Exo7

Ensembles et applications

Vidéo ■ partie 1. Ensembles
Vidéo ■ partie 2. Applications
Vidéo ■ partie 3. Injection, surjection, bijection
Vidéo ■ partie 4. Ensembles finis
Vidéo ■ partie 5. Relation d'équivalence
Exercices ♦ Logique, ensembles, raisonnements
Exercices ♦ Injection, surjection, bijection
Exercices ♦ Dénombrement
Exercices ♦ Relation d'équivalence, relation d'ordre

Motivations

Au début du XX^{e} siècle le professeur Frege peaufinait la rédaction du second tome d'un ouvrage qui souhaitait refonder les mathématiques sur des bases logiques. Il reçut une lettre d'un tout jeune mathématicien : « *J'ai bien lu votre premier livre. Malheureusement vous supposez qu'il existe un ensemble qui contient tous les ensembles. Un tel ensemble ne peut exister.* » S'ensuit une démonstration de deux lignes. Tout le travail de Frege s'écroulait et il ne s'en remettra jamais. Le jeune Russell deviendra l'un des plus grands logiciens et philosophes de sont temps. Il obtient le prix Nobel de littérature en 1950.
Voici le « paradoxe de Russell » pour montrer que l'ensemble de tous les ensembles ne peut exister. C'est très bref, mais difficile à appréhender. Par l'absurde, supposons qu'un tel ensemble $\mathscr{E}$ contenant tous les ensembles existe. Considérons

$$F = \Big\{E \in \mathscr{E} \mid E \notin E\Big\}.$$

Expliquons l'écriture $E \notin E$: le E de gauche est considéré comme un élément, en effet l'ensemble $\mathscr{E}$ est l'ensemble de tous les ensembles et E est un élément de cet ensemble ; le E de droite est considéré comme un ensemble, en effet les élément de $\mathscr{E}$ sont des ensembles ! On peut donc s'interroger si l'élément E appartient à l'ensemble E. Si non, alors par définition on met E dans l'ensemble F.
La contradiction arrive lorsque l'on se pose la question suivante : a-t-on $F \in F$ ou $F \notin F$? L'une des deux affirmation doit être vraie. Et pourtant :

- Si $F \in F$ alors par définition de F, F est l'un des ensembles E tel que $F \notin F$. Ce qui est contradictoire.
- Si $F \notin F$ alors F vérifie bien la propriété définissant F donc $F \in F$! Encore contradictoire.

Aucun des cas n'est possible. On en déduit qu'il ne peut exister un tel ensemble $\mathscr{E}$ contenant tous les ensembles.
Ce paradoxe a été popularisé par l'énigme suivante : « *Dans une ville, le barbier rase tous ceux qui ne se rasent pas eux-mêmes. Qui rase le barbier ?* » La seule réponse valable est qu'une telle situation ne peut exister.

Ne vous inquiétez pas, Russell et d'autres ont fondé la logique et les ensembles sur des bases solides. Cependant il n'est pas possible dans ce cours de tout redéfinir. Heureusement, vous connaissez déjà quelques ensembles :

- l'ensemble des entiers naturels $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$.
- l'ensemble des entiers relatifs $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$.
- l'ensemble des rationnels $\mathbb{Q} = \left\{\frac{p}{q} \mid p \in \mathbb{Z}, q \in \mathbb{N} \setminus \{0\}\right\}$.
- l'ensemble des réels $\mathbb{R}$, par exemple $1, \sqrt{2}, \pi, \ln(2), \ldots$
- l'ensemble des nombres complexes $\mathbb{C}$.

Nous allons essayer de voir les propriétés des ensembles, sans s'attacher à un exemple particulier. Vous vous apercevrez assez rapidement que ce qui est au moins aussi important que les ensembles, ce sont les relations entre ensembles : ce sera la notion d'application (ou fonction) entre deux ensembles.

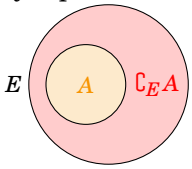
1. Ensembles

1.1. Définir des ensembles

- On va définir informellement ce qu'est un ensemble : un ***ensemble*** est une collection d'éléments.
- Exemples :
$$\{0, 1\}, \quad \{\text{rouge}, \text{noir}\}, \quad \{0, 1, 2, 3, \ldots\} = \mathbb{N}.$$
- Un ensemble particulier est l'***ensemble vide***, noté $\varnothing$ qui est l'ensemble ne contenant aucun élément.
- On note
$$\boxed{x \in E}$$
si x est un élément de E, et $x \notin E$ dans le cas contraire.
- Voici une autre façon de définir des ensembles : une collection d'éléments qui vérifient une propriété.
- Exemples :
$$\{x \in \mathbb{R} \mid |x - 2| < 1\}, \quad \{z \in \mathbb{C} \mid z^5 = 1\}, \quad \{x \in \mathbb{R} \mid 0 \leqslant x \leqslant 1\} = [0, 1].$$

1.2. Inclusion, union, intersection, complémentaire

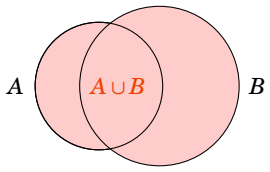
- L'***inclusion***. $E \subset F$ si tout élément de E est aussi un élément de F (autrement dit : $\forall x \in E\ (x \in F)$). On dit alors que E est un ***sous-ensemble*** de F ou une ***partie*** de F.
- L'***égalité***. $E = F$ si et seulement si $E \subset F$ et $F \subset E$.
- ***Ensemble des parties*** de E. On note $\mathscr{P}(E)$ l'ensemble des parties de E. Par exemple si $E = \{1, 2, 3\}$:
$$\mathscr{P}(\{1, 2, 3\}) = \{\varnothing, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}.$$
- ***Complémentaire***. Si $A \subset E$,
$$\boxed{\complement_E A = \{x \in E \mid x \notin A\}}$$
On le note aussi $E \setminus A$ et juste $\complement A$ s'il n'y a pas d'ambiguïté (et parfois aussi A^c ou $\overline{A}$).



– ***Union***. Pour $A, B \subset E$,

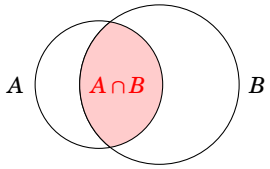
$$A \cup B = \{x \in E \mid x \in A \text{ ou } x \in B\}$$

Le *«ou»* n'est pas exclusif : x peut appartenir à A et à B en même temps.



– ***Intersection***.

$$A \cap B = \{x \in E \mid x \in A \text{ et } x \in B\}$$



1.3. Règles de calculs

Soient A, B, C des parties d'un ensemble E.

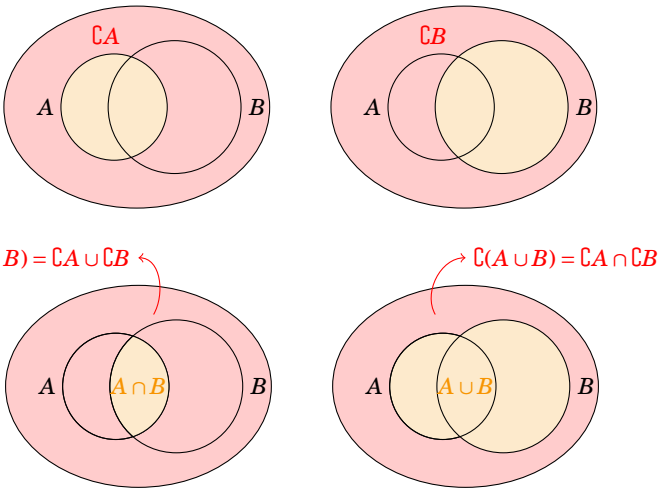
– $A \cap B = B \cap A$
– $A \cap (B \cap C) = (A \cap B) \cap C$ (on peut donc écrire $A \cap B \cap C$ sans ambigüité)
– $A \cap \varnothing = \varnothing$, $A \cap A = A$, $A \subset B \iff A \cap B = A$

– $A \cup B = B \cup A$
– $A \cup (B \cup C) = (A \cup B) \cup C$ (on peut donc écrire $A \cup B \cup C$ sans ambiguïté)
– $A \cup \varnothing = A$, $A \cup A = A$, $A \subset B \iff A \cup B = B$

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

– $\complement(\complement A) = A$ et donc $A \subset B \iff \complement B \subset \complement A$.
– $\complement(A \cap B) = \complement A \cup \complement B$
– $\complement(A \cup B) = \complement A \cap \complement B$

Voici les dessins pour les deux dernières assertions.



