Écran privé 1

Programme de baccalauréat en informatique

Mathématiques pour informaticien

MAT-22257

Le cours va débuter à

15h30

Les mathématiques c'est aussi merveilleux que la musique sauf qu'il n'existe pas d'instrument pour en jouer !

UNIVERSITÉ LAVAL
Département d'informatique et de génie logiciel

Écran 1 - Diapositive1.jpg

Programme de baccalauréat en informatique
Conception et analyse d'algorithmes
IFT-17588 Z3

Bonjour à tous

UNIVERSITÉ LAVAL
Département d'informatique
et de génie logiciel

Écran 1 - Diapositive2.jpg

UNIVERSITÉ LAVAL

PLAN DE COURS **Été 2008**

Faculté des sciences et de génie
Département d'informatique et de génie logiciel

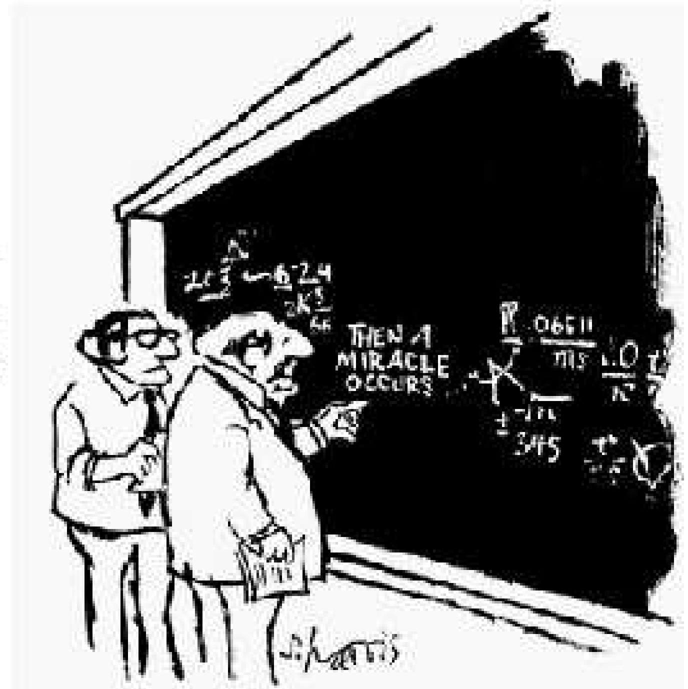
MAT–22257 Z3 – Mathématiques pour informaticiens

Informations générales

Crédits : 2
Temps consacré : 2–1–0–3
Formule pédagogique : LR
Préalable(s) : IFT–10540 ou MAT–10364
Concomitant(s) : *aucun*
Site Web : http://cours.ift.ulaval.ca/2008e/22257/
Intranet Pixel : https://pixel.fsg.ulaval.ca
Enseignant(s) : De Carufel, Jean–Lou jean–lou.decarufel@ift.ulaval.ca
Responsable : Laviolette, Francois francois.laviolette@ift.ulaval.ca

Description sommaire

Ensembles, relations, graphes. Combinatoire, sommations et dénombrement de base. Séries génératrices et résolution de récurrences. Rappels sur les limites, suites, séries et l'infini.



"I think you should be more explicit here in step two."

Écran public Public Screen

Horaire et disponibilités

Plages normales :

Lundi 15h30 à 17h00

Jeudi 14h30 à 16h00

Dépannages :

Vendredi 10h30 à 12h00

Examen	Date	Heure	Pondération de la note finale	Document(s) autorisé(s)
Examen intra	Samedi 7 juin 2008	13h30 à 16h30	35.00%	Aucun
Examen final	Samedi 12 juillet 2008	13h30 à 16h30	40.00%	Aucun

Travail	Équipes	Date	Heure	Pondération de la note finale
Devoir 1	1 à 3	Vendredi 6 juin 2008	23h55	15.00%
Devoir 2	1 à 3	Vendredi 4 juillet 2008	23h55	10.00%

Échelle des cotes

Échelle des cotes			
A+ [92.00 – 100]	A [86.00 – 91.99]	A– [80.00 – 85.99]	**Réussite**
B+ [77.00 – 79.99]	B [74.00 – 76.99]	B– [71.00 – 73.99]	**Réussite**
C+ [69.00 – 70.99]	C [67.00 – 68.99]	C– [65.00 – 66.99]	**Réussite**
D+ [62.00 – 64.99]	D [60.00 – 61.99]		**Réussite**
E [0.00 – 59.99]			Échec
X			**Abandon sans échec (dans les délais prévus)**

Documents utiles: voir site web du cours

Écran public Public Screen

MAT-22257
Mathématiques pour informaticiens
ÉTÉ-2008
Feuille de route

Semaine 1

Théorie des ensembles (1)

Module : 1 et début de Module :2

Objectifs spécifiques

Au terme de cette semaine, vous serez en mesure :

- de définir formellement des ensembles;
- d'effectuer des opérations de base sur un ensemble;
- d'exposer les principaux axiomes de la théorie des ensembles finis.
- de démontrer les principaux théorèmes de la théorie des ensembles finis.

Activités d'apprentissage :

Lectures : Bref rappel du cours Logique et techniques de preuve	
Lectures : Notes de cours de Jules Desharnais	Chapitre 11
[illegible]	Série 1, au complet

Rappel:

⟨⟨***Bref rappel du cours de Logique et techniques de preuve***⟩⟩

Page 4 Les préséances des opérateurs.
Pages 5 et 6 La substitution textuelle.
Page 9 La règle de Leibniz.
Pages 13 à 16 Syntaxe des expressions booléennes.
Page 27 Les règles de Leibniz, de transitivité et de substitution.
Page 46 Problèmes #1, 3, 7 et 13.
Page 52 Règle du Modus Ponens.
Page 61 et 62 Les types.
Pages 75 à 83 Les quantificateurs $\forall$ et $\exists$.

notes de cours de Jules Desharnais. Les références données ici sont reliées à la version Automne 2006 de ces notes de cours, version qui est disponible sur la page web de Mat-22257.

IMPORTANT --- pour le premier chapitre du cours, la théorie des ensembles finis :
Toutes les solutions ainsi que les tables et formules données aux examens sont basés sur la version A06 des notes de cours de Jules Desharnais.

