

Quelques exemples de fonctions.

Exemple 3.5. Est-ce que

$$F : \mathbb{N} \rightarrow \mathbb{N}, F(m) = \frac{m(m+1)(m+5)}{3}$$

est une fonction ? Car $\frac{m(m+1)(m+5)}{3}$ semble être une fraction, et pas un nombre naturel.

Nous allons donner une *preuve cas par cas* que l'énoncé

"Si $m \in \mathbb{N}$ alors $\frac{m(m+1)(m+5)}{3} \in \mathbb{N}$ " est vrai.

Soit $m \in \mathbb{N}$. Il y a trois cas possible: existe un nombre naturel a tel que (i) $m = 3a$ ou (ii) $m = 3a + 1$ ou (iii) $m = 3a + 2$.

En cas (i): on a

$$F(m) = F(3a) = \frac{3a(3a+1)(3a+5)}{3} = a(3a+1)(3a+5) \in \mathbb{N};$$

en cas (ii) on a

$$F(m) = F(3a+1) = \frac{(3a+1)(3a+2)(3a+6)}{3} = (3a+1)(3a+2)(a+2) \in \mathbb{N};$$

et en cas (iii) on a

$$F(m) = F(3a+2) = \frac{(3a+2)(3a+3)(3a+7)}{3} = (3a+2)(a+1)(3a+7) \in \mathbb{N}.$$

Dans tous les cas $F(m) \in \mathbb{N}$.

Donc $F : \mathbb{N} \rightarrow \mathbb{N}$ est une fonction après tout.

Exemple 3.6. Soit A un ensemble. La *fonction identité* est la fonction $1_A : A \rightarrow A$ où

$$1_A(a) = a$$

pour chaque $a \in A$.

Soit $A \subseteq B$ un sous-ensemble. La *fonction inclusion* est la fonction $\iota : A \rightarrow B$:

$$\iota(a) = a$$

pour chaque $a \in A$.

Si

$$A = \{a, 1, \heartsuit, \pi, \emptyset\}, B = \{a, b, c, 1, 2, 3, \heartsuit, \clubsuit, \pi, \emptyset, \}$$

alors

$$1_A = \begin{pmatrix} a & 1 & \heartsuit & \pi & \emptyset \\ a & 1 & \heartsuit & \pi & \emptyset \end{pmatrix}$$

et

$$\iota_A = \begin{pmatrix} a & 1 & \heartsuit & \pi & \emptyset \\ a & 1 & \heartsuit & \pi & \emptyset \end{pmatrix}.$$

La différence entre 1_A et ι est le codomaine (mais la portée et la formule sont les mêmes).

3.5. Injectivité, surjectivité et bijectivité. Une fonction peut avoir des propriétés. Les suivantes sont les plus importantes.

Définition 3.6. Soit $F : A \rightarrow B$ une fonction. On dit que

- (i) F est injective si $F(a_1) = F(a_2)$ seulement si $a_1 = a_2$.
- (ii) F est surjective si chaque élément de B est l'image d'un élément de A .
- (iii) F est bijective si chaque élément de B est l'image d'un seul élément de A .

Conclusion: F est bijective si et seulement si F est injective et surjective. Par exemple, la fonction inclusion ι est injective, et la fonction identité 1_A est bijective.

Proposition 3.2. Soit la fonction $F : A \rightarrow B$ donnée par la notation "deux-lignes" (sans répétitions dans la première ligne), disons

$$F = \begin{pmatrix} a_1 & a_2 & a_3 & \dots & a_n \\ f_1 & f_2 & f_3 & \dots & f_n \end{pmatrix}.$$

Alors la fonction est

- (i) injective si et seulement si chaque élément de B se trouve au maximum une fois sur la 2-ième ligne;
- (ii) surjective si et seulement si chaque élément de B se trouve au minimum une fois sur la 2-ième ligne;
- (iii) bijective si et seulement si chaque élément de B se trouve exactement une fois sur la 2-ième ligne.

Proof. (i) Supposons que chaque élément de B se trouve au maximum une fois sur la deuxième ligne. Montrons par une *preuve directe* que F est injective .

Soient a et a' des éléments de A tels que $b = F(a) = F(a')$. Ces deux éléments a et a' se trouvent sur la première ligne, c'est à dire ils existent i et j tels que $a = a_i$ et $a' = a_j$ et donc $F(a) = F(a_i) = f_i$, $F(a') = F(a_j) = f_j$. Nous avons que $b = f_i = f_j$. Mais b se trouve au maximum une fois sur la 2-ième ligne. Ça veut dire $i = j$ et donc $a = a_i = a_j = a'$. Alors nous avons montré que F est injective (si chaque élément de B se trouve au maximum une fois sur la deuxième ligne).