Les preuves sont pour l'essentiel une reformulation des opérateurs logiques, en voici quelques-unes :

- Preuve de $A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$: $x\in A\cap(B\cup C)\iff x\in A$ et $x\in(B\cup C)\iff x\in A$ et ($x\in B$ ou $x\in C$) $\iff$ ($x\in A$ et $x\in B$) ou ($x\in A$ et $x\in C$) $\iff$ ($x\in A\cap B$) ou ($x\in A\cap C$) $\iff x\in(A\cap B)\cup(A\cap C)$.
- Preuve de $\complement(A\cap B)=\complement A\cup\complement B$: $x\in\complement(A\cap B)\iff x\notin(A\cap B)\iff \text{non}\big(x\in A\cap B\big)\iff \text{non}\big(x\in A$ et $x\in B\big)\iff \text{non}(x\in A)$ ou $\text{non}(x\in B)\iff x\notin A$ ou $x\notin B\iff x\in\complement A\cup\complement B$.

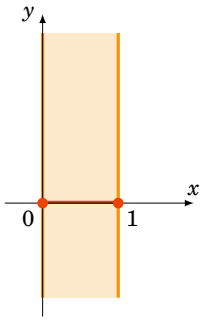
Remarquez que l'on repasse aux éléments pour les preuves.

1.4. Produit cartésien

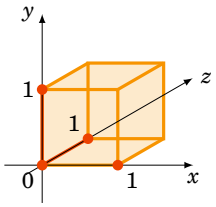
Soient E et F deux ensembles. Le ***produit cartésien***, noté $E\times F$, est l'ensemble des couples (x,y) où $x\in E$ et $y\in F$.

Exemple 1

1. Vous connaissez $\mathbb{R}^2=\mathbb{R}\times\mathbb{R}=\big\{(x,y)\mid x,y\in\mathbb{R}\big\}$.
2. Autre exemple $[0,1]\times\mathbb{R}=\big\{(x,y)\mid 0\leqslant x\leqslant 1, y\in\mathbb{R}\big\}$



3. $[0,1]\times[0,1]\times[0,1]=\big\{(x,y,z)\mid 0\leqslant x,y,z\leqslant 1\big\}$



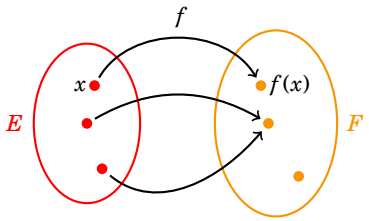
Mini-exercices

1. En utilisant les définitions, montrer : $A\neq B$ si et seulement s'il existe $a\in A\setminus B$ ou $b\in B\setminus A$.
2. Énumérer $\mathscr{P}(\{1,2,3,4\})$.
3. Montrer $A\cup(B\cap C)=(A\cup B)\cap(A\cup C)$ et $\complement(A\cup B)=\complement A\cap\complement B$.
4. Énumérer $\{1,2,3\}\times\{1,2,3,4\}$.
5. Représenter les sous-ensembles de $\mathbb{R}^2$ suivants : $\big(]0,1[\cup[2,3[\big)\times[-1,1]$, $\big(\mathbb{R}\setminus]0,1[\cup[2,3[\big)\times\big((\mathbb{R}\setminus[-1,1])\cap[0,2]\big)$.

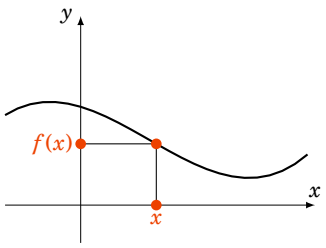
2. Applications

2.1. Définitions

– Une ***application*** (ou une ***fonction***) $f : E \to F$, c'est la donnée pour chaque élément $x \in E$ d'un unique élément de F noté $f(x)$.
Nous représenterons les applications par deux types d'illustrations : les ensembles «patates», l'ensemble de départ (et celui d'arrivée) est schématisé par un ovale ses éléments par des points. L'association $x \mapsto f(x)$ est représentée par une flèche.

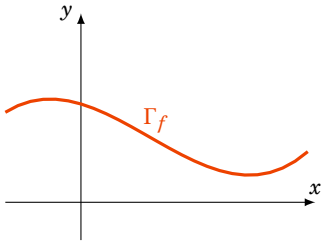


L'autre représentation est celle des fonctions continues de $\mathbb{R}$ dans $\mathbb{R}$ (ou des sous-ensembles de $\mathbb{R}$). L'ensemble de départ $\mathbb{R}$ est représenté par l'axe des abscisses et celui d'arrivée par l'axe des ordonnées. L'association $x \mapsto f(x)$ est représentée par le point $(x, f(x))$.

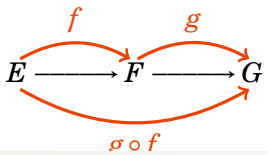


– ***Égalité***. Deux applications $f, g : E \to F$ sont égales si et seulement si pour tout $x \in E$, $f(x) = g(x)$. On note alors $f = g$.
– Le ***graphe*** de $f : E \to F$ est

$$\boxed{\Gamma_f = \left\{ \big(x, f(x)\big) \in E \times F \mid x \in E \right\}}$$



– ***Composition***. Soient $f : E \to F$ et $g : F \to G$ alors $g \circ f : E \to G$ est l'application définie par $g \circ f(x) = g\big(f(x)\big)$.



Exemple 2

1. L'***identité***, $\mathrm{id}_E : E \to E$ est simplement définie par $x \mapsto x$ et sera très utile dans la suite.
2. Définissons f, g ainsi

$$f : \begin{array}{ccc}]0,+\infty[& \longrightarrow &]0,+\infty[\\ x & \longmapsto & \frac{1}{x} \end{array}, \qquad g : \begin{array}{ccc}]0,+\infty[& \longrightarrow & \mathbb{R} \\ x & \longmapsto & \frac{x-1}{x+1} \end{array}.$$

Alors $g \circ f :]0,+\infty[\to \mathbb{R}$ vérifie pour tout $x \in]0,+\infty[$:

$$g \circ f(x) = g\big(f(x)\big) = g\left(\frac{1}{x}\right) = \frac{\frac{1}{x}-1}{\frac{1}{x}+1} = \frac{1-x}{1+x} = -g(x).$$

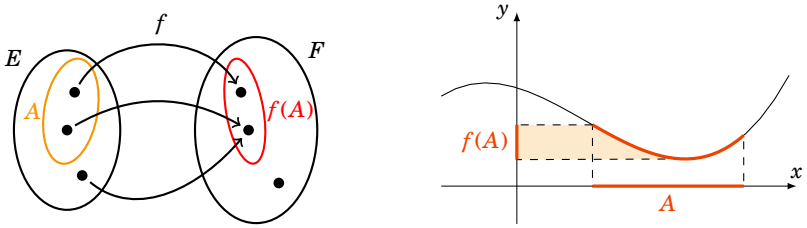
2.2. Image directe, image réciproque

Soient E, F deux ensembles.