TAB. 1.1 – **Préséance (priorité) des opérateurs**

(1) $[x := e]$ (substitution textuelle) (priorité élevée)

(2) $.$ (application de fonction)

(3) $+ \quad - \quad \neg \quad \mathcal{P}$ (opérateurs unaires préfixes)

(4) $\cdot \quad / \quad \div \quad \mathrm{mod} \quad \mathrm{pgcd} \quad \times \quad \circ \quad \bullet$

(5) $+ \quad - \quad \cup \quad \cap$ (opérateurs binaires)

(6) $\downarrow \quad \uparrow$

(7) $= \quad < \quad > \quad \in \quad \subset \quad \subseteq \quad \supset \quad \supseteq \quad | \quad \neq \quad \not< \quad \not> \quad \notin \quad \not\subset \quad \not\subseteq \quad \not\supset \quad \not\supseteq \quad \nmid$ (conjonctifs, voir page 16)

(8) $\vee \quad \wedge$

(9) $\Rightarrow \quad \Leftarrow \quad \not\Rightarrow \quad \not\Leftarrow$

(10) $\equiv \quad \not\equiv$ (priorité faible)

Les opérateurs binaires non associatifs sont associatifs à gauche, sauf $\Rightarrow$, qui est associatif à droite. Si $\square$ est un opérateur binaire et que $a \square b$ est une expression booléenne, alors la notation $a \not\square b$ est une abréviation pour l'expression $\neg(a \square b)$. L'opérateur $\not\square$ a la même préséance que $\square$. On voit des exemples de tels opérateurs aux lignes (7, 9, 10). Vous pouvez utiliser cette abréviation en tout temps et il n'est pas nécessaire de donner un numéro de loi pour la justifier *si un tel numéro de loi n'existe pas.*

À cause des conventions de préséance,

$$2 \cdot 3 + 8 = (2 \cdot 3) + 8.$$

Écran public Public Screen

1.2 Substitution textuelle

(1.2) Notation. *Substitution textuelle.*

Soient E et R des expressions, et x une variable.

$$E[x := R]$$

dénote l'expression E avec *TOUTES* les occurrences libres de x remplacées par (R).

Expression	Résultat	Suppression des parenthèses inutiles
$x[x := t+5]$	$(t+5)$	$t+5$
$(y+x)[y := t+5]$	$((t+5)+x)$	$t+5+x$
$(x \cdot y)[x := t+5]$	$((t+5) \cdot y)$	$(t+5) \cdot y$
$(y+y)[y := 5]$	$((5)+(5))$	$5+5$
$(y+10)[x := 5]$	$(y+10)$	$y+10$

Présentation que nous adopterons :

$$
\begin{aligned}
& (x+2)[x := t+2] \\
= & \quad \langle \text{ Substitution } \rangle \\
& ((t+2)+2) \\
= & \quad \langle \text{ Suppression des parenthèses inutiles } \rangle \\
& t+2+2
\end{aligned}
$$

Lois de l'égalité

Soient x, y des variables et X, Y des expressions.

(1.10) Réflexivité : $x = x$

(1.11) Symétrie (commutativité) : $(x = y) = (y = x)$

(1.12) Transitivité : $\dfrac{X = Y, \quad Y = Z}{X = Z}$

Loi énoncée par Leibniz (il y a 350 ans) :

Deux expressions sont égales si et seulement si le remplacement de l'une par l'autre dans n'importe quelle expression E ne change pas la valeur de E.

Conséquence de cette loi :

(1.13) Leibniz : $\dfrac{X = Y}{E[z := X] = E[z := Y]}$

Exemple : la règle de Leibniz avec

$$X : b+3 \qquad Y : c+5 \qquad E : d+z \qquad z : z$$

donne

$$\frac{b+3 \;=\; c+5}{(d+z)[z := b+3] \;=\; (d+z)[z := c+5]}$$

c'est-à-dire

$$\frac{b+3 \;=\; c+5}{d+b+3 \;=\; d+c+5}$$

PAS à $\Rightarrow$

IMPORTANT: la règle de Leibniz ne s'appliqu'à $=$ **! ! !**

Écran public Public Screen

2.1 Syntaxe des expressions booléennes

Une *expression booléenne* est construite à partir des constantes vrai et faux, de variables booléennes, qui peuvent prendre les valeurs vrai et faux (seulement) et des opérateurs booléens. Les opérateurs booléens les plus couramment utilisés sont :

$\equiv, =, \Leftrightarrow$	égalité, équivalence
$\not\equiv, \neq$	inégalité, inéquivalence
$\neg$	négation, non
$\vee$	disjonction, ou
$\wedge$	conjonction, et
$\Rightarrow$	implication, si ...alors
$\Leftarrow$	conséquence

Définition des opérateurs booléens

Voici les tables de tous les opérateurs unaires et binaires. Dans ces tables, v et f signifient respectivement vrai et faux.

		id	$\neg$	
v	v	v	f	f
f	v	f	v	f

								$\equiv$			$\not\equiv$						
			$\vee$	$\Leftarrow$		$\Rightarrow$		$=$	$\wedge$	$\bar\wedge$	$\neq$					$\bar\vee$	
v	v	v	v	v	v	v	v	v	v	f	f	f	f	f	f	f	f
v	f	v	v	v	v	f	f	f	f	v	v	v	v	f	f	f	f
f	v	v	v	f	f	v	v	f	f	v	v	f	f	v	v	f	f
f	f	v	f	v	f	v	f	v	f	v	f	v	f	v	f	v	f

où $\bar\wedge$: nand et $\bar\vee$: nor

Les tables de vérité sont utilisées pour évaluer les expressions booléennes.

Évaluation de $\neg p \wedge (q \Rightarrow r)$

p	q	r	$\neg p$	$q \Rightarrow r$	$\neg p \wedge (q \Rightarrow r)$
v	v	v	f	v	f
v	v	f	f	f	f
v	f	v	f	v	f
v	f	f	f	v	f
f	v	v	v	v	v
f	v	f	v	f	f
f	f	v	v	v	v
f	f	f	v	v	v

Les colonnes p, q, r définissent l'état. Tous les états possibles sont énumérés. Les autres colonnes traitent les sous-expressions de l'expression donnée. Pour l'état

$$(p, \mathsf{vrai}),\ (q, \mathsf{vrai}),\ (r, \mathsf{faux}),$$

l'expression est fausse : $\big(\neg p \wedge (q \Rightarrow r)\big)[p, q, r := \mathsf{vrai}, \mathsf{vrai}, \mathsf{faux}] \ = \ \mathsf{faux}$

(2.1) Exercice. Donnez la table de vérité de l'expression

$$\big((p \equiv q) \equiv r\big) \ \equiv \ \big(p \equiv (q \equiv r)\big)\ .$$

Écran public Public Screen

2. (a) $p = q$ se prononce « *p égale q* ».

