb{Z}_- = \{0\}$.

Définition

Si A, E sont des ensembles, alors l'ensemble $\{x \in E \mid x \notin A\}$ est appelé *complémentaire de* A *dans* E, et noté $E \setminus A$.
Si $A \subset E$, l'ensemble $E \setminus A$ est noté aussi C_A.

Exemple

Quel que soit un ensemble E on a: $C_{\varnothing} = E$ et $C_E = \varnothing$.

Règles de calcul

Intersection et réunion sont commutatives:
$A \cap B = B \cap A, \quad A \cup B = B \cup A,$
et associatives:
$A \cap (B \cap C) = (A \cap B) \cap C, \qquad A \cup (B \cup C) = (A \cup B) \cup C.$
On a:
$A \cup A = A \cap A = A, \quad A \cap \varnothing = \varnothing, A \cup \varnothing = A.$

Proposition

$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ *(l'intersection est distributive par rapport à la réunion).*

Démonstration. On va montrer d'abord que $A \cap (B \cup C) \subset (A \cap B) \cup (A \cap C)$.
Si $x \in A \cap (B \cup C)$, alors $x \in A$ et $\big(x \in B$ ou $x \in C\big)$. Donc $\big(x \in A$ et $x \in B\big)$ ou bien $\big(x \in A$ et $x \in C\big)$. Autrement dit $x \in A \cap B$ ou $x \in A \cap C$. Ce qui est équivalent à $x \in (A \cap B) \cup (A \cap C)$.
De la même façon, on vérifie que $(A \cap B) \cup (A \cap C) \subset A \cap (B \cup C)$.
Donc chacun de deux ensembles de notre énoncé fait partie de l'autre. Cela veut dire qu'ils sont égaux. □

Exercice

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

Proposition

Soit E un ensemble et A, $B \subset E$. Alors $C_{A \cup B} = C_A \cap C_B$ et $C_{A \cap B} = C_A \cup C_B$.

Démonstration. Nous avons

$$x \in C_{A \cup B} \iff \neg(x \in A \cup B) \iff \neg\Big((x \in A) \vee (x \in B)\Big)$$

Par la loi de De Morgan on a

$$\neg\Big((x \in A) \vee (x \in B)\Big) \iff \Big(\neg(x \in A) \wedge \neg(x \in B)\Big)$$

La dernière assertion est équivalente à $(x \in C_A) \wedge (x \in C_B)$, d'où

$$x \in C_{A \cup B} \iff x \in C_{A \cap B}.$$

La démonstration de la deuxième formule est similaire. □

Définition

Soit A, B des ensembles. L'ensemble de tous les couples ordonnés (x, y) tels que $x \in A$, $y \in B$ est appellé *le produit cartésien* de A et B, noté $A \times B$.

Exemple

$A = \mathbb{R}$, $B = \mathbb{R}$ alors $A \times B = \mathbb{R} \times \mathbb{R}$ est identifié avec le plan euclidien. (faire le dessin!)
NB. L'ordre de deux composantes d'un couple est important:
$(x, y) \neq (y, x)$ comme on le voit sur le dessin.

Remarque

Nous avons décrit quelques procédures précises qui permettent de construire des nouveaux ensembles à partir des ensembles déjà existants. Il se trouvent que toutes les façons de construire des ensembles ne sont pas bonnes. On peut montrer par exemple que *l'ensemble de tous les ensembles n'existe pas*, c'est-à-dire l'hypothèse de l'existence de cet ensemble mène à une contradiction.

Applications

Définition

Soit A, B des ensembles. Une loi qui associe à chaque élément x de A un unique élément y de B est appellée *application* ou *fonction* de A dans B. On écrit

$$f : A \to B, \qquad \text{ou} \qquad A \xrightarrow{f} B$$

Pour un élement $x \in A$ l'élément de B qui lui est associé est noté $f(x)$, et on écrit $x \longmapsto f(x)$. L'élément $f(x)$ est appelé *l'image de x par f* et x est dit *l'antécédent* de $f(x)$.

Exemples

1) $\mathbb{R} \xrightarrow{f} \mathbb{R}$ définie par la formule $f(x) = \sin(x)$ est une application de $\mathbb{R}$ dans $\mathbb{R}$. L'élément $0 \in \mathbb{R}$ a un nombre infini d'antécédents, notamment, pour tout $k \in \mathbb{Z}$ le nombre $k\pi$ est un antécédent de 0.
2) La formule $f(n) = n^2$ définit une application de $\mathbb{N}$ dans lui-même.