Définition 1

Soit $A \subset E$ et $f : E \to F$, l'***image directe*** de A par f est l'ensemble

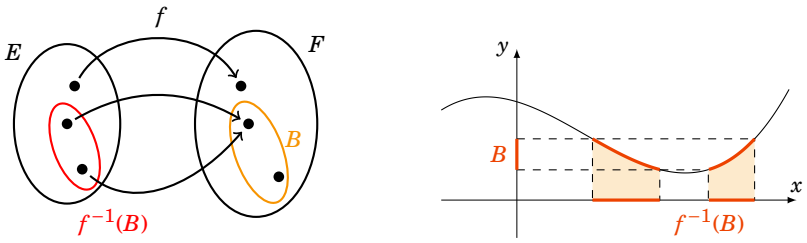
$$f(A) = \{f(x) \mid x \in A\}$$



Définition 2

Soit $B \subset F$ et $f : E \to F$, l'***image réciproque*** de B par f est l'ensemble

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



Remarque

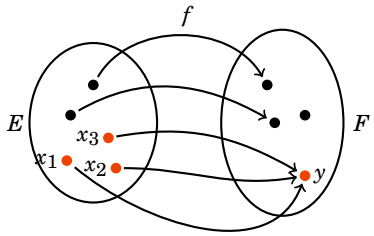
Ces notions sont plus difficiles à maîtriser qu'il n'y paraît !

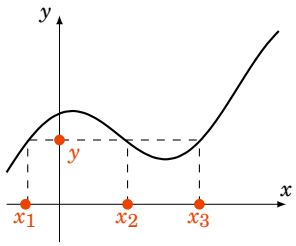
- $f(A)$ est un sous-ensemble de F, $f^{-1}(B)$ est un sous-ensemble de E.
- La notation «$f^{-1}(B)$» est un tout, rien ne dit que f est un fonction bijective (voir plus loin). L'image réciproque existe quelque soit la fonction.
- L'image directe d'un singleton $f(\{x\}) = \{f(x)\}$ est un singleton. Par contre l'image réciproque d'un singleton $f^{-1}(\{y\})$ dépend de f. Cela peut être un singleton, un ensemble à plusieurs éléments ; mais cela peut-être E tout entier (si f est une fonction constante) ou même l'ensemble vide (si aucune image par f ne vaut y).

2.3. Antécédents

Fixons $y \in F$. Tout élément $x \in E$ tel que $f(x) = y$ est un ***antécédent*** de y.
En termes d'image réciproque l'ensemble des antécédents de y est $f^{-1}(\{y\})$.

Sur les dessins suivants, l'élément y admet 3 antécédents par f. Ce sont x_1, x_2, x_3.





Mini-exercices

1. Pour deux applications $f, g : E \to F$, quelle est la négation de $f = g$?
2. Représenter le graphe de $f : \mathbb{N} \to \mathbb{R}$ définie par $n \mapsto \frac{4}{n+1}$.
3. Soient $f, g, h : \mathbb{R} \to \mathbb{R}$ définies par $f(x) = x^2$, $g(x) = 2x+1$, $h(x) = x^3 - 1$. Calculer $f \circ (g \circ h)$ et $(f \circ g) \circ h$.
4. Pour la fonction $f : \mathbb{R} \to \mathbb{R}$ définie par $x \mapsto x^2$ représenter et calculer les ensembles suivants : $f([0,1[)$, $f(\mathbb{R})$, $f(]-1,2[)$, $f^{-1}([1,2[)$, $f^{-1}([-1,1])$, $f^{-1}(\{3\})$, $f^{-1}(\mathbb{R} \setminus \mathbb{N})$.

3. Injection, surjection, bijection

3.1. Injection, surjection

Soit E, F deux ensembles et $f : E \to F$ une application.

Définition 3

f est ***injective*** si pour tout $x, x' \in E$ avec $f(x) = f(x')$ alors $x = x'$. Autrement dit :

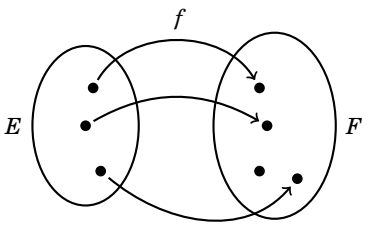
$$\forall x, x' \in E \quad \big(f(x) = f(x') \implies x = x'\big)$$

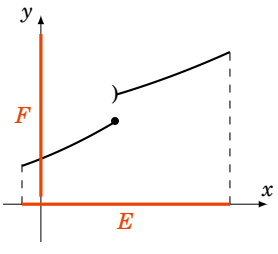
Définition 4

f est ***surjective*** si pour tout $y \in F$, il existe $x \in E$ tel que $y = f(x)$. Autrement dit :

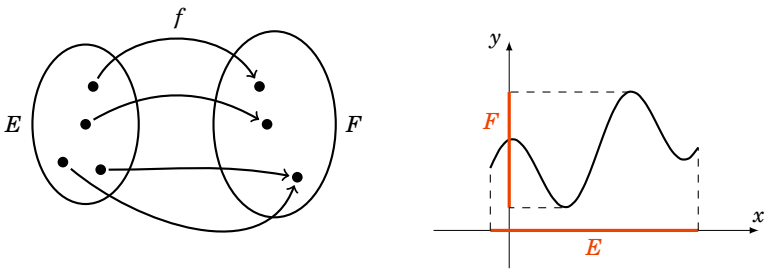
$$\forall y \in F \quad \exists x \in E \quad \big(y = f(x)\big)$$

Une autre formulation : f est surjective si et seulement si $f(E) = F$.
Les applications f représentées sont injectives :





Les applications f représentées sont surjectives :



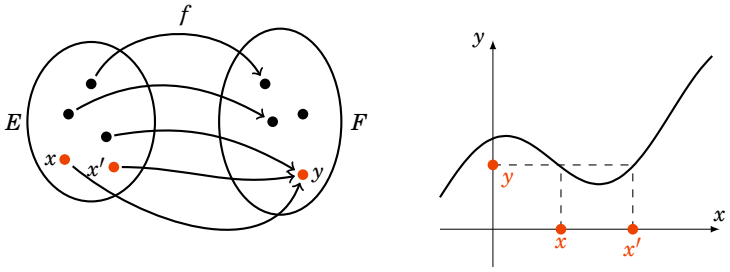
Remarque

Encore une fois ce sont des notions difficiles à appréhender. Une autre façon de formuler l'injectivité et la surjectivité est d'utiliser les antécédents.

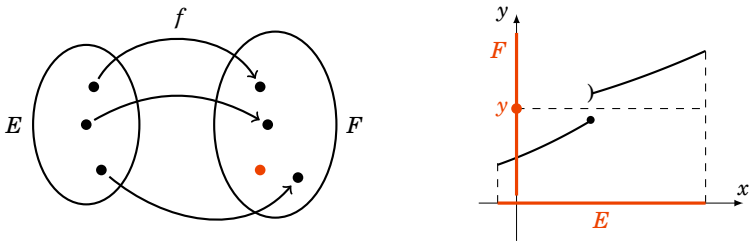
- f est injective si et seulement si tout élément y de F a *au plus* 1 antécédent (et éventuellement aucun).
- f est surjective si et seulement si tout élément y de F a *au moins* 1 antécédent.