   (b) $p \equiv q$ se prononce « *p est équivalent à q* ». ou *p si et seulement si q*

   (c) Dans $p \Rightarrow q$ et $q \Leftarrow p$, p s'appelle *l'antécédent* et q le *conséquent*.

3. $(p \vee q) \equiv \mathsf{vrai}$ si

$$\begin{array}{ll} & p \equiv \mathsf{vrai} \\ \text{ou} & q \equiv \mathsf{vrai} \\ \text{ou} & p \equiv \mathsf{vrai} \text{ et } q \equiv \mathsf{vrai}\ . \end{array}$$

Par conséquent,

$$\textit{j'ai une auto rouge} \ \vee \ \textit{j'étudie l'informatique}$$

est vrai si j'ai une auto rouge, ou si j'étudie l'informatique, ou si j'ai une auto rouge et que j'étudie l'informatique. On dit que l'opérateur $\vee$ est le *ou inclusif*.

Pour exprimer le *ou exclusif*, on utilise l'inégalité (ou l'inéquivalence), car elle est vraie quand exactement l'un de ses opérandes est vrai. Ainsi

$$\textit{j'ai une auto rouge} \ \not\equiv \ \textit{j'étudie l'informatique}$$

exprime que j'ai une auto rouge ou que j'étudie l'informatique, mais pas les deux.

4. $(p \Rightarrow q) \equiv \mathsf{faux}$ seulement lorsque $p \equiv \mathsf{vrai}$ et $q \equiv \mathsf{faux}$.

Intuitivement, l'expression

$$x > 2 \Rightarrow x > 0 \quad \textit{est vraie.}$$

Écran public Public Screen

2.3 Égalité versus équivalence

(2.2) Notation. Supposons que $\circ$ et $\star$ sont des opérateurs dits *conjonctifs* (ligne (j) de la table de préséance des opérateurs). Ceci signifie que

$$a \circ b \star c \quad \text{est une abréviation de} \quad a \circ b \ \wedge \ b \star c\,.$$

Par exemple,

$$a < b = c \quad \text{est une abréviation de} \quad a < b \ \wedge \ b = c\,,$$
$$a = b = c \quad \text{est une abréviation de} \quad a = b \ \wedge \ b = c\,.$$

En ce qui concerne l'omission des parenthèses, l'égalité $(=)$ est considérée comme un opérateur conjonctif même si elle est associative. Les expressions

$$a = b = c \qquad \text{et} \qquad a \equiv b \equiv c$$

peuvent donner des résultats différents.

$$\boxed{(\mathsf{faux} = \mathsf{faux} = \mathsf{vrai}) \quad \neq \quad (\mathsf{faux} \equiv \mathsf{faux} \equiv \mathsf{vrai})}$$

$$\begin{array}{ll}
 & \mathsf{faux} = \mathsf{faux} = \mathsf{vrai} \\
= & \qquad \langle = \text{est conjonctive} \rangle \\
 & (\mathsf{faux} = \mathsf{faux}) \wedge (\mathsf{faux} = \mathsf{vrai}) \\
= & \qquad \langle \text{Évaluation des} = \rangle \\
 & \mathsf{vrai} \wedge \mathsf{faux} \\
= & \qquad \langle \text{Évaluation de} \wedge \rangle \\
 & \mathsf{faux}
\end{array}$$

$$\begin{array}{ll}
 & \mathsf{faux} \equiv \mathsf{faux} \equiv \mathsf{vrai} \\
= & \qquad \langle \text{Évaluation de} \equiv \text{gauche} \rangle \\
 & \mathsf{vrai} \equiv \mathsf{vrai} \\
= & \qquad \langle \text{Évaluation de} \equiv \rangle \\
 & \mathsf{vrai}
\end{array}$$

Écran public Public Screen

La logique équationnelle E (calcul des propositions)

1. Un ensemble d'axiomes (par exemple, $p \vee q \equiv q \vee p$).
2. Trois règles d'inférence
   - **Leibniz :** $\dfrac{P = Q}{E[r := P] = E[r := Q]}$
   - **Transitivité :** $\dfrac{P = Q, \quad Q = R}{P = R}$
   - **Substitution :** $\dfrac{P}{P[r := Q]}$

Conventions :
- $P, Q, R, \ldots$ sont des expressions booléennes.
- $p, q, r, \ldots$ sont des variables booléennes.

Remarquez que les trois règles d'inférence ci-dessus sont simplement (1.13), (1.12) et (1.9), réécrites avec cette convention.

Écran public Public Screen

Règle du modus ponens

Supposons que P et $P \Rightarrow Q$ soient des théorèmes. Nous pouvons alors montrer que Q est un théorème :

$$
\begin{array}{ll}
 & P \Rightarrow Q \qquad \text{—C'est un théorème par hypothèse} \\
= & \langle\ \mathsf{vrai}\ \text{est un théorème (3.6)}\ \ \& \\
 & \quad P\ \text{est un théorème par hypothèse}\ \ \& \\
 & \quad \text{Deux théorèmes quelconques sont équivalents (Métathéorème (3.100))}\ \rangle \\
 & \mathsf{vrai} \Rightarrow Q \\
= & \langle\ (3.89),\ \text{avec}\ p := Q\ \rangle \\
 & Q
\end{array}
$$

Nous pouvons exprimer ce résultat sous la forme d'une règle :

Règle du modus ponens : $\dfrac{P, \quad P \Rightarrow Q}{Q}$

Cette règle est très utile, mais comme les autres règles introduites jusqu'ici, on omet souvent de la mentionner lorsqu'on l'utilise.

Écran public Public Screen

6.1 Types

Un type est un ensemble de valeurs. Voici les types de base :

TAB. 6.1 – Quelques types élémentaires

nom	symbole	type (ensemble de valeurs)
entiers (relatifs)	$\mathbb{Z}$	$\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots$
naturels	$\mathbb{N}$	$0, 1, 2, 3, \ldots$
entiers positifs	$\mathbb{Z}^+, \mathbb{N}^+$	$1, 2, 3, 4, \ldots$
entiers négatifs	$\mathbb{Z}^-$	$-1, -2, -3, -4, \ldots$
rationnels	$\mathbb{Q}$	i/j, où i, j entiers, $j \neq 0$
réels	$\mathbb{R}$	tous les nombres réels
réels positifs	$\mathbb{R}^+$	tous les nombres réels positifs
booléens	$\mathbb{B}$	vrai, faux

E:t versus $E \in t$

Pour n'importe quelle expression E et n'importe quel type t,

$$E \in t$$

est une expression.

