MAT-22257

⟨⟨*Notes complémentaires sur la théorie des relations et exemples de démonstrations de type "classique"*⟩⟩

Par François Laviolette
Université Laval

Version : Été 2007

1 Introduction

Les démonstrations que nous avons étudiées jusqu'à maintenant sont de type "formel". Elles sont basées sur une très longue liste d'axiomes et de théorèmes déjà démontrés qu'on essaie de composer ensemble via des règles d'inférence de base. Cette approche est très mécanisée, en ce sens qu'on peut assez facilement développer des algorithmes permettant de vérifier si telle ou telle démonstration est valide ou non. En fait des structures similaires à celle que nous avons étudiées jusqu'à maintenant ont été implémentées afin de vérifier automatiquement si certains logiciels sont conforment ou pas à leur spécification. Dans ce chapitre et pour le reste de la session nous aborderons les démonstrations mathématiques selon un point de vue différent, davantage répendues en mathématique, que nous dénommerons "démonstrations de type classique". Dans cette approche, on met davantage l'accent sur la signification des énoncés dans la construction d'une démonstration. De façon simplifiée, on peut dire qu'une démonstration formelle s'adresse davantage à un ordinateur qui peut alors mécaniquement vérifier la validité de la preuve, alors qu'une démonstration classique s'adresse à des humains prenant davantage la forme d'une explication du pourquoi un énoncé est vrai ou non. D'ailleurs, les démonstrations "classiques" prendront davantage la forme de véritable texte français. Ceci dit, les démonstrations de type formel et classique sont deux points de vue d'un seul et même concept, les approches sont différentes, mais en bout de ligne, équivalentes puisque bâties sur les mêmes axiomes et règles d'inférence des mathématiques.

2 Deux idées sous-jacentes aux démonstrations de type “classique”

L’approche est basée principalement sur deux questions importantes qui sont respectivement :

1. Que faire si l’énoncé qu’on souhaite démontrer contient un quantificateur universel (c.-à-d., un $\forall$) ?
2. Que faire si l’énoncé qu’on souhaite démontrer contient un quantificateur existentiel (c.-à-d., un $\exists$) ?

2.1 une démonstration avec un $\forall$

L’idée ici est d’appliquer le méta-théorème qui dit que démontrer $(\forall x : X \mid Q(x) : P(x))$ revient à démontrer que pour une entité inconnue fixée x appartenant au type X, on peut **déduire** que x satisfait P en **ne supposant** sur x **que** le fait qu’il satisfasse Q.

Ainsi, une preuve “classique” d’un énoncé commençant par un $\forall$ sera toujours structurée comme suit :

Démonstration
On veut montrer : $(\forall x : X \mid Q(x) : P(x))$.
Soit $x : X$, choisi tel que $Q(x)$ est vrai.
Alors pour telle raison blablabla.
Ce qui implique ceci et celà.
Et on peut finalement en conclure que $P(x)$ est vrai.
C.Q.F.D.

Notez que la démonstration commence par une “présentation” de la variable x, de son type et, le cas échéant, de la ou les propriétés que nous savons que cette variable satisfait. C’est une étape essentielle. Dans une démonstration, on ne peut utiliser une variable qui n’a pas été “présentée”, on doit d’abord s’entendre avec le lecteur sur ce qu’est cette inconnue. En échange, une fois cette étape faite, même si la valeur de la variable est inconnue, elle ne changera plus jusqu’à la fin de la démonstration. Autrement dit, une fois “présentée”, une variable reste inconnue, mais ne varie plus.

Notez également que la démonstration se termine par le fait qu’après plusieurs étapes d’argumentation mathématiquement correcte, on en arrive à conclure que cette variable x doit obligatoirement satisfaire la propriété P.

2.2 une démonstration avec un $\exists$

L’idée ici est simplement de comprendre que démontrer $(\exists x : X \mid Q(x) : P(x))$ revient à trouver un élément x de l’ensemble X dont on est **sûr** de l’existence et dont on est **sûr** qu’il satisfasse la propriété Q. Cependant, il faut en plus avoir “intelligemment” choisi ce x de telle sorte qu’on puisse ensuite déduire que ce x satisfait la propriété P.