Dans les exemples précédents les fonctions ont été définies par des formules (polynômiales, trigonométriques etc.); ce n'est pas un seul moyen de définir des fonctions comme le montre l'exemple suivant.
Fonction de Dirichlet: $\chi : \mathbb{R} \longrightarrow \mathbb{R}$,

$$\chi(x) = 1 \qquad \text{si} \qquad x \in \mathbb{Q}$$
$$\chi(x) = 0 \qquad \text{si} \qquad x \notin \mathbb{Q}$$

Définition

Soit $f : A \longrightarrow B$ une application. Le sous-ensemble $\{(x, f(x)) \mid x \in A\} \subset A \times B$ est dit *le graphe de f* et noté Γ_f.

Exemples

1) Soit $f : \mathbb{R} \to \mathbb{R}$ la fonction donnée par: $f(x) = x$. Alors son graphe Γ_f est une ligne droite dans le plan euclidien $\mathbb{R}^2$, notamment la bissectrice de l'angle droit formé de deux axes de coordonnées. (faire les dessins!)
2) Soit $f : \mathbb{R} \to \mathbb{R}$ la fonction donnée par: $f(x) = 0$. Alors son graphe Γ_f est l'axe des abscisses.

Définition

Soit $f : A \longrightarrow B, \quad g : B \longrightarrow C$ des applications. L'application de A dans C qui associe à chaque $x \in A$ l'élément $g(f(x))$ de C est appelée *l'application composée* (où simplement *la composée*) de f et g, et notée $g \circ f$.

Exemple

Soit $f : \mathbb{R} \to \mathbb{R}$ l'application définie par la formule $f(x) = x^3$. Alors pour l'application $g = f \circ f$ on a $g(x) = (x^3)^3 = x^{27}$.

Exercice

Calculer $f \circ g$ où $f, g : \mathbf{R}_+^* \to \mathbf{R}_+^*$ sont les applications suivantes:

1) $f(x) = x, \quad g(x) = \frac{1}{x}$;

2) $f(x) = \frac{1}{x}, \quad g(x) = \frac{1}{x}$;

3) $f(x) = \frac{1}{x}, \quad g(x) = \frac{1}{x^2}$.

Remarque

En géneral $f \circ g \neq g \circ f$ même si f, g sont des applications d'un ensemble A dans lui-même. Par example, si $f(x) = x^3$, $g(x) = 2x$ (des applications de $\mathbb{R}$ dans $\mathbb{R}$) on a

$$(f \circ g)(x) = 8x^3, \qquad (g \circ f)(x) = 2x^3.$$

Définition

Soit A un ensemble, et $B \subset A$. L'application qui à chaque élément $x \in B$ associe x lui-même considéré comme un élément de A est appelée *l'application inclusion*. Si $B = A$ cette application est appelée *l'application identité* de A et notée Id_A.

Définition

Soit $f : A \to B$ une application, et $A' \subset A$. La composée de l'application inclusion et de f est appelée *la restriction de f sur A'* et notée $f|A' : A' \to A$.
C'est-à-dire $(f|A')(x) = f(x)$ pour tout $x \in A'$.

Définition

Une application $f : A \longrightarrow B$ est dite *injective* si

$$f(x) = f(y) \Longrightarrow (x = y)$$

(c'est-à-dire si $z \in B$ admet un antécédent dans A, alors cet antécédent est unique.)

Définition

Une application $f : A \longrightarrow B$ est dite *surjective* si:

$$\forall z \in B, \quad \exists x \in A \text{ tel que } f(x) = z$$

(c'est-à-dire chaque z dans B admet un antécédent dans A).

Exemples

1) $f(x) = \sin(x)$ n'est pas injective car $f(0) = f(\pi) = 0$ et n'est pas surjective car $\forall x \ \ |\sin(x)| \leqslant 1$.

2) En revanche, la fonction $h : \mathbb{R} \longrightarrow [-1; 1]$ définie par $h(x) = \sin(x)$ est surjective.
3) La fonction $g : \mathbb{N} \longrightarrow \mathbb{N} \quad g(n) = n^2$ est injective mais elle n'est pas surjective (vérifiez!).

Graphe d'une fonction surjective:
pour chaque y la droite l_y intersecte le graphe Γ_f. (faire les dessins!)
Graphe d'une fonction f injective:
Chaque droite l_y intersecte Γ_f une fois maximum.

Définition

Une application qui est injective et surjective est dite *bijective* (ou *une bijection*).
Donc f est bijective si et seulement si chaque $y \in B$ admet un unique antécédent dans A.

Exemples

1) $f : \mathbb{Z} \longrightarrow \mathbb{Z}, \quad f(x) = -x$ est bijective (car chaque $y \in \mathbb{Z}$ admet un unique antécédent par rapport à f, notamment $-y$).