Écran public Public Screen

7.1 Quantification existentielle

La disjonction $\vee$ est
- associative
- commutative
- a faux comme élément neutre.

On peut donc l'utiliser comme quantificateur : $(\vee x \mid R : P)$. Nous écrirons :

$$(\exists x \mid R : P).$$

Transfert pour quantification existentielle

(7.1) Axiome, transfert : $\underline{(\exists x \mid R : P) \;\equiv\; (\exists x \mid : R \wedge P)}$ 

(7.6) Pourvu que $\neg$libre('x','P'),

$$(\exists x \mid R : P) \;\equiv\; P \wedge (\exists x \mid : R)$$

Écran public Public Screen

7.2 Quantification universelle

La conjonction $\wedge$ est
- associative
- commutative
- a **vrai** comme élément neutre.

On peut donc l'utiliser comme quantificateur : $(\wedge x \mid R : P)$. Nous écrirons :

$$(\forall x \mid R : P).$$

Généralisation des lois de De Morgan

(7.15) Axiome, De Morgan : $\boxed{(\forall x \mid R : P) \equiv \neg(\exists x \mid R : \neg P)}$

Cette loi est une généralisation de $p \wedge q \equiv \neg(\neg p \vee \neg q)$.

(7.16) De Morgan :
(a) $(\exists x \mid R : P) \equiv \neg(\forall x \mid R : \neg P)$
(b) $(\forall x \mid R : \neg P) \equiv \neg(\exists x \mid R : P)$
(c) $(\exists x \mid R : \neg P) \equiv \neg(\forall x \mid R : P)$

Théorèmes de transfert pour $\forall$

(7.17) Transfert :
(a) $(\forall x \mid R : P) \equiv (\forall x \mid : R \Rightarrow P)$
(b) $(\forall x \mid R : P) \equiv (\forall x \mid : \neg R \vee P)$
(c) $(\forall x \mid R : P) \equiv (\forall x \mid : R \wedge P \equiv R)$
(d) $(\forall x \mid R : P) \equiv (\forall x \mid : R \vee P \equiv P)$

Métathéorème sur la quantification universelle

Écran public Public Screen

(7.33) Métathéorème : P est un théorème ssi $(\forall x \mid : P)$ est un théorème.

Monotonie du quantificateur universel

(7.34) Monotonie de $\forall$:

$$(\forall x \mid R : Q \Rightarrow P) \;\Rightarrow\; \big((\forall x \mid R : Q) \Rightarrow (\forall x \mid R : P)\big)$$

Monotonie du quantificateur existentiel

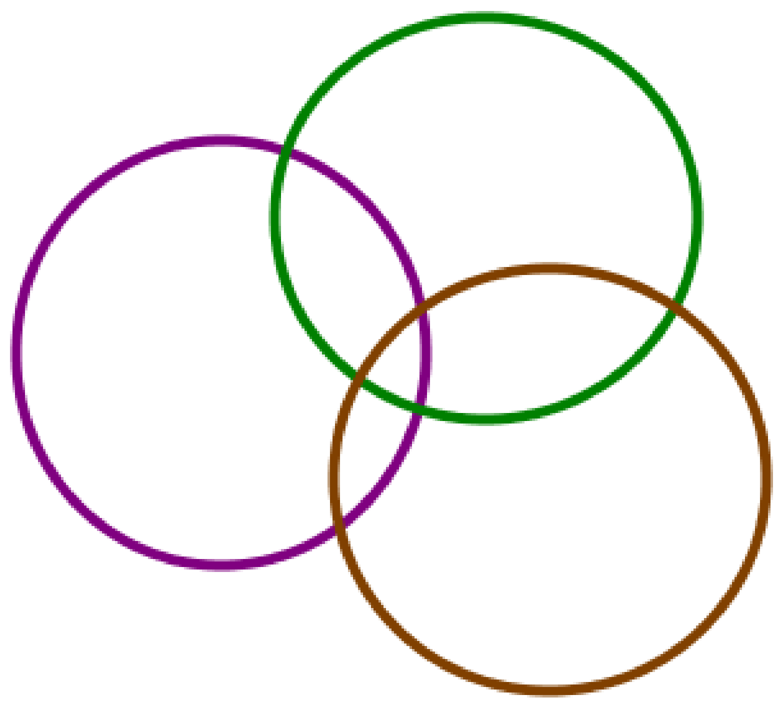
(7.36) Monotonie de $\exists$:

$$(\forall x \mid R : Q \Rightarrow P) \;\Rightarrow\; \big((\exists x \mid R : Q) \Rightarrow (\exists x \mid R : P)\big)$$

Écran public Public Screen

Chapitre 11

Théorie des ensembles



Un *ensemble* est une collection de valeurs. On peut définir un ensemble par *énumération* (on dit aussi en *extension*) et par *compréhension*.

Énumération

Une manière de définir un *ensemble* est d'*énumérer* (lister) ses *éléments* entre accolades { } :

$$\{8, 4, -3.5, 10\}$$

est l'ensemble qui contient les éléments 8, 4, -3.5 et 10.

Soit l'état

$$(a, 5),\ (b, 13),\ (c, 8).$$

L'évaluation de l'expression

$$\{b, c\}$$

dans cet état donne l'ensemble

$$\{13, 8\}.$$

Compréhension

Lorsque le nombre de ses éléments est trop grand pour les énumérer, on définit un ensemble par *compréhension*, c'est-à-dire en utilisant des expressions qui décrivent les *propriétés* de ses éléments :

$$\{n{:}\mathbb{Z} \mid 0 \leq n \leq 8 : 2^n\}$$

est l'ensemble qui *contient* les valeurs de la forme 2^n, où $0 \leq n \leq 8$, c'est-à-dire

$$\{2^0, 2^1, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8\}\ ,$$

ou encore, en développant,

$$\{1, 2, 4, 8, 16, 32, 64, 128, 256\}\ .$$

Une énumération peut être vue comme une abréviation d'une compréhension :

$$\{5, 12, 7\} \quad = \quad \{x \mid x = 5 \vee x = 12 \vee x = 7 : x\}$$

ou en général,

(11.1) $\{e_0, \ldots, e_{n-1}\} \quad = \quad \{x \mid x = e_0 \vee \ldots \vee x = e_{n-1} : x\}\ .$

Forme générale d'une expression de compréhension

La forme générale ressemble à une quantification :

(11.2) $\{x{:}t \mid R : E\}$

les deux formes sont acceptées

x est une liste de variables de quantification, R est l'expression booléenne décrivant le domaine et E est l'expression du corps. Si $E{:}t_1$, alors

$$\{x{:}t \mid R : E\}{:}\mathsf{ensemble}(t_1) \ .$$

La forme traditionnelle de la compréhension

La notation mathématique traditionnelle pour la compréhension est

$$\{x \mid R\} \ ,$$

Appartenance et égalité

Soit une expression e de type t et soit une expression S de type $\mathsf{ensemble}(t)$. L'expression

$$e \in S$$

se prononce

e *appartient à* S

ou encore e *est un élément de* S .