Remarque

Voici deux fonctions non injectives :



Ainsi que deux fonctions non surjectives :



Exemple 3

1. Soit $f_1 : \mathbb{N} \to \mathbb{Q}$ définie par $f_1(x) = \frac{1}{1+x}$. Montrons que f_1 est injective : soit $x, x' \in \mathbb{N}$ tels que $f_1(x) = f_1(x')$. Alors $\frac{1}{1+x} = \frac{1}{1+x'}$, donc $1+x = 1+x'$ et donc $x = x'$. Ainsi f_1 est injective. Par contre f_1 n'est pas surjective. Il s'agit de trouver un élément y qui n'a pas d'antécédent par f_1. Ici il est facile de voir que l'on a toujours $f_1(x) \leqslant 1$ et donc par exemple $y = 2$ n'a pas d'antécédent. Ainsi f_1 n'est pas surjective.
2. Soit $f_2 : \mathbb{Z} \to \mathbb{N}$ définie par $f_2(x) = x^2$. Alors f_2 n'est pas injective. En effet on peut trouver deux éléments $x, x' \in \mathbb{Z}$ différents tels que $f_2(x) = f_2(x')$. Il suffit de prendre par exemple $x = 2$, $x' = -2$.

   f_2 n'est pas non plus surjective, en effet il existe des éléments $y \in \mathbb{N}$ qui n'ont aucun

antécédent. Par exemple $y = 3$: si $y = 3$ avait un antécédent x par f_2, nous aurions $f_2(x) = y$, c'est-à-dire $x^2 = 3$, d'où $x = \pm\sqrt{3}$. Mais alors x n'est pas un entier de $\mathbb{Z}$. Donc $y = 3$ n'a pas d'antécédent et f_2 n'est pas surjective.

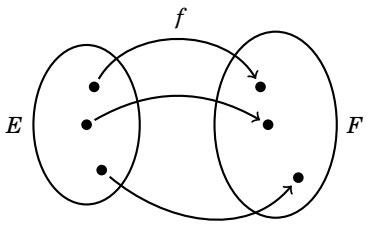
3.2. Bijection

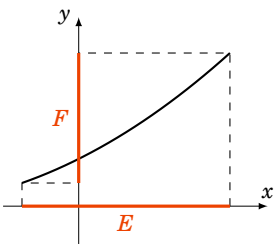
Définition 5

f est ***bijective*** si elle injective et surjective. Cela équivaut à : pour tout $y \in F$ il existe un unique $x \in E$ tel que $y = f(x)$. Autrement dit :

$$\forall y \in F \quad \exists! x \in E \quad \big(y = f(x)\big)$$

L'existence du x vient de la surjectivité et l'unicité de l'injectivité. Autrement dit, tout élément de F a un unique antécédent par f.





Proposition 1

Soit E, F des ensembles et $f : E \to F$ une application.

1. L'application f est bijective si et seulement si il existe une application $g : F \to E$ telle que $f \circ g = \mathrm{id}_F$ et $g \circ f = \mathrm{id}_E$.
2. Si f est bijective alors l'application g est unique et elle aussi est bijective. L'application g s'appelle la ***bijection réciproque*** de f et est notée f^{-1}. De plus $\big(f^{-1}\big)^{-1} = f$.

Remarque

- $f \circ g = \mathrm{id}_F$ se reformule ainsi

$$\forall y \in F \quad f\big(g(y)\big) = y.$$

- Alors que $g \circ f = \mathrm{id}_E$ s'écrit :

$$\forall x \in E \quad g\big(f(x)\big) = x.$$

- Par exemple $f : \mathbb{R} \to]0, +\infty[$ définie par $f(x) = \exp(x)$ est bijective, sa bijection réciproque est $g :]0, +\infty[\to \mathbb{R}$ définie par $g(y) = \ln(y)$. Nous avons bien $\exp\big(\ln(y)\big) = y$, pour tout $y \in]0, +\infty[$ et $\ln\big(\exp(x)\big) = x$, pour tout $x \in \mathbb{R}$.

Démonstration

1. – Sens $\Rightarrow$. Supposons f bijective. Nous allons construire une application $g : F \to E$. Comme f est surjective alors pour chaque $y \in F$, il existe un $x \in E$ tel que $y = f(x)$ et on pose $g(y) = x$. On a $f\big(g(y)\big) = f(x) = y$, ceci pour tout $y \in F$ et donc $f \circ g = \mathrm{id}_F$. On compose à droite avec f donc $f \circ g \circ f = \mathrm{id}_F \circ f$. Alors pour tout $x \in E$ on a $f\big(g \circ f(x)\big) = f(x)$ or f est injective et donc $g \circ f(x) = x$. Ainsi $g \circ f = \mathrm{id}_E$. Bilan : $f \circ g = \mathrm{id}_F$ et $g \circ f = \mathrm{id}_E$.
   – Sens $\Leftarrow$. Supposons que g existe et montrons que f est bijective.
     – f est surjective : en effet soit $y \in F$ alors on note $x = g(y) \in E$; on a bien : $f(x) = f\big(g(y)\big) = f \circ g(y) = \mathrm{id}_F(y) = y$, donc f est bien surjective.
     – f est injective : soient $x, x' \in E$ tels que $f(x) = f(x')$. On compose par g (à gauche) alors $g \circ f(x) = g \circ f(x')$ donc $\mathrm{id}_E(x) = \mathrm{id}_E(x')$ donc $x = x'$; f est bien injective.
2. – Si f est bijective alors g est aussi bijective car $g \circ f = \mathrm{id}_E$ et $f \circ g = \mathrm{id}_F$ et on applique ce que l'on vient de démontrer avec g à la place de f. Ainsi $g^{-1} = f$.
   – Si f est bijective, g est unique : en effet soit $h : F \to E$ une autre application telle que $h \circ f = \mathrm{id}_E$ et $f \circ h = \mathrm{id}_F$; en particulier $f \circ h = \mathrm{id}_F = f \circ g$, donc pour tout $y \in F$, $f\big(h(y)\big) = f\big(g(y)\big)$ or f est injective alors $h(y) = g(y)$, ceci pour tout $y \in F$; d'où $h = g$.

Proposition 2

Soient $f : E \to F$ et $g : F \to G$ des applications bijectives. L'application $g \circ f$ est bijective et sa bijection réciproque est

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}$$

Démonstration

D'après la proposition 1, il existe $u : F \to E$ tel que $u \circ f = \mathrm{id}_E$ et $f \circ u = \mathrm{id}_F$. Il existe aussi $v : G \to F$ tel que $v \circ g = \mathrm{id}_F$ et $g \circ v = \mathrm{id}_G$. On a alors $(g \circ f) \circ (u \circ v) = g \circ (f \circ u) \circ v = g \circ \mathrm{id}_F \circ u = g \circ u = \mathrm{id}_E$. Et $(u \circ v) \circ (g \circ f) = u \circ (v \circ g) \circ f = u \circ \mathrm{id}_F \circ f = u \circ f = \mathrm{id}_E$. Donc $g \circ f$ est bijective et son inverse est $u \circ v$. Comme u est la bijection réciproque de f et v celle de g alors : $u \circ v = f^{-1} \circ g^{-1}$.

Mini-exercices

1. Les fonctions suivantes sont-elles injectives, surjectives, bijectives ?
   – $f_1 : \mathbb{R} \to [0, +\infty[$, $x \mapsto x^2$.
   – $f_2 : [0, +\infty[\to [0, +\infty[$, $x \mapsto x^2$.
   – $f_3 : \mathbb{N} \to \mathbb{N}$, $x \mapsto x^2$.
   – $f_4 : \mathbb{Z} \to \mathbb{Z}$, $x \mapsto x - 7$.
   – $f_5 : \mathbb{R} \to [0, +\infty[$, $x \mapsto |x|$.
2. Montrer que la fonction $f :]1, +\infty[\to]0, +\infty[$ définie par $f(x) = \frac{1}{x-1}$ est bijective. Calculer sa bijection réciproque.

4. Ensembles finis

4.1. Cardinal

Définition 6

Un ensemble E est ***fini*** s'il existe un entier $n \in \mathbb{N}$ et une bijection de E vers $\{1,2,\dots,n\}$. Cet entier n est unique et s'appelle le ***cardinal*** de E (ou le ***nombre d'éléments***) et est noté $\operatorname{Card} E$.