2) On va construire une bijection $\mathbb{N} \xrightarrow{\varphi} \mathbb{Z}$. Posons

$$\varphi(x) = \begin{cases} \frac{x}{2} & \textit{si x est pair;} \\ -\frac{x+1}{2} & \textit{si x est impair.} \end{cases}$$

Vérifions que φ est injective.
Supposons que $\varphi(x) = \varphi(y)$ alors
• si $\varphi(x) \geqslant 0$ alors x est pair, y aussi et $\frac{x}{2} = \frac{y}{2}$, soit $x = y$.
• si $\varphi(x) < 0$ alors x et y sont impairs et $-\frac{x+1}{2} = -\frac{y+1}{2} \Longrightarrow x = y$.
Vérifions que φ est surjective.
Soit $n \in \mathbb{N}$ alors $n = \varphi(2n)$, $2n \in \mathbb{N}$.
Soit $m \in \mathbb{Z}, m < 0$. Alors $m = \varphi(-2m - 1)$ où $-2m - 1 \in \mathbb{N}$.

Remarque

L'ensemble $\mathbb{N}$ est un sous-ensemble propre de $\mathbb{Z}$, c'est-à-dire $\mathbb{N} \subset \mathbb{Z}$, et $\mathbb{N} \neq \mathbb{Z}$. Cependant on a établi une bijection entre $\mathbb{N}$ et $\mathbb{Z}$ ce qui veut dire que $\mathbb{N}$ contient "autant d'élements" que $\mathbb{Z}$.

3) L'application

$$f : [0, 1] \to [0, 2]; \quad f(t) = 2t$$

est une bijection. (Rappelons que $[a, b] = \{x \in \mathbb{R} \mid a \leqslant x \leqslant b\}$.)
En effet, montrons d'abord que f est injective. Si $f(x) = f(y)$, alors $2x = 2y$ ce qui implique $x = y$. Montrons maintenant que f est surjective. Soit $y \in [0, 2]$. Posons $x = y/2$, alors $x \in [0, 1]$ et $f(x) = 2x = y$.

Exercice

Soit a, b nombres réels et $a < b$. Montrer que l'application

$$g : [0, 1] \to [a, b]; \qquad f(t) = a + t \cdot (b - a)$$

est bijective.

Définition

Soit $f : A \longrightarrow B$ une application.
• Soit $X \subset A$, alors le sous-ensemble

$$\{y \in B \mid y = f(x) \ \text{ pour un } x \in X\}$$

est appelé *l'image de X par f*, noté $\mathrm{Im}\ X$. L'image de A est noté aussi par $\mathrm{Im}\ (f)$. f est surjective si et seulement si $\mathrm{Im}\ (f) = Y$.
• Soit $Y \subset B$, le sous-ensemble

$$\{x \in A \mid f(x) \in Y\}$$

est appelé *l'image réciproque de Y par f* noté $f^{-1}(Y)$.

Exemple

Soit $f : \mathbb{R} \longrightarrow \mathbb{R}$, $f(x) = x^2$. Alors $\mathrm{Im}\ (f) = \mathrm{Im}\ (\mathbb{R}) = \mathbb{R}_+$ et $f^{-1}(\{1\}) = \{-1; 1\}$.

Proposition

1) La composée de 2 applications injectives est injective.
2) La composée de 2 applications surjectives est surjective.
3) La composée de 2 applications bijectives est bijective.

Démonstration. 1) Soit $A \xrightarrow{f} B \xrightarrow{g} C$ où f, g sont des applications injectives. Pour montrer que $g \circ f$ est injective, supposons que $(g \circ f)(x) = (g \circ f)(y)$, pour $x, y \in A$.
Alors $g(f(x)) = g(f(y))$. Puisque g est injective, cela implique $f(x) = f(y)$. De plus, f étant injective, on déduit $x = y$.
Donc $(g \circ f)$ est injective.

2) Soit $A \xrightarrow{f} B \xrightarrow{g} C$, où f, g sont des applications surjectives.
Soit $z \in C$. L'application g étant surjective, il existe $y \in B$ tel que $g(y) = z$.

De plus, f étant surjective, il existe $x \in A$ tel que $f(x) = y$.
Finalement $z = g(y) = g(f(x)) = (g \circ f)(x)$ et l'application $g \circ f$ est surjective.
3) découle de 1) et 2). $\square$

Définition

(Rappel). Soit A un ensemble. On note Id_A l'application $A \to A$ définie par $\mathrm{Id}_A(x) = x$. On l'appelle *l'application identité*.

Proposition

Soit $f : A \longrightarrow B$ une application. Alors f est bijective si et seulement si il existe une application $g : B \longrightarrow A$, telle que

$$g \circ f = \mathrm{Id}_A \quad \text{et} \quad f \circ g = \mathrm{Id}_B.$$

g est appelée l'application réciproque à f, et notée f^{-1}.

Démonstration.
Premièrement, supposons qu'il existe $g : B \longrightarrow A$, tel que $f \circ g = \mathrm{Id}_B$, $g \circ f = \mathrm{Id}_A$, et montrons que f est bijective.