Elle a la valeur vrai si e est un élément de S et la valeur faux sinon.

(11.4) Exemple.

$$10 \in \{5, 10, 2, 3\} \equiv \mathsf{vrai}$$
$$8 \in \{5, 10, 2, 3\} \equiv \mathsf{faux}$$
$$(\neg(10 \in \{5, 10, 2, 3\})) = (10 \notin \{5, 10, 2, 3\}) = \mathsf{faux}$$

Extensionnalité

(11.7) Notation. Pour le reste du chapitre,

$$S, T, U, V : \mathsf{ensemble}(t) ,$$

c'est-à-dire que les symboles S, T, U, V sont des variables de type $\mathsf{ensemble}(t)$, où le type t dépend des circonstances.

(11.8) Axiome, extensionnalité : $S = T \;\equiv\; (\forall x \mid : x \in S \equiv x \in T)$

Autrement dit, deux ensembles sont égaux si, et seulement si, ils ont les mêmes éléments.

Quelques remarques

1. L'ensemble $\{\{\}\}$ (qui est égal à $\{\emptyset\}$) n'est pas vide. Il contient un élément, soit l'ensemble $\{\}$ (ou encore $\emptyset$).
2. L'expression $e \in \{e\}$ a la valeur vrai.
3. Par l'abréviation (11.1), et puisque $\vee$ est idempotent et commutatif,
   (a) les répétitions d'éléments ne comptent pas. Par exemple,
   $$\{2,3,2\} = \{2,3\} ;$$
   (b) l'ordre d'énumération des éléments n'est pas important. Par exemple,
   $$\{1,2,3\} = \{3,2,1\} = \{1,3,2\} .$$
4. Les ensembles peuvent être éléments d'autres ensembles. Par exemple,
   $$\{\{1,2\}, \emptyset, \{2,3,4\}\}$$
   contient les éléments $\{1,2\}$, $\emptyset$ et $\{2,3,4\}$.
5. Un ensemble peut contenir des éléments de types différents : $\{2, \mathsf{vrai}\}$.

Ensembles versus prédicats

Écran public Public Screen

(11.10) $x \in \{x \mid R\} \equiv R$

Du théorème (11.13), on tire le théorème suivant qui exprime le fait que deux ensembles définis par des prédicats caractéristiques différents sont égaux si et seulement si les deux prédicats sont équivalents :

(11.16) $\{x \mid Q\} = \{x \mid R\} \;\equiv\; (\forall x \,|\!: Q \equiv R)$

Par exemple, $\{n \mid n^2 \geq 10\} = \{n \mid n^2 > 9\}$, car $(\forall n \,|\!: n^2 \geq 10 \equiv n^2 > 9)$.

(11.17) Métathéorème : $\{x \mid Q\} = \{x \mid R\}$ est un théorème si et seulement si $(\forall x \,|\!: Q \equiv R)$ est un théorème.

Avec le métathéorème (11.17), nous avons trois méthodes pour démontrer l'égalité d'ensembles.

(11.18) Méthodes de démonstration de l'égalité d'ensembles $S = T$:

(a) Par la règle de Leibniz.

(b) Par l'axiome d'extensionnalité (**11**.8), il suffit de prouver

$$v \in S \;\equiv\; v \in T$$

pour un v arbitraire.

(c) Par (11.17), il suffit de montrer $Q \equiv R$ pour conclure

$$\{x \mid Q\} \;=\; \{x \mid R\}\ .$$

Écran public Public Screen

Cardinalité des ensembles finis

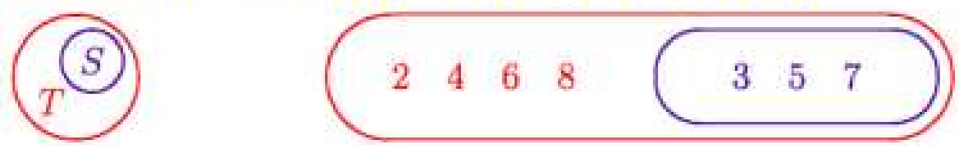
La *cardinalité* ou la *taille* d'un ensemble fini S, dénotée par $\#S$, est le nombre d'éléments de S. Elle est définie ainsi :

(11.19) Axiome, cardinalité : $\#S = (\sum x \mid x \in S : 1)$

La notation $|S|$ pour la cardinalité de S est aussi très fréquemment employée dans la littérature.

Sous-ensemble et surensemble

Diagrammes de Venn de $S \subseteq T$ et $\{3,5,7\} \subseteq \{2,3,4,5,6,7,8\}$



(11.21) Axiome, sous-ensemble : $S \subseteq T \;\equiv\; (\forall x \mid x \in S : x \in T)$

Si $S \subseteq T$, on dit que S *est un sous-ensemble de* T, ou que S *est inclus dans* T, ou que T *contient* S. Le symbole $\subseteq$ s'appelle l'*inclusion*5 .

(11.22) Axiome, sous-ensemble propre : $S \subset T \;\equiv\; S \subseteq T \wedge S \neq T$

Si $S \subset T$, on dit que S *est un sous-ensemble propre de* T, ou que S *est strictement inclus dans* T, ou que T *contient strictement* S. Le symbole $\subset$ s'appelle l'*inclusion stricte*.

Écran public Public Screen

Ensemble universel U

L'ensemble qui contient tous les éléments dont on veut parler dans un contexte donné s'appelle *l'ensemble universel* ; on le dénote par **U**. Par exemple, dans un contexte où tous les ensembles contiennent des entiers, on a

$$\mathbf{U} = \mathsf{ensemble}(\mathbb{Z}) \; .$$

Complément

Supposons l'ensemble universel **U** donné. Le *complément* d'un ensemble S, noté $\sim S$, est l'ensemble des éléments qui appartiennent à **U** mais pas à S.

(11.25) Axiome, complément : $v \in \sim S \;\equiv\; v \in \mathbf{U} \wedge v \notin S$

Par exemple, si $\mathbf{U} = \mathbb{Z}$, alors $\sim\{n \mid \mathsf{pair}.n\} = \{n \mid \mathsf{impair}.n\}$.

