Notes complémentaires sur la théorie des relations

et
exemples de démonstrations de type "classique"

1 Introduction

Les démonstrations que nous avons étudiées

jusqu'à maintenant sont de type "formel"...

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

1. Que faire si l’énoncé qu’on souhaite démontrer contient un quantificateur universel $\forall$?
2. Que faire si l’énoncé qu’on souhaite démontrer contient un quantificateur existentiel $\exists$?

2.1 Une démonstration avec un $\forall$

(7.23) Métathéorème :

P est un théorème ssi $(\forall x| : P)$ est un théorème.

(7.3) Axiome, transfert :

$$(\forall x|R : P) \equiv (\forall x| : R \Rightarrow P)$$

Intuition

On veut montrer : $(\forall x : X \mid Q(x) : P(x))$.

Soit $x : X$, choisit tel que $Q(x)$ est vrai.

Alors pour telle raison blablabla.

Ce qui implique ceci et cela.

Et on peut finalement en conclure que $P(x)$ est vrai.

C.Q.F.D.

2.2 Une démonstration avec un $\exists$

(7.26) Transfert : $(\exists x | R : P) \equiv (\exists x | : R \wedge P)$

Intuition

On veut montrer : $(\exists x : X \mid Q(x) : P(x))$.

Soit $x : X$, un élément qui satisfait Q.

$\langle$ Un tel x existe car blablabla.$\rangle$

Alors pour telle raison blablabla.

Ce qui implique ceci et cela.

Ce qui nous permet de conclure que $P(x)$ est vrai.

C.Q.F.D.

2.3 Une démonstration en général

Une démonstration de type “classique” est bien entendu quelque chose de bien plus complexe...

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

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.

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

(7.24) Axiome, De Morgan :

$$(\exists x | R : P) \equiv \neg(\forall x | R : \neg P)$$

(7.25)(a) De Morgan :

$$(\forall x | R : P) \equiv \neg(\exists x | R : \neg P)$$

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

Nous devons donc démontrer que

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

Ce qui est équivalent à démontrer $\langle$(7.25)(b)$\rangle$

$$(\forall m : \mathbb{N} \mid : \neg(\forall n : \mathbb{N} \mid : n < m))$$

Ce qui est équivalent à démontrer $\langle$(7.25)(c)$\rangle$

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

Démontrons donc que

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

Soit $m : \mathbb{N}$. Soit $n := m + 1$,

$\langle$ Un tel n existe et **est bien** un nombre de $\mathbb{N}$ — Propriétés de l'arithmé-

tique. $\rangle$

Alors on a que $n = m + 1 \geq m$.

$\langle$ — Propriété de l'arithmétique. $\rangle$

Ce qui implique que $\neg(n < m)$.

$\langle$ — Propriété de l'arithmétique. $\rangle$

C.Q.F.D.

2.5 Une démonstration avec un $\Leftrightarrow$ ($\equiv$)

(3.97) Implication mutuelle :

$$(p \equiv q) \equiv (p \Rightarrow q) \wedge (q \Rightarrow p)$$

(3.97) Implication mutuelle :

$$(p \Leftrightarrow q) \equiv (p \Rightarrow q) \wedge (q \Rightarrow p)$$

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 $a(\rho \circ \rho)c$. $\langle$ Définition de $\circ$. $\rangle$
Donc, on a $a\rho^2 c$. $\langle$ Définition de ρ^2. $\rangle$
C'est-à-dire $\langle a, c\rangle \in \rho^2$.
Donc, on a $\langle a, c\rangle \in \rho$. $\langle$ Car par hypothèse, on a $\rho^2 \subseteq \rho$. $\rangle$
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 $\rho^2 \subseteq \rho$,
équivalent à $(\forall a, c \mid \langle a, c\rangle \in \rho^2 : \langle a, c\rangle \in \rho)$.

Soient a et c, choisis tels que $\langle a, c\rangle \in \rho^2$.
Alors on a $\langle a, c\rangle \in \rho \circ \rho$. $\langle$ Définition de ρ^2. $\rangle$

Soit b, choisi tel que $a\rho b$ et $b\rho c$.

$\langle$ Un tel b existe car $\langle a, c\rangle \in \rho \circ \rho$, voir définition de $\circ$. $\rangle$

Alors on a $a\rho c$.

$\langle$ Car par hypothèse : $(\forall a, b, c \mid a\rho b \wedge b\rho c : a\rho c)$. $\rangle$

Et donc, on a $\langle a, c\rangle \in \rho$).

(⇐: est démontré.)

C.Q.F.D.

RAPPEL :

- On dira qu'une relation $\rho \subseteq B \times C$ est

$$\begin{cases} (a) \ \textit{totale} \quad \text{si} \ (\forall b : B \mid : \ (\exists c : C \mid : \ b\rho c\,)) \\ (b) \ \textit{surjective} \quad \text{si} \ (\forall c : C \mid : \ (\exists b : B \mid : \ b\rho c\,)) \\ (c) \ \textit{déterministe} \quad \text{si} \\ \qquad (\forall \ b : B, \ c, c' : C \mid : \ b\rho c \wedge b\rho c' \ : \ c = c'\,) \\ (d) \ \textit{injective} \quad \text{si} \\ \qquad (\forall \ b, b' : B, \ c : C \mid : \ b\rho c \wedge b'\rho c \ : \ b = b'\,) \end{cases}$$

- Une relation est appelée une application si elle est à la fois totale et déterministe.
  Autrement dit, ne 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 il la relation f est une application.

NOTATION À DONNER

Note1 : lorsqu'une relation f est une application, l'expression $\langle x, y\rangle \in f$ pourra être remplacé 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'arrivé.

Note2 : 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'arrivé de f.

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

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

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

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

Note3 : 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'arrivé.)

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

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

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 la 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 Note1 permet de réécrire les définitions d'injectivité et de surjectivité :

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

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

ce qui est équivalent à :

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

et, ce qui est équivalent à :

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

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

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

ce qui est équivalent à :

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