Quelques exemples :

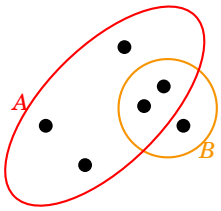
1. $E = \{\text{rouge}, \text{noir}\}$ est en bijection avec $\{1,2\}$ et donc est de cardinal 2.
2. $\mathbb{N}$ n'est pas un ensemble fini.
3. Par définition le cardinal de l'ensemble vide est 0.

Enfin quelques propriétés :

1. Si A est un ensemble fini et $B \subset A$ alors B est un ensemble fini et $\operatorname{Card} B \leqslant \operatorname{Card} A$.
2. Si A, B sont des ensembles finis disjoints (c'est-à-dire $A \cap B = \varnothing$) alors $\operatorname{Card}(A \cup B) = \operatorname{Card} A + \operatorname{Card} B$.
3. Si A est un ensemble fini et $B \subset A$ alors $\operatorname{Card}(A \setminus B) = \operatorname{Card} A - \operatorname{Card} B$.
4. Enfin pour A, B deux ensembles finis quelconques :

$$\boxed{\operatorname{Card}(A \cup B) = \operatorname{Card} A + \operatorname{Card} B - \operatorname{Card}(A \cap B)}$$

Voici une situation où s'applique la dernière propriété :



4.2. Injection, surjection, bijection et ensembles finis

Proposition 3

Soit E, F deux ensembles finis et $f : E \to F$ une application.

1. Si f est injective alors $\operatorname{Card} E \leqslant \operatorname{Card} F$.
2. Si f est surjective alors $\operatorname{Card} E \geqslant \operatorname{Card} F$.
3. Si f est bijective alors $\operatorname{Card} E = \operatorname{Card} F$.

Démonstration

1. Supposons f injective. Notons $F' = f(E) \subset F$ alors la restriction $f_| : E \to F'$ (définie par $f_|(x) = f(x)$) est une bijection. Donc pour chaque $y \in F'$ est associé un unique $x \in E$ tel que $y = f(x)$. Donc E et F' ont le même nombre d'éléments. Donc $\operatorname{Card} F' = \operatorname{Card} E$. Or $F' \subset F$, ainsi $\operatorname{Card} E = \operatorname{Card} F' \leqslant \operatorname{Card} F$.
2. Supposons f surjective. Pour tout élément $y \in F$, il existe au moins un élément x de E tel que $y = f(x)$ et donc $\operatorname{Card} E \geqslant \operatorname{Card} F$.
3. Cela découle de (1) et (2) (ou aussi de la preuve du (1)).

Proposition 4

Soit E, F deux ensembles finis et $f : E \to F$ une application. Si

$$\mathrm{Card}\, E = \mathrm{Card}\, F$$

alors les assertions suivantes sont équivalentes :

i. f est injective,

ii. f est surjective,

iii. f est bijective.

Démonstration

Le schéma de la preuve est le suivant : nous allons montrer successivement les implications :

$$(i) \Longrightarrow (ii) \Longrightarrow (iii) \Longrightarrow (i)$$

ce qui prouvera bien toutes les équivalences.

- $(i) \Longrightarrow (ii)$. Supposons f injective. Alors $\mathrm{Card}\, f(E) = \mathrm{Card}\, E = \mathrm{Card}\, F$. Ainsi $f(E)$ est un sous-ensemble de F ayant le même cardinal que F ; cela entraîne $f(E) = F$ et donc f est surjective.
- $(ii) \Longrightarrow (iii)$. Supposons f surjective. Pour montrer que f est bijective, il reste à montrer que f est injective. Raisonnons par l'absurde et supposons f non injective. Alors $\mathrm{Card}\, f(E) < \mathrm{Card}\, E$ (car au moins 2 éléments ont la même image). Or $f(E) = F$ car f surjective, donc $\mathrm{Card}\, F < \mathrm{Card}\, E$. C'est une contradiction, donc f doit être injective et ainsi f est bijective.
- $(iii) \Longrightarrow (i)$. C'est clair : une fonction bijective est en particulier injective.

Appliquez ceci pour montrer le ***principe des tiroirs*** :

Proposition 5

Si l'on range dans k tiroirs, $n > k$ paires de chaussettes alors il existe (au moins) un tiroir contenant (au moins) deux paires de chaussettes.

Malgré sa formulation amusante, c'est une proposition souvent utile. Exemple : dans un amphi de 400 étudiants, il y a au moins deux étudiants nés le même jour !

4.3. Nombres d'applications

Soient E, F des ensembles finis, non vides. On note $\mathrm{Card}\, E = n$ et $\mathrm{Card}\, F = p$.

Proposition 6

Le nombre d'applications différentes de E dans F est :

$$\boxed{p^n}$$

Autrement dit c'est $\boxed{(\mathrm{Card}\, F)^{\mathrm{Card}\, E}}$.

Exemple 4

En particulier le nombre d'applications de E dans lui-même est n^n. Par exemple si $E = \{1,2,3,4,5\}$ alors ce nombre est $5^5 = 3125$.

Démonstration

Fixons F et $p = \mathrm{Card}\, F$. Nous allons effectuer une récurrence sur $n = \mathrm{Card}\, E$. Soit (P_n) l'assertion suivante : le nombre d'applications d'un ensemble à n éléments vers un ensemble à p éléments est p^n.

- *Initialisation.* Pour $n = 1$, une application de E dans F est définie par l'image de l'unique élément de E. Il y a $p = \mathrm{Card}\, F$ choix possibles et donc p^1 applications distinctes. Ainsi P_1 est vraie.
- *Hérédité.* Fixons $n \geqslant 1$ et supposons que P_n est vraie. Soit E un ensemble à $n+1$ éléments. On choisit et fixe $a \in E$; soit alors $E' = E \setminus \{a\}$ qui a bien n éléments. Le nombre d'applications de E' vers F est p^n, par l'hypothèse de récurrence (P_n). Pour chaque application $f : E' \to F$ on peut la prolonger en une application $f : E \to F$ en choisissant l'image de a. On a p choix pour l'image de a et donc $p^n \times p$ choix pour les applications de E vers F. Ainsi P_{n+1} est vérifiée.
- *Conclusion.* Par le principe de récurrence P_n est vraie, pour tout $n \geqslant 1$.

Proposition 7

Le nombre d'injections de E dans F est :

$$p \times (p-1) \times \cdots \times (p-(n-1)).$$

Démonstration

Supposons $E = \{a_1, a_2, \ldots, a_n\}$; pour l'image de a_1 nous avons p choix. Une fois ce choix fait, pour l'image de a_2 il reste $p-1$ choix (car a_2 ne doit pas avoir la même image que a_1). Pour l'image de a_3 il y a $p-2$ possibilités. Ainsi de suite : pour l'image de a_k il y $p-(k-1)$ choix... Il y a au final $p \times (p-1) \times \cdots \times (p-(n-1))$ applications injectives.

Notation ***factorielle*** : $n! = 1 \times 2 \times 3 \times \cdots \times n$. Avec $1! = 1$ et par convention $0! = 1$.

Proposition 8

Le nombre de bijections d'un ensemble E de cardinal n dans lui-même est :

$$\boxed{n!}$$

Exemple 5

Parmi les 3125 applications de $\{1,2,3,4,5\}$ dans lui-même il y en a $5! = 120$ qui sont bijectives.