Supposons F est injective. Nous allons montrer par une *preuve indirecte* que chaque élément de B se trouve au maximum une fois sur la deuxième ligne.

Supposons $b \in B$ se trouve au moins deux fois sur la 2-ième ligne, disons à positions i et j ($i \neq j$). Donc $b = f_i = f_j$. Mais $f_i = F(a_i)$ et $f_j = F(a_j)$, alors $F(a_i) = F(a_j)$ et $a_i \neq a_j$. Donc F n'est pas injective. On conclut la preuve indirecte que si F est injective alors chaque élément de B se trouve au maximum une fois sur la deuxième ligne.

Ça finit la preuve de (i).

(ii) et (iii): exercices. □

Exemple 3.7. Soit $A := \{a, b, c\}$ et $B := \{1, 2, 3, 4\}$.

$F_1 : A \rightarrow B$ définie par $F_1 := \begin{pmatrix} a & b & c \\ 3 & 2 & 1 \end{pmatrix}$ est injective,

$F_2 : B \rightarrow A$ définie par $F_2 := \begin{pmatrix} 1 & 2 & 3 & 4 \\ a & b & c & a \end{pmatrix}$ est surjective. Il n'existe pas de fonction de A dans B qui est surjective et il n'existe pas de fonction de B dans A qui est injective. Vous voyez pourquoi ?

Proposition 3.3. Soient A et B deux ensembles finis.

- (i) Il existe une fonction injective $F : A \rightarrow B$ si et seulement si $|A| \leq |B|$.
- (ii) Il existe une fonction surjective $F : A \rightarrow B$ si et seulement si $|A| \geq |B|$.
- (iii) Il existe une fonction bijective $F : A \rightarrow B$ si et seulement si $|A| = |B|$.

Proof. Avant de commencer les preuves, fixons une suite ordonnée *sans répétitions* des éléments de A , disons

$$A = \{a_1, a_2, \dots, a_n\}$$

où $n = |A|$. Il y a beaucoup de façons, mais fixons une manière.

Et fixons aussi une suite ordonnée sans répétitions des éléments de B , disons

$$B = \{b_1, b_2, \dots, b_m\}$$

où $m = |B|$.

(i) Supposons il existe une fonction injective $F : A \rightarrow B$. Nous voulons montrer $|A| \leq |B|$. Montrons d'abord par une *preuve par l'absurde* que dans la suite ordonnée $(F(a_1), F(a_2), \dots, F(a_n))$ il n'y a pas de répétition.

Sinon, il y a $i \neq j$ tels que $F(a_i) = F(a_j)$. Par la définition d'injectivité il suit que $a_i = a_j$. Mais dans la suite choisie des a_k 's il n'y a pas de répétitions. Donc $i = j$. et au même temps $i \neq j$. Ce qui est absurde. Donc en effet, dans la suite ordonnée $(F(a_1), F(a_2), \dots, F(a_n))$ il n'y a pas de répétitions.

Il suit que le sous-ensemble

$$\text{Im}(F) = \{F(a_1), F(a_2), \dots, F(a_n)\} \subseteq B$$

a $n = |A|$ éléments différents. Et le fait que $\text{Im}(F) \subseteq B$ implique que $|A| = |\text{Im}(F)| \leq |B|$.

Nous venons de montrer que s'il existe une fonction injective $F : A \rightarrow B$ alors $|A| \leq |B|$.

Deuxième partie de la preuve de (i). Supposons $|A| \leq |B|$. Il faut montrer qu'il existe une fonction injective $F : A \rightarrow B$.

Définition d'une telle fonction, à l'aide de nos deux suites ordonnées choisies :

$$F(a_i) := b_i$$

pour chaque $1 \leq i \leq n = |A|$. Ou en notation "deux-lignes"

$$F := \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix}.$$

Ça fait du sens, car $n \leq m = |B|$! C'est une fonction injective, car la deuxième ligne il n'y a pas de répétitions, prop. 3.2(ii). Donc en effet si $|A| \leq |B|$, alors il existe une fonction injective $F : A \rightarrow B$.

La preuve de (i) est complète.

(iii) Si on a montré (i) et (ii), alors (iii) en suit tout de suite.