Ainsi, une preuve “classique” d’un énoncé commençant par un $\exists$ sera toujours structurée comme suit :

Démonstration
On veut montrer : $(\exists x : X \mid Q(x) : P(x))$.
Soit $x : X$, choisi de telle façon. $\langle$ Un tel x existe et satisfait la propriété Q car blablabla.$\rangle$
Alors pour telle et telle raisons, on a donc ceci et celà.
Ce qui nous permet de conclure que $P(x)$ est vrai.
C.Q.F.D.

Notez qu'ici encore, on n'utilse pas une variable sans l'avoir préalablement présentée. Mais contrairement à la situation du $\forall$, on doit au moment de sa présentation être sûr de l'existence d'une telle variable. L'unique raison pour laquelle à la sous-section 2.1, on ne se préoccupe pas de savoir si un tel x existe, c'est que s'il n'existe pas de $x : X$ tel que $Q(x)$ est vrai, alors $(\forall x : X \mid Q(x) : P(x))$ est nécessairement vrai. Donc, en démonstration classique, on présente **toujours** une variable avant de l'utiliser et à moins qu'elle n'origine d'un $\forall$, on s'assure toujours de son existence dans ce contexte.

2.3 une démonstration en générale

Une démonstration de type "classique" est bien entendu quelque chose de bien plus complexe que ce que les deux dernières sous-sections en ont dit. Cependant, ces dernières serviront de balises pour les démonstrations relativement simples qui seront demandées à l'intérieur de ce cours. Pour les démonstrations plus costaudes, vous n'aurez pas à les faire par vous-mêmes, mais seulement (et c'est déjà pas mal) à les comprendre.

Voici un exemple simple d'énoncé, suivit d'une première tentative de démonstration incorrecte et d'une seconde tentative qui sera correcte.

Démontrons que $(\forall n : \mathbb{N} \mid : (\exists m : \mathbb{N} \mid : m > n))$

Première tentative de démonstration (incorrecte)
Soit $n : \mathbb{N}$.
Soit m, un nombre *magique* qui est plus grand que tout nombre naturel.
Alors bien sûr, on a que $m > n$.

C.Q.F.D.

Bien évidemment, ce qui clôche dans cette démonstration, c'est qu'il n'existe pas de tel nombre magique. Cependant, si pour une raison ou une autre, on pouvait démontrer qu'un tel nombre existe, alors la démonstration deviendrait correcte. En attendant, voici ce qu'il aurait fallu faire :

Démontrons que $(\forall n : \mathbb{N} \mid : (\exists m : \mathbb{N} \mid : m > n))$

Deuxième tentative de démonstration (correcte)
Soit $n : \mathbb{N}$.
Soit $m := n + 1$, $\langle$ Un tel m existe, il est même lui-même un nombre de $\mathbb{N}$ — Voir les propriétés de l'arithmétique. $\rangle$
Alors bien sûr, on a que $m = n + 1 > n$. $\langle$ — Propriété de l'arithmétique. $\rangle$

C.Q.F.D.

Notez que le m qu'on a choisi ici est construit à partir du n qui avait préalablement été présenté, ce qui est tout à fait légal. On n'aurait cependant pas pu faire un tel argument si nous avions eu à démontrer $(\exists m : \mathbb{N} \mid : (\forall n : \mathbb{N} \mid : m > n))$. D'ailleurs, ce dernier énoncé est faux, donc impossible à démontrer.

Notez aussi qu'à l'intérieur de ce cours, nous prendrons toutes les propriétés de l'arithmétique pour acquises. Ainsi, tout comme ce fut le cas lors de la deuxième tentative de démonstration, les propriétés de base de l'arithmétique sont supposées connues de tous et n'ont donc pas à être explicitement justifiées, une simple référence de la forme "Propriété de l'arithmétique" suffira. En effet, nous savons tous que si n est un nombre naturel, $n + 1$ est plus grand que n.

2.4 une démonstration avec un $\neg\exists$ ou un $\neg\forall$

Les démonstrations de type "classique" sont mal adaptées aux énoncés contenant un $\neg\exists$ ou un $\neg\forall$. En effet, il est difficile de "présenter" une variable x qui "n'existe pas" ou de démontrer que parmi tous les x possibles, il y en a qui ne satisfont pas P. Pour ces raisons, il est utile en de telles situations de faire appel aux lois de De Morgan. En voici un exemple.