Démonstration

Nous allons le prouver par récurrence sur n. Soit (P_n) l'assertion suivante : le nombre de bijections d'un ensemble à n éléments dans un ensemble à n éléments est $n!$

- P_1 est vraie. Il n'y a qu'une bijection d'un ensemble à 1 élément dans un ensemble à 1 élément.
- Fixons $n \geqslant 1$ et supposons que P_n est vraie. Soit E un ensemble à $n+1$ éléments. On fixe $a \in E$. Pour chaque $b \in E$ il y a -par l'hypothèse de récurrence- exactement $n!$ applications bijectives de $E \setminus \{a\} \to E \setminus \{b\}$. Chaque application se prolonge en une bijection de $E \to F$ en

posant $a \mapsto b$. Comme il y a $n+1$ choix de $b \in E$ alors nous obtenons $n! \times (n+1)$ bijections de E dans lui-même. Ainsi P_{n+1} est vraie.

– Par le principe de récurrence le nombre de bijections d'un ensemble à n éléments est $n!$

On aurait aussi pu directement utiliser la proposition 7 avec $n = p$ (sachant qu'alors les injections sont aussi des bijections).

4.4. Nombres de sous-ensembles

Soit E un ensemble fini de cardinal n.

Proposition 9

Il y a $2^{\mathrm{Card}\, E}$ sous-ensembles de E :

$$\boxed{\mathrm{Card}\, \mathscr{P}(E) = 2^n}$$

Exemple 6

Si $E = \{1,2,3,4,5\}$ alors $\mathscr{P}(E)$ a $2^5 = 32$ parties. C'est un bon exercice de les énumérer :

– l'ensemble vide : $\varnothing$,
– 5 singletons : $\{1\}, \{2\}, \ldots$,
– 10 paires : $\{1,2\}, \{1,3\}, \ldots, \{2,3\}, \ldots$,
– 10 triplets : $\{1,2,3\}, \ldots$,
– 5 ensembles à 4 éléments : $\{1,2,3,4\}, \{1,2,3,5\}, \ldots$,
– et E tout entier : $\{1,2,3,4,5\}$.

Démonstration

Encore une récurrence sur $n = \mathrm{Card}\, E$.

– Si $n = 1$, $E = \{a\}$ est un singleton, les deux sous-ensembles sont : $\varnothing$ et E.
– Supposons que la proposition soit vraie pour $n \geqslant 1$ fixé. Soit E un ensemble à $n+1$ éléments.
On fixe $a \in E$. Il y a deux sortes de sous-ensembles de E :
  – les sous-ensembles A qui ne contiennent pas a : ce sont les sous-ensembles $A \subset E \setminus \{a\}$. Par l'hypothèse de récurrence il y en a 2^n.
  – les sous-ensembles A qui contiennent a : ils sont de la forme $A = \{a\} \cup A'$ avec $A' \subset E \setminus \{a\}$. Par l'hypothèse de récurrence il y a 2^n sous-ensembles A' possibles et donc aussi 2^n sous-ensembles A.

  Le bilan : $2^n + 2^n = 2^{n+1}$ parties $A \subset E$.
– Par le principe de récurrence, nous avons prouvé que si $\mathrm{Card}\, E = n$ alors $\mathrm{Card}\, \mathscr{P}(E) = 2^n$.

4.5. Coefficients du binôme de Newton

Définition 7

Le nombre de parties à k éléments d'un ensemble à n éléments est noté $\binom{n}{k}$ ou C_n^k.

Exemple 7

Les parties à deux éléments de $\{1,2,3\}$ sont $\{1,2\}$, $\{1,3\}$ et $\{2,3\}$ et donc $\binom{3}{2}=3$. Nous avons déjà classé les parties de $\{1,2,3,4,5\}$ par nombre d'éléments et donc

- $\binom{5}{0}=1$ (la seule partie n'ayant aucun élément est l'ensemble vide),
- $\binom{5}{1}=5$ (il y a 5 singletons),
- $\binom{5}{2}=10$ (il y a 10 paires),
- $\binom{5}{3}=10$,
- $\binom{5}{4}=5$,
- $\binom{5}{5}=1$ (la seule partie ayant 5 éléments est l'ensemble tout entier).

Sans calculs on peut déjà remarquer les faits suivants :

Proposition 10

- $\binom{n}{0}=1$, $\binom{n}{1}=n$, $\binom{n}{n}=1$.
- $\boxed{\binom{n}{n-k}=\binom{n}{k}}$
- $\boxed{\binom{n}{0}+\binom{n}{1}+\cdots+\binom{n}{k}+\cdots+\binom{n}{n}=2^n}$

Démonstration

1. Par exemple : $\binom{n}{1}=n$ car il y a n singletons.
2. Compter le nombre de parties $A\subset E$ ayant k éléments revient aussi à compter le nombre de parties de la forme $\complement A$ (qui ont donc $n-k$ éléments), ainsi $\binom{n}{n-k}=\binom{n}{k}$.
3. La formule $\binom{n}{0}+\binom{n}{1}+\cdots+\binom{n}{k}+\cdots+\binom{n}{n}=2^n$ exprime que faire la somme du nombre de parties à k éléments, pour $k=0,\ldots,n$, revient à compter toutes les parties de E.

Proposition 11

$$\boxed{\binom{n}{k}=\binom{n-1}{k}+\binom{n-1}{k-1}\quad 0<k<n}$$

Démonstration

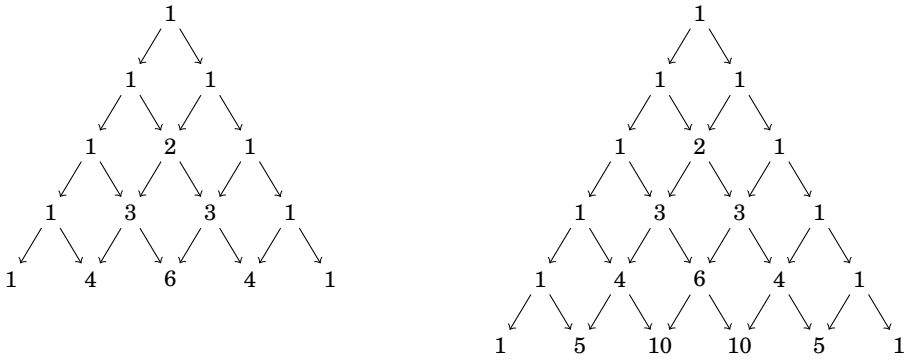
Soit E un ensemble à n éléments, $a\in E$ et $E'=E\setminus\{a\}$. Il y a deux sortes de parties $A\subset E$ ayant k éléments :

- celles qui ne contiennent pas a : ce sont donc des parties à k éléments dans E' qui a $n-1$ éléments. Il y a en a donc $\binom{n-1}{k}$,
- celles qui contiennent a : elles sont de la forme $A=\{a\}\cup A'$ avec A' une partie à $k-1$ éléments dans E' qui a $n-1$ éléments. Il y en a $\binom{n-1}{k-1}$.

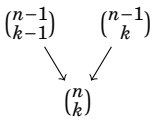
Bilan : $\binom{n}{k}=\binom{n-1}{k-1}+\binom{n-1}{k}$.

Le triangle de Pascal est un algorithme pour calculer ces coefficients $\binom{n}{k}$. La ligne du haut correspond à $\binom{0}{0}$, la ligne suivante à $\binom{1}{0}$ et $\binom{1}{1}$, la ligne d'après à $\binom{2}{0}$, $\binom{2}{1}$ et $\binom{2}{2}$.
La dernière ligne du triangle de gauche aux coefficients $\binom{4}{0}$, $\binom{4}{1}$, …, $\binom{4}{4}$.

Comment continuer ce triangle pour obtenir le triangle de droite ? Chaque élément de la nouvelle ligne est obtenu en ajoutant les deux nombres qui lui sont au-dessus à droite et au-dessus à gauche.