Remarquons que f est injective. En effet, si $f(x) = f(y)$ alors $g(f(x)) = g(f(y))$ donc $(g \circ f)(x) = (g \circ f)(y)$. Or $(g \circ f)(x) = \mathrm{Id}_B(x) = x$, de même pour y; donc $x = y$.
De plus f est surjective, car si $y \in B$, $y = \mathrm{Id}_B(y) = (f \circ g)(y) = f(z)$, avec $z = g(y)$, donc $y \in f(A)$. On en déduit que f est bijective.

Deuxièmement, soit $f : A \longrightarrow B$ une bijection.
Alors $\forall y \in B$, $\exists x \in A$ tel que $f(x) = y$ (car f est surjective). On pose $g(y) = x$ (un tel x est unique, puisque f est injective) et on obtient ainsi une application $g : B \longrightarrow A$.
Par définition on a $(g \circ f) = I_{d_A}$, $(f \circ g) = I_{d_B}$.

Corollaire

Il existe une bijection $g : \mathbb{Z} \longrightarrow \mathbb{N}$.

2 . Ensembles finis

Définition

Soit $n \geqslant 1$ un entier positif. On note par $[[1, n]]$ l'ensemble $\{1, 2, ..., n\}$.

Proposition

Soit $n, k \in \mathbb{N}_*$.
1) S'il existe une application injective $[[1, n]] \longrightarrow [[1, k]]$ alors $n \leqslant k$.
2) S'il existe une application surjective $[[1, n]] \longrightarrow [[1, k]]$ alors $n \geqslant k$.
3) S'il existe une application bijective $[[1, n]] \longrightarrow [[1, k]]$ alors $n = k$.

Démonstration. 1) Récurrence sur n.
Initialisation. Si $n = 1$, alors $k \geqslant 1 = n$, car $k \in \mathbb{N}_*$.
Hérédité. On suppose que notre proposition est déjà démontrée au rang n. Soit $f : [[1, n+1]] \longrightarrow [[1, k]]$ une application injective.
Supposons d'abord que $f(n+1) = k$. f étant injective, on a $f(s) < k$ pour $s < n+1$, donc $f([[1, n]]) \subset [[1, k-1]]$,
et on obtient une application injective $[[1, n]] \to [[1, k-1]]$.
Par l'hypothése de récurrence, $n \leqslant k-1$ donc $n+1 \leqslant k$.

3) Supposons mantenant que $f(n+1) = s$ et $1 \leqslant s \leqslant k-1$.
Soit $\sigma : [[1,k]] \longrightarrow [[1,k]]$ une bijection définie par la formule suivante:

$$\sigma(x) = \begin{cases} x & si\ x \neq s,\ x \neq k; \\ k & si\ x = s; \\ s & si\ x = k; \end{cases}$$

C'est-à-dire, σ permute les éléments s et k et laisse fixe tous les autres éléments de $[[1,k]]$.
L'application $(\sigma \circ f)$ est injective (en tant que la composée de deux applications injectives).
De plus $(\sigma \circ f)(n+1) = \sigma(f(n+1)) = \sigma(s) = k$;
en applicant à $\sigma \circ f$ le raisonnement précédent on obtient $n+1 \leqslant k$.

Exercice

Démontrer 2).

Le point 3) découle de 1) et 2). $\square$

Définition

Une ensemble E est appelé *ensemble fini*, si pour certain $n \in \mathbb{N}_*$ il existe une bijection $f : [[1, n]] \longrightarrow E$, ou si E est vide.
Le nombre n est appelé *la cardinalité de E* ou *le cardinal de E*, noté $\mathrm{card}\ (E)$ ou $\sharp E$. Par convention on pose $\mathrm{card}\ (\varnothing) = 0$.

Autrement dit un ensemble est fini s'il existe une suite finie $a_1, ..., a_n$, $(a_i \in E)$ telle que chaque élément de E apparaît une seule fois dans cette suite. La donnée d'une bijection $f : [[1, n]] \longrightarrow E$ est équivalente à celle d'une telle suite: $a_i = f(i)$.

Remarque

Pour un ensemble fini E le nombre n ci-dessus est unique. En effet si on a deux bijections

$$[[1, n]] \xrightarrow{f} E \xleftarrow{g} [[1, k]]$$

alors $g^{-1} \circ f : [[1, n]] \longrightarrow [[1, k]]$ est une bijection, donc $n = k$.

Exemple

L'ensemble de tous les nombres entiers positifs n tels que n est pair et $n < 20$ est fini, et sa cardinalité est égale à 10.