Démontrons que $\neg(\exists m : \mathbb{N} \mid : (\forall n : \mathbb{N} \mid : m > n))$

Démonstration
Nous devons donc démontrer que $\neg(\exists m : \mathbb{N} \mid : (\forall n : \mathbb{N} \mid : m > n))$
Ce qui est équivalent à démontrer $(\forall m : \mathbb{N} \mid : \neg(\forall n : \mathbb{N} \mid : n < m))$. ⟨ *Voir* ***(7.20)****, Axiome, De Morgan.* ⟩
Ce qui est équivalent à démontrer $(\forall m : \mathbb{N} \mid : (\exists n : \mathbb{N} \mid : \neg(n < m)))$. ⟨ *Voir* ***(7.21)(b)****, De Morgan* ⟩

Démontrons donc que $(\forall m : \mathbb{N} \mid : (\exists n : \mathbb{N} \mid : \neg(n < m)))$.

Soit $m : \mathbb{N}$.
Soit $n := m + 1$, ⟨ Un tel n existe et **est bien** un nombre de $\mathbb{N}$ — Propriétés de l'arithmétique. ⟩
Alors on a que $n = m + 1 \geq m$. ⟨ — Propriété de l'arithmétique. ⟩
Ce qui implique que $\neg(n < m)$. ⟨ — Propriété de l'arithmétique. ⟩

C.Q.F.D.

Notez finalement que les lettres "C.Q.F.D." signifie "Ce qu'il fallait démontrer". Alors avant de les écrire, il est important de s'assurer que ce qu'on a fait est bien *ce qu'il fallait démontrer*.
Dans la démonstration précédente, on devait démontrer $(\forall m : \mathbb{N} \mid : (\exists n : \mathbb{N} \mid : \neg(n < m)))$ et on a
(1) chosi un $m : \mathbb{N}$ tout à fait quelconque (on a rien dit sur ce m hormis qu'il était dans $\mathbb{N}$).
(2) choisi un n, pas n'importe lequel, mais dont on était sûr de l'existence et de son appartenance à $\mathbb{N}$.
(3) grâce à une certaine séquence d'arguments mathématiquement corrects, on a réussi à démontrer que pour ce m et ce n, on a bien $\neg(n < m)$.
Ce Qu'il Fallait Démontrer.

2.5 une démonstration avec un $\Leftrightarrow$

Contrairement à leurs pendants formels, les démonstrations de type "classique" sont mal adaptées aux énoncés contenant un $\equiv$ (classiquement noté $\Leftrightarrow$). La principale raison vient du fait qu'une démonstration de type "classique" est davantage construite à l'image de la pensée humaine et donc utilise fortement ce qu'on appelle le *Modus Ponens*. Le Modus Ponens (ou "mode de raisonnement", en Français) est un type de raisonnement logique consistant à montrer un énoncé Q en montrant d'abord qu'un autre énoncé P est vrai et en montrant ensuite que $P \Rightarrow Q$. Si on y réfléchiy un peu, on constate que c'est fondamentalement de cette façon que l'humain argumente.

Ainsi, en démonstrations "classiques", il est très souvent préférable de scinder une démonstration de type $P \Leftrightarrow Q$ en deux parties : la première étant une démonstration de $P \Rightarrow Q$ et la seconde, une démonstration de

$P \Leftarrow Q$. Par le principe de l'implication mutuelle, on sait que c'est équivalent à démontrer directement $P \Leftrightarrow Q$, car

$$P \Rightarrow Q \ \wedge \ P \Leftarrow Q \ \ \equiv \ \ P \Leftrightarrow Q.$$

2.5.1 Exemples de démonstrations en présence d'un $\Leftrightarrow$

Théorème C.1 (Définitions équivalentes de la transitivité.)
Soit ρ une relation sur un ensemble B. Alors,

$$\rho^2 \subseteq \rho \ \ \equiv \ \ (\forall a, b, c \mid a\rho b \wedge b\rho c : a\rho c).$$

Démonstration
$\boxed{\Rightarrow:}$ Supposons donc que $\rho^2 \subseteq \rho$ (c.-à-d. : $\rho \circ \rho \subseteq \rho$).
Et démontrons que $(\forall a, b, c \mid a\rho b \wedge b\rho c : a\rho c)$.
Soient a, b, c, choisis tels que $a\rho b$ et $b\rho c$.
Alors on a $a(\rho \circ \rho)c$. ⟨ Définition de $\circ$. ⟩
Donc, on a $a\rho^2 c$. ⟨ Définition de ρ^2. ⟩
C'est-à-dire $\langle a, c\rangle \in \rho^2$.
Donc, on a $\langle a, c\rangle \in \rho$. ⟨ Car par hypothèse, on a $\rho^2 \subseteq \rho$. ⟩
Et donc $a\rho c$.