Ce qui fait que cela fonctionne c'est bien sûr la proposition 11 qui se représente ainsi :



Une autre façon de calculer le coefficient du binôme de Newton repose sur la formule suivante :

Proposition 12

$$\boxed{\binom{n}{k} = \frac{n!}{k!(n-k)!}}$$

Démonstration

Cela se fait par récurrence sur n. C'est clair pour $n = 1$. Si c'est vrai au rang $n-1$ alors écrivons $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$ et utilisons l'hypothèse de récurrence pour $\binom{n-1}{k-1}$ et $\binom{n-1}{k}$. Ainsi

$$\begin{aligned}\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k} &= \frac{(n-1)!}{(k-1)!(n-1-(k-1))!} + \frac{(n-1)!}{k!(n-1-k)!} \\ &= \frac{(n-1)!}{(k-1)!(n-k-1)!} \times \left(\frac{1}{n-k} + \frac{1}{k}\right) = \frac{(n-1)!}{(k-1)!(n-k-1)!} \times \frac{n}{k(n-k)} \\ &= \frac{n!}{k!(n-k)!}\end{aligned}$$

4.6. Formule du binôme de Newton

Théorème 1

Soient $a, b \in \mathbb{R}$ et n un entier positif alors :

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} \cdot b^k$$

Autrement dit :

$$(a+b)^n = \binom{n}{0} a^n \cdot b^0 + \binom{n}{1} a^{n-1} \cdot b^1 + \cdots + \binom{n}{k} a^{n-k} \cdot b^k + \cdots + \binom{n}{n} a^0 \cdot b^n$$

Le théorème est aussi vrai si a et b sont des nombres complexes.

Exemple 8

1. Pour $n = 2$ on retrouve la formule archi-connue : $(a+b)^2 = a^2 + 2ab + b^2$.
2. Il est aussi bon de connaître $(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$.
3. Si $a = 1$ et $b = 1$ on retrouve la formule : $\sum_{k=0}^{n} \binom{n}{k} = 2^n$.

Démonstration

Nous allons effectuer une récurrence sur n. Soit (P_n) l'assertion : $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} \cdot b^k$.

- *Initialisation.* Pour $n = 1$, $(a+b)^1 = \binom{1}{0} a^1 b^0 + \binom{1}{1} a^0 b^1$. Ainsi P_1 est vraie.
- *Hérédité.* Fixons $n \geqslant 2$ et supposons que P_{n-1} est vraie.

$$\begin{aligned}
(a+b)^n = (a+b)\cdot(a+b)^{n-1} &= a\left(a^{n-1} + \cdots + \binom{n-1}{k} a^{n-1-k} b^k + \cdots + b^{n-1}\right) \\
&\quad + b\left(a^{n-1} + \cdots + \binom{n-1}{k-1} a^{n-1-(k-1)} b^{k-1} + \cdots + b^{n-1}\right) \\
&= \cdots + \left(\binom{n-1}{k} + \binom{n-1}{k-1}\right) a^{n-k} b^k + \cdots \\
&= \cdots + \binom{n}{k} a^{n-k} b^k + \cdots = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} \cdot b^k
\end{aligned}$$

Ainsi P_{n+1} est vérifiée.

- *Conclusion.* Par le principe de récurrence P_n est vraie, pour tout $n \geqslant 1$.

Mini-exercices

1. Combien y a-t-il d'applications injectives d'un ensemble à n éléments dans un ensemble à $n+1$ éléments ?
2. Combien y a-t-il d'applications surjectives d'un ensemble à $n+1$ éléments dans un ensemble à n éléments ?
3. Calculer le nombre de façons de choisir 5 cartes dans un jeux de 32 cartes.
4. Calculer le nombre de listes à k éléments dans un ensemble à n éléments (les listes sont ordonnées : par exemple $(1,2,3) \neq (1,3,2)$).

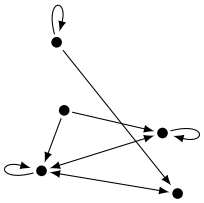
5. Développer $(a-b)^4$, $(a+b)^5$.
6. Que donne la formule du binôme pour $a=-1, b=+1$? En déduire que dans un ensemble à n éléments il y a autant de parties de cardinal pair que de cardinal impair.

5. Relation d'équivalence

5.1. Définition

Une ***relation*** sur un ensemble E, c'est la donnée pour tout couple $(x,y) \in E \times E$ de «Vrai» (s'ils sont en relation), ou de «Faux» sinon.

Nous schématisons une relation ainsi : les éléments de E sont des points, une flèche de x vers y signifie que x est en relation avec y, c'est-à-dire que l'on associe «Vrai» au couple (x,y).



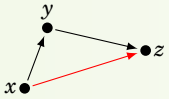
Définition 8

Soit E un ensemble et $\mathscr{R}$ une relation, c'est une ***relation d'équivalence*** si :

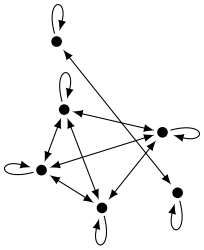
- $\forall x \in E,\ x\mathscr{R}x$, (***réflexivité***)

- $\forall x,y \in E,\ x\mathscr{R}y \implies y\mathscr{R}x$, (***symétrie***)

- $\forall x,y,z \in E,\ x\mathscr{R}y$ et $y\mathscr{R}z \implies x\mathscr{R}z$, (***transitivité***)



Exemple de relation d'équivalence :



5.2. Exemples

Exemple 9

Voici des exemples basiques.

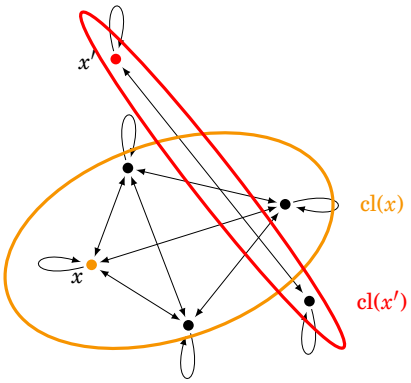
1. La relation $\mathscr{R}$ «être parallèle» est une relation d'équivalence pour l'ensemble E des droites affines du plan.
   - réflexivité : une droite est parallèle à elle-même,
   - symétrie : si D est parallèle à D' alors D' est parallèle à D,
   - transitivité : si D parallèle à D' et D' parallèle à D'' alors D est parallèle à D''.
2. La relation «être du même âge» est une relation d'équivalence.
3. La relation «être perpendiculaire» n'est pas une relation d'équivalence (ni la réflexivité, ni la transitivité ne sont vérifiées).
4. La relation $\leqslant$ (sur $E = \mathbb{R}$ par exemple) n'est pas une relation d'équivalence (la symétrie n'est pas vérifiée).

5.3. Classes d'équivalence

Définition 9

Soit $\mathscr{R}$ une relation d'équivalence sur un ensemble E. Soit $x \in E$, la ***classe d'équivalence*** de x est

$$\boxed{\mathrm{cl}(x) = \{y \in E \mid y \mathscr{R} x\}}$$



$\mathrm{cl}(x)$ est donc un sous-ensemble de E, on le note aussi $\overline{x}$. Si $y \in \mathrm{cl}(x)$, on dit que y un ***représentant*** de $\mathrm{cl}(x)$.

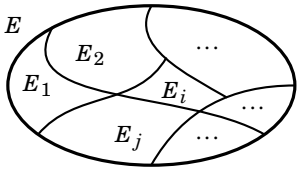
Soit E un ensemble et $\mathscr{R}$ une relation d'équivalence.

Proposition 13

On a les propriétés suivantes :

1. $\mathrm{cl}(x) = \mathrm{cl}(y) \iff x \mathscr{R} y$.
2. Pour tout $x, y \in E$, $\mathrm{cl}(x) = \mathrm{cl}(y)$ ou $\mathrm{cl}(x) \cap \mathrm{cl}(y) = \varnothing$.
3. Soit C un ensemble de représentants de toutes les classes alors $\{\mathrm{cl}(x) \mid x \in C\}$ constitue une partition de E.