(11.26) $v \in \sim S \;\equiv\; v \notin S \qquad$ (où $v \in \mathbf{U}$)

(11.27) $\sim\sim S = S$

Remarquons que les notations S^C et $\overline{S}$ sont aussi utilisées pour dénoter le complément de S.

Union, intersection et différence

(11.28) Axiome, union : $v \in S \cup T \;\equiv\; v \in S \vee v \in T$

(11.29) Axiome, intersection : $v \in S \cap T \;\equiv\; v \in S \wedge v \in T$

(11.30) Axiome, différence : $v \in S - T \;\equiv\; v \in S \wedge v \notin T$

(11.31) Exemple.

$$\begin{aligned} \{0,1,2\} \cup \{2,3,4\} &= \{0,1,2,3,4\} \\ \{0,1,2\} \cap \{2,3,4\} &= \{2\} \\ \{0,1,2\} - \{2,3,4\} &= \{0,1\} \end{aligned}$$

Des axiomes (11.25) et (11.30), on tire

$$\sim S = \mathbf{U} - S \; .$$

Les ensembles S et T sont dits *disjoints* s'ils n'ont pas d'éléments en commun, c'est-à-dire si

Écran public Public Screen

Par exemple, $\{0,1,2\}$ et $\{5,8\}$ sont disjoints, mais pas $\{2,5,8\}$ et $\{2,8,15\}$.

Ensemble puissance

L'*ensemble puissance* d'un ensemble S, noté $\mathcal{P}S$, est l'ensemble des sous-ensembles de S.

(11.32) Axiome, ensemble puissance : $v \in \mathcal{P}S \;\equiv\; v \subseteq S$

(11.33) Exemple.

$$\mathcal{P}\{1,2,3\} = \{\ \emptyset,\ \{1\},\ \{2\},\ \{3\},\ \{1,2\},\ \{1,3\},\ \{2,3\},\ \{1,2,3\}\ \}$$

$$(\{1,3\} \in \mathcal{P}\{1,2,3\}) = (\{1,3\} \subseteq \{1,2,3\}) = \text{vrai}$$

$$(\{1,4\} \in \mathcal{P}\{1,2,3\}) = (\{1,4\} \subseteq \{1,2,3\}) = \text{faux}$$

Écran public Public Screen

Propriétés de $\cup$

(11.34) **Commutativité de $\cup$:** $S \cup T = T \cup S$

(11.35) **Associativité de $\cup$:** $(S \cup T) \cup U = S \cup (T \cup U)$

(11.36) **Idempotence de $\cup$:** $S \cup S = S$

(11.37) **Zéro de $\cup$:** $S \cup \mathbf{U} = \mathbf{U}$

(11.38) **Identité (élément neutre) de $\cup$:** $S \cup \emptyset = S$

(11.39) **Affaiblissement :** $S \subseteq S \cup T$

(11.40) **Tiers exclu :** $S \cup \sim S = \mathbf{U}$

Propriétés de $\cap$

(11.41) **Commutativité de $\cap$:** $S \cap T = T \cap S$

(11.42) **Associativité de $\cap$:** $(S \cap T) \cap U = S \cap (T \cap U)$

(11.43) **Idempotence de $\cap$:** $S \cap S = S$

(11.44) **Zéro de $\cap$:** $S \cap \emptyset = \emptyset$

(11.45) **Identité (élément neutre) de $\cap$:** $S \cap \mathbf{U} = S$

(11.46) **Affaiblissement :** $S \cap T \subseteq S$

(11.47) **Contradiction :** $S \cap \sim S = \emptyset$

Combinaison de $\cup$ et $\cap$

(11.48) **Distributivité de $\cup$ sur $\cap$:** $S \cup (T \cap U) = (S \cup T) \cap (S \cup U)$

(11.49) **Distributivité de $\cap$ sur $\cup$:** $S \cap (T \cup U) = (S \cap T) \cup (S \cap U)$

(11.50) **De Morgan :** (a) $\sim(S \cup T) = \sim S \cap \sim T$
(b) $\sim(S \cap T) = \sim S \cup \sim T$

Monotonie de $\cup$ et $\cap$

(11.51) **Monotonie de $\cup$:** $S \subseteq T \wedge U \subseteq V \Rightarrow S \cup U \subseteq T \cup V$

(11.52) **Monotonie de $\cap$:** $S \subseteq T \wedge U \subseteq V \Rightarrow S \cap U \subseteq T \cap V$

table fml ENSEMBLES

Propriétés de $-$

(11.57) $S - T = S \cap \sim T$

(11.58) $S - T \subseteq S$

(11.59) $S - \emptyset = S$

(11.60) $S \cap (T - S) = \emptyset$

(11.61) $S \cup (T - S) = S \cup T$

(11.62) $S - (T \cup U) = (S - T) \cap (S - U)$

(11.63) $S - (T \cap U) = (S - T) \cup (S - U)$

Implication versus inclusion

(11.64) $(\forall x \mid : P \Rightarrow Q) \equiv \{x \mid P\} \subseteq \{x \mid Q\}$

Propriétés de $\subseteq$

(11.65) **Antisymétrie :** $S \subseteq T \wedge T \subseteq S \equiv S = T$

(11.66) **Réflexivité :** $S \subseteq S$

(11.67) **Transitivité :** $S \subseteq T \wedge T \subseteq U \Rightarrow S \subseteq U$

(11.68) $\emptyset \subseteq S$

(11.69) $S \subset T \equiv S \subseteq T \wedge \neg(T \subseteq S)$

(11.70) $S \subset T \equiv S \subseteq T \wedge (\exists x \mid x \in T : x \notin S)$

(11.71) $S \subseteq T \equiv S \subset T \vee S = T$

(11.72) $S \not\subset S$

(11.73) $S \subset T \Rightarrow S \subseteq T$

(11.74) $S \subset T \Rightarrow T \not\subseteq S$

(11.75) $S \subseteq T \Rightarrow T \not\subset S$

(11.76) $S \subseteq T \wedge \neg(U \subseteq T) \Rightarrow \neg(U \subseteq S)$

(11.77) $(\exists x \mid x \in S : x \notin T) \Rightarrow S \neq T$

(11.78) **Transitivité :** (a) $S \subseteq T \wedge T \subset U \Rightarrow S \subset U$
(b) $S \subset T \wedge T \subseteq U \Rightarrow S \subset U$
(c) $S \subset T \wedge T \subset U \Rightarrow S \subset U$

table de fmls

(1.17) Leibniz : $\dfrac{X = Y}{g.X = g.Y}$

(3.2) Axiome, associativité de $\equiv$: $((p \equiv q) \equiv r) \equiv (p \equiv (q \equiv r))$