($\Rightarrow$: est démontré.)

$\boxed{\Leftarrow:}$ Supposons donc que $(\forall a, b, c \mid a\rho b \wedge b\rho c : a\rho c)$.
Et démontrons que $\rho^2 \subseteq \rho$, en démontrant que $(\forall a, c \mid \langle a, c\rangle \in \rho^2 : \langle a, c\rangle \in \rho)$.
Soient a et c, choisis tels que $\langle a, c\rangle \in \rho^2$.
Alors on a $\langle a, c\rangle \in \rho \circ \rho$. ⟨ Définition de ρ^2. ⟩
Soit b, choisi tel que $a\rho b$ et $b\rho c$. ⟨ Un tel b existe car $\langle a, c\rangle \in \rho \circ \rho$, voir définition de $\circ$. ⟩
Alors on a $a\rho c$. ⟨ Car par hypothèse : $(\forall a, b, c \mid a\rho b \wedge b\rho c : a\rho c)$. ⟩
Et donc, on a $\langle a, c\rangle \in \rho)$.

($\Leftarrow$: est démontré.)

C.Q.F.D.

RAPPEL :

- On dira qu'une relation $\rho \subseteq B \times C$ a la propriété de

$$\begin{cases} (a) & \textit{totalité} & \text{si} & (\forall b : B \mid : (\exists c : C \mid : b\rho c)) \\ (b) & \textit{surjectivité} & \text{si} & (\forall c : C \mid : (\exists b : B \mid : b\rho c)) \\ (c) & \textit{déterminisme} & \text{si} & (\forall\ b : B,\ c, c' : C \mid : b\rho c \wedge b\rho c' \ :\ c = c') \\ (d) & \textit{injectivité} & \text{si} & (\forall\ b, b' : B,\ c : C \mid : b\rho c \wedge b'\rho c \ :\ b = b') \end{cases}$$

- Une relation est appelée une application si elle est à la fois totale et déterministe.
  Autrement dit, une relation $f \subseteq X \times Y$ est une application lorsque pour chaque $x \in X$

  il existe **un** et **un seul** $y \in Y$ tel que $x\rho y$

  car le fait que pour chaque $x \in X$ il existe **un** $y \in$ établi que ρ est une relation totale et le fait que pour chaque $x \in X$ il n'existe qu **un seul** $y \in$ établi que ρ est une relation déterministe.

- Ainsi, si une relation f est définie par une *règle de correspondance* qui est bien définie (c'est-à-dire que cette règle fait effectivement correspondre à chaque élément de l'ensemble de départ **un** et **un seul** élément de l'ensemble d'arrivé), alors la relation f est une application.

NOTATION À DONNER

Note 1 : lorsqu'une relation f est une application, l'expression $\langle x, y\rangle \in f$ pourra être remplacée par $f(x) = y$ (ou encore $f.x = y$). Contrairement au cas où la relation f n'est pas une application, cette nouvelle notation ne comporte ici aucune ambiguïté puisque qu'à chaque "x" de l'ensemble de départ ne correspond qu'**un** et **un seul** "y" de l'ensemble d'arrivée.

Note 2 : pour "connaître complètement" une application f, il suffit d'en connaître l'ensemble de départ et l'ensemble d'arrivée, et de savoir à quel élément y de l'ensemble d'arrivée correspond chacun des éléments x de l'ensemble de départ. (Ce y est noté $f(x)$.)

Autrement dit, une application f peut être définie à l'aide d'une *règle de correspondance* pourvu que soit préalablement définis l'ensemble de départ de f et l'ensemble d'arrivée de f.

Il y a plusieurs notations permettant de bien définir une application, nous utiliserons souvent celle-ci :

$$\begin{array}{rccc} f : & B & \longrightarrow & C \\ & b & \longmapsto & \ldots \end{array}$$

Et bien sûr, cette notation signifie :
f est une application d'ensemble de départ B, d'ensemble d'arrivée C, qui est définie par la règle de correspondance : $f(b) = ...$

Par exemple, on définit la parabole sur le plan cartésien par :

$$\begin{array}{rccc} f: & \mathbb{R} & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & x^2 \end{array}$$

Note 3 : Dans le cadre de ce cours, pour démontrer qu'une relation définie par règle de correspondance est une application, il sera suffisant de dire que cette règle de correspondance est bien définie (c'est à dire que cette règle associe bien à chaque élément de l'ensemble de départ **un** et **un seul** élément de l'ensemble d'arrivée.)