Une ***partition*** de E est un ensemble $\{E_i\}$ de parties de E tel que $E = \bigcup_i E_i$ et $E_i \cap E_j = \varnothing$ (si $i \neq j$).



Exemples :

1. Pour la relation «être du même âge», la classe d'équivalence d'une personne est l'ensemble des personnes ayant le même âge. Il y a donc une classe d'équivalence formée des personnes de 19 ans, une autre formée des personnes de 20 ans,... Les trois assertions de la proposition se lisent ainsi :
   - On est dans la même classe d'équivalence si et seulement si on est du même âge.
   - Deux personnes appartiennent soit à la même classe, soit à des classes disjointes.
   - Si on choisit une personne de chaque âge possible, cela forme un ensemble de représentants C. Maintenant une personne quelconque appartient à une et une seule classe d'un des représentants.
2. Pour la relation «être parallèle», la classe d'équivalence d'une droite est l'ensemble des droites parallèles. À chaque classe d'équivalence correspond une et une seule direction.

Voici un exemple que vous connaissez depuis longtemps :

Exemple 10

Définissons sur $E = \mathbb{Z} \times \mathbb{N}^*$ la relation $\mathscr{R}$ par

$$(p,q)\mathscr{R}(p',q') \iff pq' = p'q.$$

Tout d'abord $\mathscr{R}$ est une relation d'équivalence :
- $\mathscr{R}$ est réflexive : pour tout (p,q) on a bien $pq = pq$ et donc $(p,q)\mathscr{R}(p,q)$.
- $\mathscr{R}$ est symétrique : pour tout (p,q), (p',q') tels que $(p,q)\mathscr{R}(p',q')$ on a donc $pq' = p'q$ et donc $p'q = pq'$ d'où $(p',q')\mathscr{R}(p,q)$.
- $\mathscr{R}$ est transitive : pour tout (p,q), (p',q'), (p'',q'') tels que $(p,q)\mathscr{R}(p',q')$ et $(p',q')\mathscr{R}(p'',q'')$ on a donc $pq' = p'q$ et $p'q'' = p''q'$. Alors $(pq')q'' = (p'q)q'' = q(p'q'') = q(p''q')$. En divisant par $q' \neq 0$ on obtient $pq'' = qp''$ et donc $(p,q)\mathscr{R}(p'',q'')$.

Nous allons noter $\frac{p}{q} = \mathrm{cl}(p,q)$ la classe d'équivalence d'un élément $(p,q) \in \mathbb{Z} \times \mathbb{N}^*$. Par exemple, comme $(2,3)\mathscr{R}(4,6)$ (car $2 \times 6 = 3 \times 4$) alors les classes de $(2,3)$ et $(4,6)$ sont égales : avec notre notation cela s'écrit : $\frac{2}{3} = \frac{4}{6}$.
C'est ainsi que l'on définit les rationnels : l'ensemble $\mathbb{Q}$ des rationnels est l'ensemble de classes d'équivalence de la relation $\mathscr{R}$.
Les nombres $\frac{2}{3} = \frac{4}{6}$ sont bien égaux (ce sont les mêmes classes) mais les écritures sont différentes (les représentants sont distincts).

5.4. L'ensemble $\mathbb{Z}/n\mathbb{Z}$

Soit $n \geqslant 2$ un entier. Définissons la relation suivante sur l'ensemble $E = \mathbb{Z}$:

$$a \equiv b \pmod{n} \iff a - b \text{ est un multiple de } n$$

Exemples pour $n = 7$: $10 \equiv 3 \pmod 7$, $19 \equiv 5 \pmod 7$, $77 \equiv 0 \pmod 7$, $-1 \equiv 20 \pmod 7$.

Cette relation est bien une relation d'équivalence :

- Pour tout $a \in \mathbb{Z}$, $a - a = 0 = 0 \cdot n$ est un multiple de n donc $a \equiv a \pmod{n}$.
- Pour $a, b \in \mathbb{Z}$ tels que $a \equiv b \pmod{n}$ alors $a - b$ est un multiple de n, autrement dit il existe $k \in \mathbb{Z}$ tel que $a - b = kn$ et donc $b - a = (-k)n$ et ainsi $b \equiv a \pmod{n}$.
- Si $a \equiv b \pmod{n}$ et $b \equiv c \pmod{n}$ alors il existe $k, k' \in \mathbb{Z}$ tels que $a - b = kn$ et $b - c = k'n$. Alors $a - c = (a - b) + (b - c) = (k + k')n$ et donc $a \equiv c \pmod{n}$.

La classe d'équivalence de $a \in \mathbb{Z}$ est notée $\overline{a}$. Par définition nous avons donc

$$\overline{a} = \mathrm{cl}(a) = \{b \in \mathbb{Z} \mid b \equiv a \pmod{n}\}.$$

Comme un tel b s'écrit $b = a + kn$ pour un certain $k \in \mathbb{Z}$ alors c'est aussi exactement

$$\overline{a} = a + n\mathbb{Z} = \{a + kn \mid k \in \mathbb{Z}\}.$$

Comme $n \equiv 0 \pmod{n}$, $n + 1 \equiv 1 \pmod{n}$, ... alors

$$\overline{n} = \overline{0}, \quad \overline{n+1} = \overline{1}, \quad \overline{n+2} = \overline{2}, \ldots$$

et donc l'ensemble des classes d'équivalence est l'ensemble

$$\boxed{\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}}$$

qui contient exactement n éléments.
Par exemple : pour $n = 7$, $\overline{0} = \{\ldots, -14, -7, 0, 7, 14, 21, \ldots\} = 7\mathbb{Z}$; $\overline{1} = \{\ldots, -13, -6, 1, 8, 15, \ldots\} = 1 + 7\mathbb{Z}$; ... ; $\overline{6} = \{\ldots, -8, -1, 6, 13, 20, \ldots\} = 6 + 7\mathbb{Z}$. Mais ensuite $\overline{7} = \{\ldots -7, 0, 7, 14, 21, \ldots\} = \overline{0} = 7\mathbb{Z}$. Ainsi $\mathbb{Z}/7\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{6}\}$ possède 7 éléments.

Remarque

Dans beaucoup de situations de la vie courante, nous raisonnons avec les modulos. Par exemple pour l'heure : les minutes et les secondes sont modulo 60 (après 59 minutes on repart à zéro), les heures modulo 24 (ou modulo 12 sur le cadran à aiguilles). Les jours de la semaine sont modulo 7, les mois modulo 12,...

Mini-exercices

1. Montrer que la relation définie sur $\mathbb{N}$ par $x \mathscr{R} y \iff \frac{2x+y}{3} \in \mathbb{N}$ est une relation d'équivalence. Montrer qu'il y a 3 classes d'équivalence.
2. Dans $\mathbb{R}^2$ montrer que la relation définie par $(x, y) \mathscr{R} (x', y') \iff x + y' = x' + y$ est une relation d'équivalence. Montrer que deux points (x, y) et (x', y') sont dans une même classe si et seulement s'ils appartiennent à une même droite dont vous déterminerez la direction.
3. On définit une addition sur $\mathbb{Z}/n\mathbb{Z}$ par $\overline{p} + \overline{q} = \overline{p+q}$. Calculer la table d'addition dans $\mathbb{Z}/6\mathbb{Z}$ (c'est-à-dire toutes les sommes $\overline{p} + \overline{q}$ pour $\overline{p}, \overline{q} \in \mathbb{Z}/6\mathbb{Z}$). Même chose avec la multiplication $\overline{p} \times \overline{q} = \overline{p \times q}$. Mêmes questions avec $\mathbb{Z}/5\mathbb{Z}$, puis $\mathbb{Z}/8\mathbb{Z}$.

Auteurs

Arnaud Bodin
Benjamin Boutin
Pascal Romon