(3.3) Axiome, commutativité (symétrie) de $\equiv$: $p \equiv q \equiv q \equiv p$

(3.4) Axiome, identité (élément neutre) de $\equiv$: $vrai \equiv p \equiv p$

(3.6) Théorème : vrai

(3.7) Théorème, réflexivité de $\equiv$: $p \equiv p$

(3.11) Axiome, définition de faux : $faux \equiv \neg vrai$

(3.12) Axiome, distributivité de $\neg$ sur $\equiv$: $\neg(p \equiv q) \equiv \neg p \equiv q$

(3.13) Axiome, définition de $\not\equiv$: $(p \not\equiv q) \equiv \neg(p \equiv q)$

(3.14) $\neg p \equiv q \equiv p \equiv \neg q$

(3.15) Double négation : $\neg\neg p \equiv p$

(3.16) Négation de faux : $\neg faux \equiv vrai$

(3.17) $(p \not\equiv q) \equiv \neg p \equiv q$

(3.18) $\neg p \equiv p \equiv faux$

(3.19) Commutativité (symétrie) de $\not\equiv$: $(p \not\equiv q) \equiv (q \not\equiv p)$

(3.20) Associativité de $\not\equiv$: $((p \not\equiv q) \not\equiv r) \equiv (p \not\equiv (q \not\equiv r))$

(3.21) Associativité mutuelle : $((p \not\equiv q) \equiv r) \equiv (p \not\equiv (q \equiv r))$

(3.22) Interchangeabilité mutuelle : $p \not\equiv q \equiv r \equiv p \equiv q \not\equiv r$

(3.32) Axiome, commutativité (symétrie) de $\vee$: $p \vee q \equiv q \vee p$

(3.33) Axiome, associativité de $\vee$: $(p \vee q) \vee r \equiv p \vee (q \vee r)$

(3.34) Axiome, idempotence de $\vee$: $p \vee p \equiv p$

(3.36) Axiome, distributivité de $\vee$ sur $\equiv$: $p \vee (q \equiv r) \equiv p \vee q \equiv p \vee r$

(3.37) Axiome, tiers exclu : $p \vee \neg p$ ou encore $p \vee \neg p \equiv vrai$

(3.38) Zéro de $\vee$: $p \vee vrai \equiv vrai$

(3.40) Identité de $\vee$: $p \vee faux \equiv p$

(3.41) Distributivité de $\vee$ sur $\vee$: $p \vee (q \vee r) \equiv (p \vee q) \vee (p \vee r)$

(3.42) $p \vee q \equiv p \vee \neg q \equiv p$

(3.47) Axiome, De Morgan : $p \wedge q \equiv \neg(\neg p \vee \neg q)$

(3.48) De Morgan, formes alternatives : (a) $\neg(p \wedge q) \equiv \neg p \vee \neg q$
(b) $\neg(p \vee q) \equiv \neg p \wedge \neg q$
(c) $p \vee q \equiv \neg(\neg p \wedge \neg q)$

(3.49) Commutativité (symétrie) de $\wedge$: $p \wedge q \equiv q \wedge p$

(3.50) Associativité de $\wedge$: $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$

(3.51) Idempotence de $\wedge$: $p \wedge p \equiv p$

(3.52) Identité de $\wedge$: $p \wedge vrai \equiv p$

(3.53) Zéro de $\wedge$: $p \wedge faux \equiv faux$

(3.54) Distributivité de $\wedge$ sur $\wedge$: $p \wedge (q \wedge r) \equiv (p \wedge q) \wedge (p \wedge r)$

(3.55) Contradiction : $p \wedge \neg p \equiv faux$

(3.57) Règle d'or : $p \wedge q \equiv p \equiv q \equiv p \vee q$

(3.59) Distributivité de $\vee$ sur $\wedge$: $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$

(3.60) Distributivité de $\wedge$ sur $\vee$: $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$

(3.61) Absorption : (a) $p \wedge (p \vee q) \equiv p$
(b) $p \vee (p \wedge q) \equiv p$
(c) $p \wedge (\neg p \vee q) \equiv p \wedge q$
(d) $p \vee (\neg p \wedge q) \equiv p \vee q$

(3.62) $p \wedge q \equiv p \wedge \neg q \equiv \neg p$

(3.63) $p \wedge (q \equiv r) \equiv p \wedge q \equiv p \wedge r \equiv p$

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

(3.65) Remplacement : $(p \equiv q) \wedge (r \equiv p) \equiv (p \equiv q) \wedge (r \equiv q)$

(3.66) Définition de $\equiv$: $p \equiv q \equiv (p \wedge q) \vee (\neg p \wedge \neg q)$

(3.67) Ou exclusif : $p \not\equiv q \equiv (\neg p \wedge q) \vee (p \wedge \neg q)$

(3.71) $(p \wedge q) \wedge r \equiv p \equiv q \equiv r \equiv p \vee q \equiv q \vee r \equiv r \vee p \equiv p \vee q \vee r$

(3.73) Axiome, définition de $\Rightarrow$: $p \Rightarrow q \equiv p \vee q \equiv q$

(3.74) Axiome, conséquence : $p \Leftarrow q \equiv q \Rightarrow p$

(3.75) Définition alternative de $\Rightarrow$: $p \Rightarrow q \equiv \neg p \vee q$

(3.76) Définition alternative de $\Rightarrow$: $p \Rightarrow q \equiv p \wedge q \equiv p$

(3.77) Contrapositivité : $p \Rightarrow q \equiv \neg q \Rightarrow \neg p$

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

(3.79) Distributivité de $\Rightarrow$ sur $\equiv$: $p \Rightarrow (q \equiv r) \equiv p \Rightarrow q \equiv p \Rightarrow r$

(3.80) $p \Rightarrow (q \Rightarrow r) \equiv (p \Rightarrow q) \Rightarrow (p \Rightarrow r)$

(3.81) Transfert : $p \wedge q \Rightarrow r \equiv p \Rightarrow (q \Rightarrow r)$

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

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

(3.84) $p \vee (p \Rightarrow q) \equiv vrai$

(3.85) $p \vee (q \Rightarrow p) \equiv q \Rightarrow p$

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

(3.87) Réflexivité de $\Rightarrow$: $p \Rightarrow p \equiv vrai$ ou encore $p \Rightarrow p$

(3.88) Zéro à droite de $\Rightarrow$: $p \Rightarrow vrai \equiv vrai$ ou encore $p \Rightarrow vrai$