Le théorème suivant fait grandement ressortir la relation de dualité qu'il y a entre la totalité et la surjectivité et entre le déterminisme et l'injectivité. Cependant pour bien comprendre ce qui ce passe ici, il est important de bien comprendre la signification de chacune des phrases qui composent cette démonstration et non seulement de s'assurer formellement que c'est bien une démonstration correcte.

Rappelons que la *relation inverse* d'une relation $\rho \subseteq B \times C$ est notée ρ^{-1} et est définie comme suit :

$$\rho^{-1} \equiv \{\langle c, b\rangle \mid \langle b, c\rangle \in \rho\}$$

Théorème C.2 *Soient B et C, deux ensembles, et $\rho \subseteq B \times C$. Alors*

$$\begin{cases} 1.- & \rho \textit{ est total} \equiv \rho^{-1} \textit{ est surjectif ;} \\ 2.- & \rho \textit{ est déterministe} \equiv \rho^{-1} \textit{ est injectif ;} \\ 3.- & \rho \textit{ est injectif} \equiv \rho^{-1} \textit{ est déterministe ;} \\ 4.- & \rho \textit{ est surjectif} \equiv \rho^{-1} \textit{ est total.} \end{cases}$$

Démonstration Soit $\rho \subseteq B \times C$.

1.- ρ est total $\equiv \rho^{-1}$ est surjectif.

ρ est total.
=$\langle$ définition de la totalité de ρ. $\rangle$
$(\forall b : B| : (\exists c : C| : b\rho c))$.
=$\langle$ définition de ρ^{-1}. $\rangle$
$(\forall b : B| : (\exists c : C| : c\rho^{-1} b))$.
=$\langle$ définition de la surjectivité de ρ^{-1}. $\rangle$
ρ^{-1} est surjectif.

2.- ρ **est déterministe** $\equiv \rho^{-1}$ **est injectif.**

ρ est déterministe.
=$\langle$ définition du déterminisme de ρ. $\rangle$
$(\forall b : B, c, c' : C | b\rho c \wedge b\rho c' : c = c')$.
=$\langle$ définition de ρ^{-1}. $\rangle$
$(\forall b : B, c, c' : C | c\rho^{-1} b \wedge c'\rho^{-1} b : c = c')$.
=
$(\forall c, c' : C, b : B | c\rho^{-1} b \wedge c'\rho^{-1} b : c = c')$
=$\langle$ définition de l'injectivité de ρ^{-1}. $\rangle$
ρ^{-1} est injectif.

3.- ρ **est injectif** $\equiv \rho^{-1}$ **est déterministe.**

ρ est injectif.
=$\langle$ définition de l'injectivité de ρ. $\rangle$
$(\forall b, b' : B, c : C | b\rho c \wedge b'\rho c : b = b')$
=$\langle$ définition de ρ^{-1}. $\rangle$
$(\forall b, b' : B, c : C | c\rho^{-1} b \wedge c\rho^{-1} b' : b = b')$.
=
$(\forall c : C, b, b' : B | c\rho^{-1} b \wedge c\rho^{-1} b' : b = b')$
=$\langle$ définition du déterminisme de ρ^{-1}. $\rangle$
ρ^{-1} est déterministe.

4.- ρ **est surjectif** $\equiv \rho^{-1}$ **est total.**

ρ est surjectif.
=$\langle$ définition de la surjectivité de ρ. $\rangle$
$(\forall c : C | : (\exists b : B | : b\rho c))$.
=$\langle$ définition de ρ^{-1}. $\rangle$
$(\forall c : C | : (\exists b : B | : c\rho^{-1} b))$.
=$\langle$ définition de la totalité de ρ^{-1}. $\rangle$
ρ^{-1} est total.

C.Q.F.D.

Lorsqu'une relation est une application, la notation définie à la Note 1 permet de réécrire les définitions d'injectivité et de surjectivité :

Définitions 1 : *Étant donnée une application* $f : B \longrightarrow C$*, alors*

$$f \textit{ est injective } \equiv (\forall b, b' : B |\ f(b) = f(b') : b = b')$$

ce qui est équivalent à :

$$f \textit{ est injective } \equiv (\forall b, b' : B |\ b \neq b' : f(b) \neq f(b'))$$

et, ce qui est équivalent à :

$$f \textit{ est injective } \equiv (\forall b, b' : B, c : C |\ bfc \wedge b'fc : b = b')$$

Notez que si f n'est pas une application, seule la 3$^{\text{e}}$ définition d'injectivité reste valide, mais malheureusement nécessite l'utilisation d'une troisième variable (la variable c). Les deux premières définitions sont donc plus simples.