La preuve de (ii) est un exercice. □

Remarque. On dit que deux ensembles A et B sont de même *cardinalité* s'il existe une bijection de A dans B , voir [R, p.71]. Par la proposition, si les deux ensembles sont finis, alors ils sont de même cardinalité si et seulement si $|A| = |B|$.

Si un ensemble A et l'ensemble \mathbb{N} sont de même cardinalité on dit que A est dénombrable.

L'ensemble des nombres entiers, l'ensemble des fractions et l'ensemble des nombres premiers sont tous dénombrable. Mais l'ensemble des nombre réels n'est pas dénombrable.

3.6. Composition de fonctions.

Définition 3.7. Soit $F : A \rightarrow B$ et $G : B \rightarrow C$ deux fonctions.

Alors la composition est la fonction

$$G \circ F : A \rightarrow C$$

définie par

$$(G \circ F)(a) = G(F(a)).$$

Exemple 3.8. Soit $A = \{a, b, c\}$, $B = \{1, 2, 3, 4\}$, $C = \mathbb{N}$. Et $F : A \rightarrow B$ donnée par

$$F := \begin{pmatrix} a & b & c \\ 3 & 2 & 4 \end{pmatrix};$$

$G : B \rightarrow C$ donnée par

$$G := \begin{pmatrix} 1 & 2 & 3 & 4 \\ 13 & 23 & 33 & 4344 \end{pmatrix}.$$

Alors $G \circ F : \{a, b, c\} \rightarrow \mathbb{N}$:

$$G \circ F = \begin{pmatrix} a & b & c \\ 33 & 23 & 4344 \end{pmatrix}$$

Par exemple

$$(G \circ F)(c) = G(F(c)) = G(4) = 4344.$$

Exemple 3.9. Soit $F : \mathbb{N} \rightarrow \mathbb{N}$, $F(n) = n^2 + 1$ et $G : \mathbb{N} \rightarrow \mathbb{N}$, $G(n) = n^3 + n$. Alors $F \circ G : \mathbb{N} \rightarrow \mathbb{N}$ et $G \circ F : \mathbb{N} \rightarrow \mathbb{N}$ sont données par:

$$(F \circ G)(n) = F(G(n)) = F(n^3 + n) = (n^3 + n)^2 + 1$$

et

$$G \circ F(n) = G(F(n)) = G(n^2 + 1) = (n^2 + 1)^3 + (n^2 + 1).$$

Exercice 3.1. Soient $F_1 : A \rightarrow B$, $F_2 : B \rightarrow C$ et $F_3 : C \rightarrow D$ trois fonctions. Montrer que $F_3 \circ (F_2 \circ F_1) = (F_3 \circ F_2) \circ F_1$ comme fonctions de A dans D .

Remarque. Soit $F : A \rightarrow B$ et $G : D \rightarrow C$ deux fonctions et $B \subset D$. On peut quand-même définir la composition, en utilisant $\iota : B \rightarrow D$, comme la composition $G \circ (\iota \circ F)$. Est-ce que ce qu'on voudrait?

3.7. Fonction inverse.

Théorème 3.1. *Soit $F : A \rightarrow B$ une fonction. Alors F est bijective si et seulement si il existe une fonction $G : B \rightarrow A$ telle que $F \circ G = 1_B$ et $G \circ F = 1_A$.*

Dans cette situation cette fonction G est unique, appelée la *fonction inverse* et notée

$$G = F^{-1}.$$

En fait, parce que F est bijective, pour chaque $b \in B$ il existe un unique $a \in A$ tel que $F(a) = b$. Alors $F^{-1}(b) = a$. Une fonction inverse existe seulement si la fonction est bijective.

Proof. (Supposons $F : A \rightarrow B$ est bijective. Définition d'une fonction $G : B \rightarrow A$: Soit $b \in B$, il existe un unique $a \in A$ tel que $F(a) = b$. Posons $G(b) := a$. Pour chaque $a \in A$ on a:

$$(G \circ F)(a) = G(F(a)) = G(b) = a.$$

Donc $G \circ F = 1_A$. Et pour chaque $b \in B$:

$$(F \circ G)(b) = F(G(b)) = F(a) = b.$$

Donc $F \circ G = 1_B$.

De l'autre côté, supposons qu'il existe une fonction $G : B \rightarrow A$ telle que $F \circ G = 1_B$ et $G \circ F = 1_A$. Soit $b \in B$. Définissons $a := G(b) \in A$. Alors

$$F(a) = F(G(b)) = (F \circ G)(b) = 1_B(b) = b.$$

Donc a est un préimage de b pour F . Nous avons montré que F est surjective.