Exemple

L'ensemble de tous le nombres naturels $\mathbb{N}$ n'est pas fini.
En effet, supposons qu'il existe une bijection $f : [[1, n]] \longrightarrow \mathbb{N}$ pour certain n. Considèrons l'application inclusion $g : [[1, n+1]] \subset \mathbb{N}$. La composition de f^{-1} avec g serait une application injective

$$f^{-1} \circ g : [[1, n+1]] \longrightarrow [[1, n]]$$

ce qui est impossible.

Propriétés des cardinaux des ensembles finis

(les démonstrations seront omises ou juste esquissées).
1) Si A est un ensemble fini, et $f : A \to B$ une bijection, alors B est évidemment un ensemble fini, et $\mathrm{card}\ A = \mathrm{card}\ B$.
Cette propriété est importante: *s'il y a une bijection entre deux ensembles, alors leurs cardinalités sont les mêmes; il y a autant d'éléments dans l'un que dans l'autre*.
2) Soit A un ensemble fini, et $B \subset A$. Alors B est un ensemble fini et $\mathrm{card}\ B \leqslant \mathrm{card}\ A$.

Corollaire

$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ *ne sont pas finis.*

Démonstration. Chacun de ces ensemble contient l'ensemble infini $\mathbb{N}$. $\square$

3) Soit A, B des ensembles finis. Alors $A \cup B$ et $A \cap B$ sont des ensembles finis et on a

$$\text{card } A \cup B = \text{card } A + \text{card } B - \text{card } A \cap B.$$

(faire un dessin!)
4) Soit A, B, C des ensembles finis, alors $A \cup B \cup C$ est un ensemble fini et on a (en appliquant la formule précédente)

$$\text{card } (A \cup B \cup C) = \text{card } ((A \cup B) \cup C) =$$
$$= \text{card } A \cup B + \text{card } C - \text{card } ((A \cap B) \cup (A \cap C)).$$

or

$$\text{card } ((A \cap B) \cup (A \cap C)) = \text{card } (A \cap C) + \text{card } (A \cap B) - \text{card } (A \cap B \cap C).$$

Finalement

$$\text{card } (A \cup B \cup C) = \text{card } A + \text{card } B + \text{card } C$$
$$-\text{card } (A \cap B) - \text{card } (A \cap C) - \text{card } (B \cap C)$$
$$+\text{card } (A \cap B \cap C).$$

Exercice

Calculer $\text{card }(A \cup B \cup C \cup D)$ en fonction des cardinalités des ensembles A, B, C, D et leurs intersections.
Plus généralement, calculer $\text{card }(A_1 \cup ... \cup A_n)$.

Proposition

Soit A, B des ensembles finis. Alors $A \times B$ est un ensemble fini et $\text{card } A \times B = \text{card } A \times \text{card } B$.

Démonstration. Soit $A = \{a_1, ..., a_n\}$, $B = \{b_1, ..., b_m\}$, alors $\text{card } A = n$, $\text{card } B = m$.

Les éléments de $A \times B$ peuvent être arrangés dans un tableau rectangulaire $n \times m$:

$$\begin{array}{cccc} (a_1, b_1) & (a_1, b_2) & \dots & (a_1, b_m) \\ (a_2, b_1) & (a_2, b_2) & \dots & (a_2, b_m) \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \\ (a_n, b_1) & \dots & \dots & (a_n, b_m) \end{array}$$

On aura n lignes et m éléments dans chaque ligne. Donc au total $n \times m$ éléments. $\square$

Proposition

Soit X, Y des ensembles finis non vides.
1) Soit $f : X \longrightarrow Y$ une application injective. Alors $\mathrm{card}\ X \leqslant \mathrm{card}\ Y$ *et si* $\mathrm{card}\ Y = \mathrm{card}\ X$, *alors f est une bijection.*
2) Soit $g\colon X \longrightarrow Y$ une application surjective. Alors $\mathrm{card}\ X \geqslant \mathrm{card}\ Y$ *et si* $\mathrm{card}\ Y = \mathrm{card}\ X$, *alors g est une bijection.*

Démonstration.
1) Soit $n = \mathrm{card}\ X$, alors il existe une application bijective $h : [1, n] \longrightarrow X$. De même, soit $m = \mathrm{card}\ Y$, et $k : [1, m] \longrightarrow Y$ une bijection.
Alors $k^{-1} \circ f \circ h$: $[1, n] \longrightarrow [1, m]$ est une application injective, donc $n \leqslant m$.
Pour démontrer le deuxième point de 1) il nous faut un lemme.

Lemme

Soit g: $[1, n] \longrightarrow [1, n]$ une application injective.
Alors g est bijective.

Démonstration. Récurrence sur n.
Initialisation. Si $n = 1$ alors $[1, n] = 1$. Chaque application $\{1\} \longrightarrow \{1\}$ est une bijection et notre assertion est évidemment vraie.
L'hérédité: On suppose que notre Lemme est démontré au rang n. On procède au rang $n + 1$. Soit g: $[1, n + 1] \longrightarrow [1, n + 1]$ une application injective.