Définitions 2 : *Étant donnée une application* $f : B \longrightarrow C$*, alors*

$$f \textit{ est surjective } \equiv (\forall c : C| : (\exists b : B| : f(b) = c))$$

ce qui est équivalent à :

$$f \text{ est surjective } \equiv (\forall c : C| : (\exists b : B| : bfc))$$

Notez qu'ici aussi, si f n'est pas une application, seule la 2$^{\text{e}}$ définition de surjectivité reste valide.

EXERCICE : Expliquez brièvement pourquoi les définitions 1 et 2 sont respectivement équivalentes aux définitions (d) et (b) de la page précédente.

EXEMPLES de démonstrations de type "classique" appliqués à la théorie des relations :
(*Ici, les différentes propriétés reliées à l'arithmétique sont supposées connues et n'ont pas à être démontrées.*)

Étant données les deux relations suivantes :

a) $\tau \subseteq \mathbb{Z} \times \mathbb{Z}$, définie par : $\tau = \{i, j | j = 1/i : \langle i, j \rangle\}$

b) $k : \mathbb{Z} \longrightarrow \mathbb{Z}$, définie par la règle de correspondance : $h.x = 2x$

Pour chacune d'elle, déterminez si oui ou non, il s'agit :

(1) d'une fonction (c.-à-d. : déterministe) ;

(2) d'une application (c.-à-d. : déterministe et totale) ;

(3) d'une application injective (c.-à-d. : déterministe, totale et injective) ;

(4) d'une application surjective (c.-à-d. : déterministe, totale et surjective) ;

SOLUTIONS :

a)(1) (*Intuitivement, τ semble être une relation déterministe.*)
Démontrons donc que $(\forall b, c, c' | b\tau c \wedge b\tau c' : c = c')$
Soient b, c, c' choisis tels que $b\tau c$ et $b\tau c'$ ⟨*et montrons que* $c = c'$. ⟩
Comme $b\tau c$, alors par la définition de τ, on a $c = 1/b$.
Comme $b\tau c'$, alors par la définition de τ, on a $c' = 1/b$.
Donc, par la transitivité de $=$, on a $c = c'$.

τ est donc une relation déterministe.

C.Q.F.D.

a)(2) (*Intuitivement, τ semble ne pas être une relation totale, car la division par zéro n'est pas définie.*)
Nous devons donc démontrer que $\neg(\forall b : \mathbb{Z}| : (\exists c : \mathbb{Z}| : b\tau c))$
Ce qui est équivalent à démontrer $(\exists b : \mathbb{Z}| : \neg(\exists c : \mathbb{Z}| : b\tau c))$. ⟨ *Voir* ***(7.20)****, Axiome, De Morgan* ⟩
Ce qui est équivalent à démontrer $(\exists b : \mathbb{Z}| : (\forall c : \mathbb{Z}| : \neg(b\tau c)))$. ⟨ *Voir* ***(7.21)(b)****, De Morgan* ⟩
Démontrons donc que $(\exists b : \mathbb{Z}| : (\forall c : \mathbb{Z}| : \neg(b\tau c)))$.
Soit $b := 0$. ⟨ *Un tel* b *existe car clairement* $0 : \mathbb{Z}$. ⟩
Soit $c : \mathbb{Z}$
Alors, comme $1/0$ n'est pas de type $\mathbb{Z}$ ⟨ *propriété de l'arithmétique* ⟩, on ne peut pas avoir $c = 1/0$
Donc par la définition de τ, on ne peut avoir $b\tau c$,
On a donc $\neg(b\tau c)$.

τ n'est donc pas une relation totale, et par conséquent n'est pas une application.

C.Q.F.D.

a)(3)et(4) ont tous deux des réponses négatives puisque τ n'est pas une application.

C.Q.F.D.

b)(1)et(2) k est nécessairement une application (à moins d'une erreur faite par le professeur dans l'énoncé) puisque c'est ce que signifie la notation $k : \mathbb{Z} \longrightarrow \mathbb{Z}$.

k est donc une relation déterministe et totale.