Supposons $a_1, a_2 \in A$ tels que $F(a_1) = F(a_2)$. Donc

$$a_1 = 1_A(a_1) = (G \circ F)(a_1) = G(F(a_1)) = G(F(a_2)) = (G \circ F)(a_2) = a_2.$$

Donc F est aussi injective. On conclut la preuve, car une fonction surjective et injective est automatiquement bijective. \square

Preuve du commentaire après le théorème. Supposons $F : A \rightarrow B$ est injective. Supposons $G : B \rightarrow A$ et $G' : B \rightarrow A$ telles que $G \circ F = 1_A$ et aussi $G' \circ F = 1_A$. Soit $b \in B$. Parce que F est bijective il existe un $a \in A$ tel que $F(a) = b$. Alors

$$G(b) = G(F(a)) = (G \circ F)(a) = 1_A(a) = (G' \circ F)(a) = G'(F(a)) = G'(b)$$

Donc pour chaque $b \in B$ on a $G(b) = G'(b)$, c.-à-d., $G = G'$. \square

Exemple 3.10. Soit $\mathbb{R}_{>0}$ l'ensemble de nombres réels strictement positifs.

L'application $\exp : \mathbb{R} \rightarrow \mathbb{R}_{>0}$ est bijectif. Sa fonction inverse est $\ln : \mathbb{R}_{>0} \rightarrow \mathbb{R}$.

Nous donnons un exemple d'une fonction bijective un peu plus compliqué à comprendre, mais la preuve n'est pas difficile.

Théorème 3.2. *Soient A et B deux ensembles non-vides. Supposons $n = |A|$ est fini. Il existe une fonction bijective $\phi : \text{Fonctions}(A, B) \rightarrow B^n$.*

Corollaire 3.1. *Soient A et B deux ensembles finis non-vides. Posons $n = |A|$. On a*

$$|\text{Fonctions}(A, B)| = |B^n|.$$

Le corollaire est une conséquence directe du théorème et prop.3.3(iii).

Proof. Fixons une liste ordonnée des éléments de A , sans répétitions, disons $A = \{a_1, a_2, \dots, a_n\}$.

Posons $\phi : \text{Fonctions}(A, B) \rightarrow B^n$ par

$$\phi \left(F = \begin{pmatrix} a_1 & a_2 & a_3 & \dots & a_n \\ b_1 & b_2 & b_3 & \dots & b_n \end{pmatrix} \right) := (b_1, b_2, b_3, \dots, b_n) \in B^n.$$

ϕ a la fonction inverse $\psi : B^n \rightarrow \text{Fonctions}(A, B)$

$$\psi((b_1, b_2, \dots, b_n)) := F = \begin{pmatrix} a_1 & a_2 & a_3 & \dots & a_n \\ b_1 & b_2 & b_3 & \dots & b_n \end{pmatrix}$$

□

4. LOGIQUE

Après cet introduction à la théorie des ensemble nous allons faire une introduction à la logique. Mais nous allons aussi continuer de faire des constructions avec des ensembles !

Définition 4.1. ⁴ Une "proposition (logique)" est un énoncé qui peut être vrai ou faux, mais non les deux à la fois.

Un énoncé dans la vraie vie peut être vrai et faux au même temps: dans ce cas ce n'est pas considéré comme une proposition logique.

Exemples:

- $p_1 :=$ "Toronto est la capitale du Canada" (faux)
- $p_2 :=$ "le chat est un animal" (vrai)
- $p_3 :=$ "1 + 1 = 3" (faux)
- $p_4 :=$ "si $x \in E$ et $E \subseteq F$ alors $x \in F$ " (vrai)
- $p_5 :=$ "Chaque nombre naturel $n > 2$ pair est la somme de deux nombres premier" (vrai ou faux, mais inconnu)

On a le sentiment qu'on pourrait décomposer p_4 comme une combinaison d'autres propositions plus simples. En effet, c'est le cas. Et aussi, qu'on pourrait combiner des propositions pour obtenir des propositions plus compliquées. En effet.

Je répète: un énoncé est appelé une proposition logique, si cet énoncé peut être vrai ou faux. Mais ce n'est pas nécessaire d'aussi connaître la réponse, la *vérité de la proposition*.

Le but des mathématiques (et les sciences) est de formuler des propositions logique et d'en décider la vérité. Par exemple p_5 est vraie ou fausse mais on ne sais pas encore.

Plusieurs propositions ont été proposées dans les mathématiques, dont on ne connaît pas encore la vérité. Si on a des raisons de croire qu'une proposition soit vraie, mais on ne peut pas le montrer dit que c'est une conjecture. Par exemple, Goldbach ⁵ semble avoir cru que la proposition p_5 soit vraie.