(3.89) Identité à gauche de $\Rightarrow$: $vrai \Rightarrow p \equiv p$

(3.90) $p \Rightarrow faux \equiv \neg p$

(3.91) $faux \Rightarrow p \equiv vrai$ ou encore $faux \Rightarrow p$

(3.92) Affaiblissement, renforcement : (a) $p \Rightarrow p \vee q$
(b) $p \wedge q \Rightarrow p$
(c) $p \wedge q \Rightarrow p \vee q$
(d) $p \vee (q \wedge r) \Rightarrow p \vee q$
(e) $p \wedge q \Rightarrow p \wedge (q \vee r)$

(3.93) Modus ponens : $p \wedge (p \Rightarrow q) \Rightarrow q$

(3.94) $(p \Rightarrow r) \wedge (q \Rightarrow r) \equiv (p \vee q \Rightarrow r)$

(3.95) $(p \Rightarrow r) \wedge (\neg p \Rightarrow r) \equiv r$

(3.97) Implication mutuelle : $(p \Rightarrow q) \wedge (q \Rightarrow p) \equiv p \equiv q$

(3.98) Antisymétrie : $(p \Rightarrow q) \wedge (q \Rightarrow p) \Rightarrow (p \equiv q)$

(3.99) Transitivité : (a) $(p \Rightarrow q) \wedge (q \Rightarrow r) \Rightarrow (p \Rightarrow r)$
(b) $(p \equiv q) \wedge (q \Rightarrow r) \Rightarrow (p \Rightarrow r)$
(c) $(p \Rightarrow q) \wedge (q \equiv r) \Rightarrow (p \Rightarrow r)$

(3.100) Métathéorème : Deux théorèmes quelconques sont équivalents.

(4.1) $p \Rightarrow (q \Rightarrow p)$

(4.2) Monotonie de $\vee$: $(p \Rightarrow q) \Rightarrow (p \vee r \Rightarrow q \vee r)$

(4.3) Monotonie de $\wedge$: $(p \Rightarrow q) \Rightarrow (p \wedge r \Rightarrow q \wedge r)$

(7.2) Axiome, transfert : $(\forall x \mid R : P) \equiv (\forall x \mid : R \Rightarrow P)$

(7.4) Transfert : (a) $(\forall x \mid R : P) \equiv (\forall x \mid : \neg R \vee P)$
(b) $(\forall x \mid R : P) \equiv (\forall x \mid : R \wedge P \equiv R)$
(c) $(\forall x \mid R : P) \equiv (\forall x \mid : R \vee P \equiv P)$

(7.6) Transfert : (a) $(\forall x \mid Q \wedge R : P) \equiv (\forall x \mid Q : R \Rightarrow P)$
(b) $(\forall x \mid Q \wedge R : P) \equiv (\forall x \mid Q : \neg R \vee P)$
(c) $(\forall x \mid Q \wedge R : P) \equiv (\forall x \mid Q : R \wedge P \equiv R)$
(d) $(\forall x \mid Q \wedge R : P) \equiv (\forall x \mid Q : R \vee P \equiv P)$

Démontrons: **(11.50) De Morgan :** (a) $\sim(S \cup T) = \sim S \cap \sim T$

Démonstration.

EXERCICE 1

Démontrons : **(11.67) Transitivité :** $S \subseteq T \wedge T \subseteq U \;\Rightarrow\; S \subseteq U$

Démonstration.

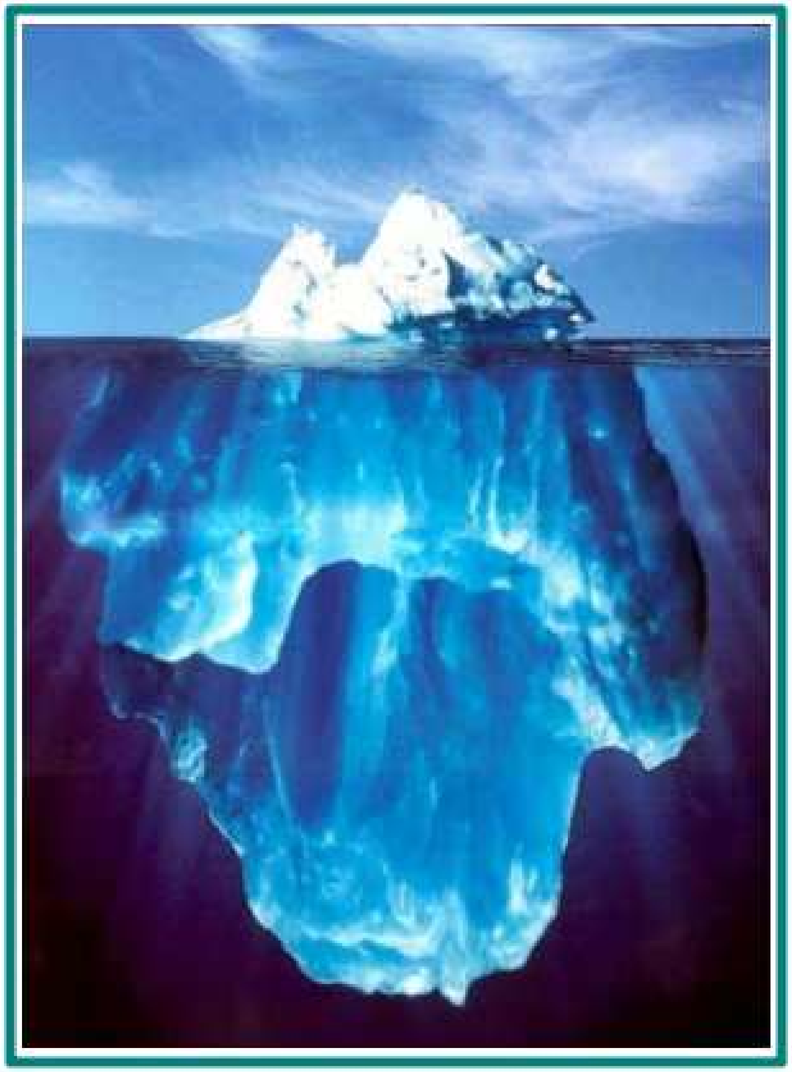
EXERCICE 2

Lemme(♣) : $\left(\forall x \mid : (p \Rightarrow q) \wedge (q \Rightarrow r)\right) \Rightarrow \left(\forall x \mid : p \Rightarrow r\right)$

Démonstration du lemme :

Lemme (de ex2)

Bonne session !



Fin