C.Q.F.D.

b)(3) (*Intuitivement, k semble être une relation injective.*)

Comme k est une application nous allons démontrer : $(\forall x, x' : \mathbb{Z} | k(x) = k(x') : x = x')$.

Soient $x, x : \mathbb{Z}$ choisis tels que $k(x) = k(x')$.

Alors on a $2x = 2x'$. ⟨ *Définition de k.* ⟩

Alors on a $\frac{2x}{2} = \frac{2x'}{2}$. ⟨ *Propriété de l'arithmétique.* ⟩

Alors on a $x = x'$. ⟨ *Propriété de l'arithmétique.* ⟩

k est bien une application injective.

C.Q.F.D.

b)(4) (*Intuitivement, k semble ne pas être une relation surjective, les nombres impairs ne semblant pas faire partie de l'image de k.*)

Comme k est une application nous devons donc démontrer : $\neg(\forall y : \mathbb{Z} | : (\exists x : \mathbb{Z} | : k(x) = y))$

Ce qui est équivalent à démontrer $(\exists y : \mathbb{Z} | : \neg(\exists x : \mathbb{Z} | : k(x) = y))$. ⟨ *Voir **(7.20)**, Axiome, De Morgan* ⟩

Ce qui est équivalent à démontrer $(\exists y : \mathbb{Z} | : (\forall x : \mathbb{Z} | : k(x) \neq y))$. ⟨ *Voir **(7.21)(b)**, De Morgan* ⟩

Démontrons donc $(\exists y : \mathbb{Z} | : (\forall x : \mathbb{Z} | : k(x) \neq y))$.

Soit $y := 3$. ⟨ *Un tel y existe car clairement $3 : \mathbb{Z}$.* ⟩

Soit $x : \mathbb{Z}$

Alors clairement, $k(x) = 2x \neq 3$, car 3 n'est pas un nombre pair. ⟨ *Définition de la parité – propriété de l'arithmétique.* ⟩

k n'est pas une application surjective.

C.Q.F.D.

Remarque C.3 *Il est à noter que de démontrer la négation d'une propriété (telle la propriété de surjectivité) revient à trouver un contre-exemple.*

Pour finir ce fascicule, voici quatre démonstrations de type classique, (un peu plus abstraites que les précédentes) et qui nous seront utiles au prochain chapitre.

Lemme C.4 *Soient $\rho \subseteq A \times B$ et $\sigma \subseteq B \times C$, deux relations déterministes.*
Alors $\rho \circ \sigma$ est une relation déterministe sur $A \times C$.

Démonstration

En supposant	:	$(\star)$	$(\forall a : A,\, b, b' : B \mid a\rho b \wedge a\rho b' : b = b')$
et	:	$(\star\star)$	$(\forall b : B,\, c, c' : C \mid b\sigma c \wedge b\sigma c' : c = c')$
Nous allons démontrer	:		$(\forall a : A,\, c, c' : C \mid a\rho \circ \sigma c \wedge a\rho \circ \sigma c' : c = c')$

Soient $a : A$, $c : C$, $c' : C$ choisis tels que $a\rho \circ \sigma c$ et $a\rho \circ \sigma c'$ $\quad \langle$*et montrons que* $c = c'$. $\rangle$

Soit $b : B$ choisi tel que $a\rho b \wedge b\sigma c$ $\quad \langle$ Comme $a\rho \circ \sigma c$, par la définition de $\circ$, un tel b existe.$\rangle$

Soit $b' : B$ choisi tel que $a\rho b' \wedge b'\sigma c'$ $\quad \langle$ Comme $a\rho \circ \sigma c'$, par la définition de $\circ$, un tel b' existe, *cependant il est a priori possible que b' soit différent de b.*$\rangle$

Comme on a $a\rho b$ et $a\rho b'$, on a donc $b = b'$. $\quad \langle$ Voir $(\star)$.$\rangle$
Ce dernier fait, combiné avec $b'\sigma c'$, nous donne $b\sigma c'$.
Ainsi, on a à la fois $b\sigma c$ et $b\sigma c'$.
On a donc $c = c'$ $\quad \langle$ Voir $(\star\star)$.$\rangle$

$\rho \circ \sigma$ est donc une relation déterministe.

C.Q.F.D.

Lemme C.5 *Soient $\rho \subseteq A \times B$ et $\sigma \subseteq B \times C$, deux relations injectives.*
Alors $\rho \circ \sigma$ est une relation injective sur $A \times C$.