On va d'abord considérer un cas particulier:
α) Supposons que $g(n+1) = n+1$.
Alors $g(s) < n+1$ pour $s < n+1$, car g est injective.
L'image de $[1, n]$ par l'application g est donc contenu dans le sous-ensemble $[1, n]$, et on obtient une application injective $g|[1, n] : [1, n] \to [1, n]$. Par l'hypothèse de récurrence, cette application est bijective ce qui implique la bijectivité de g.
Maintenant on peut procéder au cas général; on va le déduire du cas particulier α) ci-dessus.
β) Soit $g(n+1) = s$ avec $1 \leqslant s \leqslant n$.
Soit $\sigma : [1, n+1] \longrightarrow [1, n+1]$ la bijection suivante

$$\sigma(x) = \begin{cases} x & si\ x \neq s, \quad x \neq n+1; \\ s & si\ x = n+1; \\ n+1 & si\ x = s. \end{cases}$$

C'est-à-dire σ permute les éléments s et $n+1$ et laisse fixe tous les autres éléments.
Alors $\sigma \circ g$ est une application injective et $(\sigma \circ g)(n+1) = n+1$.

En appliquant α), on déduit que $\sigma \circ g$ est une bijection. Donc $g = \sigma^{-1} \circ \sigma \circ g$ est une bijection en tant que la composée de deux bijections.
La partie 2) de la proposition est démontrée de la même façon; on va omettre la démonstration. $\square$

Proposition

Soit A, B des ensembles finis. On note A^B l'ensemble de toutes les applications de B dans A. Alors A^B est un ensemble fini et

$$\mathrm{card}\ A^B = (\mathrm{card}\ A)^{\mathrm{card}\ B}.$$

Démonstration. Soit $B = \{b_1, \ldots, b_m\}$. Une application $f : B \to A$ est une loi qui associe à chaque b_i un élément $f(b_i)$ de A.
La donnée d'une telle application est donc équivalente à celle d'une suite finie

$$\{f(b_1), f(b_2), \ldots, f(b_m)\}$$

de longueur m des éléments de A. Pour calculer le nombre de telles suites remarquons que chaque terme de la suite peut être n'importe quel élément de A, donc pour déterminer une telle suite il faut faire m fois un choix arbitraire d'un élément de A.
Chaque fois on a $\mathrm{card}\ A$ possibilités pour le choix, et au total on aura $\mathrm{card}\ A \cdot \mathrm{card}\ A \cdot \ldots \cdot \mathrm{card}\ A$ suites, où le nombre de facteurs du produit est égal à m.
On obtient donc $(\mathrm{card}\ A)^m$ suites; rappelons que $m = \mathrm{card}\ B$ et notre proposition est démontrée. $\square$

Proposition

Soit A, B des ensembles finis tel que $\mathrm{card}\ A = \mathrm{card}\ B = n$. Alors l'ensemble $\mathcal{M}$ de toutes les bijections $A \longrightarrow B$ est de cardinalité $n! = 1 \cdot 2 \cdot \ldots \cdot n$.

Démonstration. Récurrence sur n. *Initialisation.* Si $n = 1$, alors il y a une seule application de A dans A et elle est bijective, et $\mathrm{card}\ \mathcal{M} = 1 = 1!$.
Hérédité. Supposons que l'on a démontré déjà la proposition au rang n. Soit $\mathrm{card}\ A = \mathrm{card}\ B = n + 1$.
Fixons un élément $a \in A$. Soit $b \in B$. Notons par $\mathcal{M}(b)$ le sous-ensemble de $\mathcal{M}$ formé de toutes les bijections $f : A \to B$ telles que $f(a) = b$.
Remarquons que pour chaque $b \in B$ l'ensemble $\mathcal{M}(b)$ est en bijection avec l'ensemble de toutes les bijections de $A' = A \setminus \{a\}$ sur $B' = B \setminus \{b\}$, donc par l'hypothèse de récurrence $\mathrm{card}\ \mathcal{M}(b) = (n-1)!$.
Ensuite l'ensemble $\mathcal{M}$ est une réunion *disjointe* des sous-ensembles $\mathcal{M}(b)$ (c'est-à-dire, les sous-ensembles $\mathcal{M}(b)$ et $\mathcal{M}(b')$ ont l'intersection vide si $b \neq b'$). Nous en avons n tels sous-ensembles, et ils ont tous la même cardinalité $(n-1)!$.
Donc au total on aura $n \times \mathrm{card}\ \mathcal{M}(b) = n!$ bijections de A sur B. $\square$

Exemple

Dressons la liste de toutes les bijections $A \longrightarrow A$ pour $A = \{1, 2, 3\}$. On va présenter chaque bijection par un tableau de 2 lignes et 3 colonnes; pour chaque élément de A on écrit au dessous de lui son image par f.
1) On considère d'abord toutes les bijections f telles que $f(1) = 1$. Il en existe deux:

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \mathrm{Id}_A$$

2) $f(1) = 2$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

3) $f(1) = 3$

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

Au total il y a $6 = 3 \times 2 = 3!$ bijections.