Conjecture 4.1 (Goldbach). *Chaque nombre naturel $n > 2$ pair est la somme de deux nombres premier.*

⁴Voir [R, p.2]

⁵Voir "Conjecture de Goldbach" dans wikipedia

Le but des mathématiques est à partir de quelques *hypothèses* de base, des propositions logiques qu'on suppose vraie, de produire une longue liste de propositions logiques qui sont *aussi vraies* (et espérons "intéressantes" pour nous). En ça en utilisant la logique et en construisant des ensembles.

L'hypothèse le plus important est que l'ensemble des entiers \mathbb{N} avec ses propriétés élémentaires EXISTE. On va discuter ses propriétés plus tard.

4.1. Les combinaisons simples logiques. Soient p et q deux propositions logiques.

La proposition " p ou q " est aussi une proposition logique, on écrit

$$p \vee q,$$

qui est *par définition* vraie si p est vraie ou si q est vraie (ou si tous les deux sont vraies).

Et c'est fausse sinon (c.-à-d. si p et q sont fausses).

Comme dans la vraie vie. (Parfois on dit la disjonction de p et de q . Mais pas moi.)

Dans la vraie vie il y a deux "ou"s.

La proposition " p ou-strict q " est aussi une proposition logique, on écrit

$$p \oplus q,$$

qui est *par définition* vraie si p est vraie ou si q est vraie (mais pas si tous les deux sont vraies).

Et c'est fausse sinon (c.-à-d. si p et q sont tous les deux fausse ou tous les deux vraies).

(Parfois on dit la disjonction exclusive de p et de q .)

La proposition " p et q " est aussi une proposition logique, on écrit

$$p \wedge q,$$

qui est *par définition* vraie si p est vraie et si aussi q est vraie. Et c'est fausse sinon (c.-à-d. si p est fausse ou si q est fausse (ou tous les deux sont fausses)).

(Parfois on dit la conjonction de p et de q .)

La proposition "non- p " (ou "pas- p ") est aussi une proposition logique (dite composée), on écrit

$$\neg p,$$

qui est *par définition* vraie si p est fausse. Et c'est fausse sinon (c.-à-d. si p est vraie).

On dit aussi la *négation* de p .

La proposition "si p alors q ", ou " p implique q ", on écrit

$$p \rightarrow q,$$

est aussi une proposition logique composée, qui est *par définition* vraie si (p est vraie et q est vraie) ou (si p est fausse). Et c'est fausse sinon (c.-à-d. uniquement si p est vraie mais q est fausse). On dit p est l'hypothèse et q la conclusion de "l'implication $p \rightarrow q$ "

Dernière définition. La proposition " p si et seulement si q ", on écrit

$$p \leftrightarrow q,$$

est aussi une proposition logique, qui est *par définition* vraie si (p et q sont tous les deux vraies) ou si (p et q sont tous les deux fausses).

Et c'est fausse sinon (c.-à-d. une des deux est vraie et l'autre est fausse). (On dit aussi " p biconditionnelle q ".)

Remarque. Soient p et q deux propositions logiques. Il faut bien comprendre: $p \rightarrow q$ est une proposition logique, qui peut être vraie ou faux.

Qu'est-ce qu'on peut dire a propos de la vérité de p et q si on sait que l'implication

$$p \rightarrow q$$

est vraie ? Il y a deux possibilités:

soit p est fausse (et q n'importe: "je m'en fous"), soit p ET q sont vraies. Le sense inverse aussi correct.

Si $p \rightarrow q$ est fausse alors nécessairement: p est vraie et q est fausse.

Il faut aussi bien comprendre que $p \leftrightarrow q$ est soi-même une proposition logique, qui peut être vraie ou faux. Si $p \leftrightarrow q$ est vraie: alors on a deux possibilités: (i) p ET q sont vraies ou (ii) p ET q sont fausses. Et si $p \leftrightarrow q$ est faux alors (p est vraie ET q est fausse) ou (p est fausse ET q est vraie).

Maintenant le jeu de la logique commence en combinant ces opérations simples.

DÉPARTEMENT DE MATHÉMATIQUES ET DE STATISTIQUE, UNIVERSITÉ DE MONTRÉAL, C.P. 6128, SUCCURSALE
CENTRE-VILLE, MONTRÉAL (QUÉBEC), CANADA H3C 3J7
E-mail address: `broera@DMS.UMontreal.CA`