Démonstration

En supposant	:	$(\diamondsuit)$	$(\forall a, a' : A,\, b : B \mid a\rho b \wedge a'\rho b : a = a')$
et	:	$(\diamondsuit\diamondsuit)$	$(\forall b, b' : B,\, c : C \mid b\sigma c \wedge b'\sigma c : b = b')$
Nous allons démontrer	:		$(\forall a, a' : A,\, c : C \mid a\rho \circ \sigma c \wedge a'\rho \circ \sigma c : a = a')$

Soient $a : A$, $a' : A$, $c : C$ choisis tels que $a\rho \circ \sigma c$ et $a'\rho \circ \sigma c$ $\quad \langle$*et montrons que* $a = a'$. $\rangle$

Soit $b : B$ choisi tel que $a\rho b \wedge b\sigma c$ $\quad \langle$ Comme $a\rho \circ \sigma c$, par la définition de $\circ$, un tel b existe.$\rangle$

Soit $b' : B$ choisi tel que $a'\rho b' \wedge b'\sigma c$ $\quad \langle$ Comme $a'\rho \circ \sigma c$, par la définition de $\circ$, un tel b' existe, *cependant il est a priori possible que b' soit différent de b.*$\rangle$

Comme on a $b\sigma c$ et $b'\sigma c$, on a donc $b = b'$. $\quad \langle$ Voir $(\diamondsuit\diamondsuit)$.$\rangle$
Ce dernier fait, combiné avec $a'\rho b'$, nous donne $a'\rho b$.
Ainsi, on a à la fois $a\rho b$ et $a'\rho b$.
On a donc $a = a'$ $\quad \langle$ Voir $(\diamondsuit)$.$\rangle$
$\rho \circ \sigma$ est donc une relation injective.

C.Q.F.D.

Lemme C.6 *Soient $\rho \subseteq A \times B$ et $\sigma \subseteq B \times C$, deux relations totales.*
Alors $\rho \circ \sigma$ est une relation totale sur $A \times C$.

Démonstration

En supposant	:	$(\heartsuit)$	$(\forall a : A \mid: (\exists b : B \mid: a \rho b))$
et	:	$(\heartsuit\heartsuit)$	$(\forall b : B \mid: (\exists c : C \mid: b \sigma c))$
Nous allons démontrer	:		$(\forall a : A \mid: (\exists c : C \mid: a \, \rho \circ \sigma \, c))$

Soient $a : A$ ⟨*et montrons que* $(\exists c : C \mid: a \, \rho \circ \sigma \, c)$. ⟩
Soit $b : B$ choisi tel que $a \rho b$ ⟨ par $\heartsuit$: un tel b appartenant à B existe bien.⟩
Soit $c : C$ choisi tel que $b \sigma c$ ⟨ par $\heartsuit\heartsuit$: un tel c appartenant à C existe bien.⟩

Alors on a bien que $a \, \rho \circ \sigma \, c$ ⟨ Par la définition de $\circ$, car $a \rho b$ et $b \sigma c$. ⟩
$\rho \circ \sigma$ est donc une relation totale.

C.Q.F.D.

Lemme C.7 *Soient $\rho \subseteq A \times B$ et $\sigma \subseteq B \times C$, deux relations surjectives.*
Alors $\rho \circ \sigma$ est une relation surjective sur $A \times C$.

Démonstration

En supposant	:	$(\spadesuit)$	$(\forall b : B \mid: (\exists a : A \mid: a \rho b))$
et	:	$(\spadesuit\spadesuit)$	$(\forall c : C \mid: (\exists b : B \mid: b \sigma c))$
Nous allons démontrer	:		$(\forall c : C \mid: (\exists a : A \mid: a \, \rho \circ \sigma \, c))$

Soit $c : C$ ⟨*et montrons que* $(\exists a : A \mid: a \, \rho \circ \sigma \, c)$. ⟩
Soit $b : B$ choisi tel que $b \sigma c$ ⟨ par $\spadesuit\spadesuit$: un tel b appartenant à B existe bien.⟩
Soit $a : A$ choisi tel que $a \rho b$ ⟨ par $\spadesuit$: un tel a appartenant à A existe bien.⟩

Alors on a bien que $a \, \rho \circ \sigma \, c$ ⟨ Par la définition de $\circ$, car $a \rho b$ et $b \sigma c$. ⟩
$\rho \circ \sigma$ est donc une relation surjective.

C.Q.F.D.