Définition

(*Rappel.*) Soit A un ensemble. On note par $P(A)$ ou par 2^A l'ensemble de tous les sous-ensembles de A.

Par example si $A = \{0, 1\}$, alors $P(A) = \{\varnothing, \{0, 1\}, \{0\}, \{1\}\}$.

Proposition

Si A est un ensemble fini, alors $P(A)$ est aussi un ensemble fini et $\mathrm{card}\ (P(A)) = 2^{\mathrm{card}\ A}$.

Démonstration.
Soit $B = \{0, 1\}$.

Lemme

Il y a une bijection entre B^A et $P(A)$.

Démonstration. On va construire deux applications mutuellement réciproques

$$B^A \xrightarrow{F} P(A), \qquad P(A) \xrightarrow{G} B^A$$

1) Construction de $F : B^A \longrightarrow P(A)$.

Soit $\varphi : A \longrightarrow B = \{0,1\}$ une application. Soit $M \subset A$ le sous-ensemble de tous les éléments x tels que $\varphi(x) = 1$.
On pose $M = F(\varphi)$.

2) Construction de $G : P(A) \longrightarrow B^A$.

Soit M une partie de A. On considère l'application $A \xrightarrow{\varphi} \{\,0,1\}$ suivante:

$$\varphi(x) = \begin{cases} 1 & si\ x \in M; \\ 0 & si\ x \notin M. \end{cases}$$

On pose $G(M) = \varphi$. Il est clair que $F \circ G = \mathrm{Id}_{P(A)}$ et $G \circ F = \mathrm{Id}_{B^A}$.
Donc $\mathrm{card}\ (P(A)) = \mathrm{card}\ B^A = (\mathrm{card}\ B)^{\mathrm{card}\ A} = 2^{\mathrm{card}\ A}$. □

Coefficients binomiaux

Définition

Soit $n, p \in \mathbb{N}_*$, $n \geqslant p$. Le nombre des sous-ensembles de cardinalité p d'un ensemble de cardinalité n est noté C_n^p ou $\begin{pmatrix} n \\ p \end{pmatrix}$.

Exemples

1) $C_2^0 = C_2^2 = 1,\ C_2^1 = 2.$

2) $C_n^0 = 1,\ C_n^1 = n,\ C_n^n = 1$ (quel que soit n).

3) $C_n^0 + C_n^1 + C_n^2 + ... + C_n^n = \mathrm{card}\ (P(A)) = 2^n.$

Proposition

$C_n^p = C_n^{n-p}.$

Démonstration. Soit A un ensemble de cardinalité n. Soit E_p l'ensemble de toutes les parties de A de cardinalité p.

Alors on a une bijection

$$E_p \xrightarrow{\varphi} E_{n-p}\ , \qquad \varphi(X) = A \ \setminus \ X \qquad \square$$

Proposition

Soit n, p des nombres entiers positifs, tels que $1 \leqslant p \leqslant n-1$. Alors

$$C_n^p = C_{n-1}^p + C_{n-1}^{p-1}.$$

Démonstration.
Soit A un ensemble de cardinalité n. Il nous faut compter les sous-ensembles de cardinalité p de A. Fixons un élément x de A et commençons par compter les sous-ensembles de A contenant x. On note $A \setminus \{x\}$ par A'.

Soit $B \subset A$, tel que $\mathrm{card}\ B = p$ et $x \in B$. Soit $B^{'} = B \backslash \{x\}$, alors $B^{'} \subset A'$ et

$\mathrm{card}\ B^{'} = \mathrm{card}\ B - 1 = p - 1$

Remarquons aussi que $\mathrm{card}\ A' = n - 1$.
Donc le nombre des parties de A contenant x est égal au nombre des parties de A' de cardinalité $p - 1$ ce qui est égal à C_{n-1}^{p-1}.
2) Comptons maintenant le nombre des parties de A ne contenant pas l'élément x.
Soit B un tel sous-ensemble. Alors $B \subset A'$. Donc le nombre des sous-ensembles de cardinalité p ne contenant pas a est le même que le nombre de sous-ensembles de cardinalité p de A', c'est-à-dire C_{n-1}^{p}.
3) On fait la somme: $C_n^p = C_{n-1}^{p-1} + C_{n-1}^{p}$. $\square$

Proposition

$C_n^p = \frac{n!}{p!(n-p)!}$.

Remarque

Par convention $0! = 1$.

Démonstration. Récurrence sur n.
Initialisation. $n = 1$. On a:

$$C_1^0 = \frac{1!}{0!1!} = 1, \quad C_1^1 = \frac{1!}{1!0!} = 1.$$

2) On suppose que notre proposition est démontrée au *rang* $n-1$ et on va la déduire au rang n.

On a

$$C_n^p = C_{n-1}^p + C_{n-1}^{p-1} = \frac{(n-1)!}{p!(n-1)!} + \frac{(n-1)!}{(p-1)!(n-p)!}$$

$$= \frac{(n-1)!}{(p-1)!(n-1-p)!}\left(\frac{1}{p} + \frac{1}{n-p}\right)$$

$$= \frac{(n-1)!}{(p-1)!(n-p-1)!} \times \frac{n-p+p}{p(n-p)} = \frac{n!}{(p-1)!(n-p)!}. \quad \square$$

Triangle de Pascal

Les nombres C_n^p peuvent être arrangés sous une forme d'un tableau triangulaire infini:

$$
\begin{array}{ccccccc}
 & & & C_0^0 & & & \\
 & & C_1^0 & & C_1^1 & & \\
 & C_2^0 & & C_2^1 & & C_2^2 & \\
C_3^0 & & C_3^1 & & C_3^2 & & C_3^3
\end{array}
$$

....

Dans ce tableau chaque nombre est égal à la somme des deux nombres au-dessous à la gauche et à la droite (par example $C_2^1 = C_1^0 + C_1^1$).

Le triangle de Pascal est un moyen efficace pour calculer les nombres C_n^p, surtout pour les petites valeurs de n, p.

Exercice

Calculer C_5^p, C_6^p pouir tout p à l'aide du triangle de Pascal.

Proposition

Soit $p < r \leqslant \frac{n}{2}$. Alors $C_n^p < C_n^r$.

Démonstration. On a:

$$C_n^p = \frac{n!}{p!(n-p)!}, \qquad C_n^{p+1} = \frac{n!}{(p+1)!(n-p-1)!},$$

donc $C_n^{p+1} = \frac{n-p}{p+1} \cdot C_n^p$.

Or $p < p+1 \leqslant \frac{n}{2}$ donc $2p+2 \leqslant n$. On en déduit que $n - p \geqslant p + 2 > p + 1$, et que $\frac{n-p}{p+1} > 1$.

Donc $C_n^p < C_n^{p+1}$ et $C_n^p < C_n^{p+1} < C_n^{p+2}$.... $\square$

Binôme de Newton

Proposition

Soit n un nombre naturel, et x, y des nombres entiers, rationnels, réels ou complexes. Alors

$$(x+y)^n = \sum_{i=0}^{n} C_n^i x^i y^{n-i}$$

c'est-à-dire

$$(x+y)^n = C_n^0 y^n + C_n^1 xy^{n-1} + \ldots + C_n^{n-1} x^{n-1} y + C_n^n x^n$$

$$= y^n + nxy^{n-1} + \ldots + nx^{n-1}y + x^n.$$

Démonstration.
Récurrence sur n.

Initialisation.
Pour $n = 1$ on a $(x+y)^1 = x + y = C_1^0 x^0 y^1 + C_1^1 xy^0$.

Hérédité: Supposons la propriété vraie au *rang* n et procédons au rang $n+1$.

$$(x+y)^{n+1} = (x+y)(x+y)^n = (x+y)\left(\sum_{i=0}^{n} C_n^i x^i y^{n-i}\right) =$$

$$= x\sum_{i=0}^{n} C_n^i x^i y^{n-i} + y\sum_{i=0}^{n} C_n^i x^i y^{n-i} = \sum_{i=0}^{n} C_n^i x^{i+1} y^{n-i} + \sum_{i=0}^{n} C_n^i x^i y^{n-i+1} =$$

(en posant $j = i+1$ dans la première somme)

$$= \sum_{j=1}^{n+1} C_n^{j-1} x^j y^{n-(j-1)} + \sum_{i=0}^{n} C_n^i x^i y^{n-i+1} =$$

(en remplaçant l'indice de sommation j par i et en mettant apart le dernier terme de la première somme)

$$= C_n^n x^{n+1} + \sum_{i=1}^{n} C_n^{i-1} x^j y^{n-i+1} + \sum_{i=1}^{n} C_n^i x^i y^{n-i+1} + C_n^0 y^{n+1}$$

$$= x^{n+1} + \sum_{i=1}^{n} x^i y^{n-i+1}(C_n^{i-1} + C_n^i) + y^{n+1} =$$

$$= \sum_{i=1}^{n} C_{n+1}^i x^i y^{n-i+1} + x^{n+1} + y^{n+1}.$$

(puisque $C_n^{i-1} + C_n^i = C_{n+1}^i$). La formule est démontrée. $\square$