La logique des logiciens

Aperçu

- toute assertion qui n'est pas intégralement démontrée est potentiellement fausse et n'est, au mieux, qu'une conjecture intéressante,
- utiliser une assertion non complètement démontrée pour en prouver d'autres augmente exponentiellement les risques d'erreur,
- c'est à l'auteur d'une assertion qu'incombe la charge de la démontrer.

D

Une **assertion** est une affirmation grammaticalement correcte dont on peut dire sans ambiguïté si elle est vraie ou fausse. On attribue donc à une assertion une valeur booléenne:

$$\begin{cases} V \text{ ou } 1 & \text{si elle est vraie,} \\ F \text{ ou } 0 & \text{si elle est fausse.} \end{cases}$$

Une assertion vraie est un **énoncé**.

E

1. «Tous les hommes sont mortels.» est une assertion vraie.
2. «Quelle heure est-il ?» n'est pas une assertion.
3. «Le nombre 3 est plus grand que le nombre 2» est une assertion vraie.
4. «235 est un nombre pair» est une assertion fausse.
5. «2+3+5» n'est pas une assertion.

Dans ce chapitre, on soulignera exceptionnellement <u>ou</u>, <u>et</u>.

D On note **non P** la **négation** de l'assertion P, c'est-à-dire l'assertion qui est vraie si P est fausse, et fausse si P est vraie.

P	non P
V	F
F	V

D On note **(P <u>ou</u> Q)** la **disjonction** des assertions P et Q, c'est-à-dire l'assertion qui est vraie si au moins une des assertions P ou Q est vraie. ((P <u>ou</u> Q) est fausse lorsque P est fausse et Q est fausse et seulement dans ce cas).
On note **(P <u>et</u> Q)** la **conjonction** des assertions P et Q, c'est-à-dire l'assertion qui est vraie lorsque P est vraie et Q est vraie et seulement dans ce cas. ((P <u>et</u> Q) est fausse dès que l'une des assertions est fausse).

P	Q	P <u>ou</u> Q	P <u>et</u> Q
F	F	F	F
F	V	V	F
V	F	V	F
V	V	V	V

E

1. $3 < 4$ <u>et</u> $2 < 4$ est vraie.
2. $3 < 4$ <u>et</u> $4 < 2$ est fausse.
3. $3 < 4$ <u>ou</u> $2 < 4$ est vraie.
4. $3 < 4$ <u>ou</u> $4 < 2$ est vraie.

D

Soient $P(A,B,C,\dots)$, $Q(A,B,C,\dots)$ des assertions dont les tables de vérité coïncident. Nous dirons que ces assertions sont **tautologiquement équivalentes**, ou, plus simplement, équivalentes ou encore **synonymes**. Nous écrirons

$$P(A,B,C,\dots) \equiv Q(A,B,C,\dots).$$

Autrement dit, ces énoncés logiques veulent dire rigoureusement la même chose quelles que soient les valeurs logiques de A,B,C,...

T

Loi de De Morgan

Soient P,Q des assertions.

1. $\text{non}(P$ *<u>ou</u>* $Q)$ *est tautologiquement équivalente à* $(\text{non}\,P)$ *<u>et</u>* $(\text{non}\,Q)$*.*
2. $\text{non}(P$ *<u>et</u>* $Q)$ *est tautologiquement équivalente à* $(\text{non}\,P)$ *<u>ou</u>* $(\text{non}\,Q)$*.*

T

Soit x un nombre réel. Donner la négation de $0 < x < 1$.

D L'assertion (non P) <u>ou</u> Q est appelée l'**implication** de Q par P et se note

$$\boldsymbol{P \implies Q}.$$

C'est l'assertion qui est vraie si P est fausse ou si P et Q sont vraies.

P	Q	$P \implies Q$
F	F	V
F	V	V
V	F	F
V	V	V

On exprime la situation «$P \implies Q$ vraie» en disant indifféremment :

- **Si** P **alors** Q.
- Pour que P, il **faut** que Q.
- Q est une **condition nécessaire** de P.
- P **seulement si** Q.
- Pour que Q, il **suffit** que P.
- P est une **condition suffisante** de Q.
- Q **si** P.
- La proposition P **implique** la proposition Q.

R

1. Si P est fausse, alors $P \implies Q$ est vraie.
   - $(1 = 0 \implies$ «Nous sommes dimanche»$)$ est une assertion vraie.
   - $(0 \neq 0 \implies 0 = 0)$ est une assertion vraie.
2. $(P \implies Q)$ vraie ne signifie pas que P ou Q soient vraies.

D Étant données deux relations P et Q, l'**implication contraposée** de $P \implies Q$ est la relation
$$\text{non}\, Q \implies \text{non}\, P.$$

P *Une implication*
$$P \implies Q$$
et sa contraposée
$$\text{non}\, Q \implies \text{non}\, P$$
sont tautologiquement équivalentes.

P

La négation de $(P \implies Q)$ *est*

$$P \ \underline{\textit{et}}\ (\text{non}\, Q).$$

D

On note $P \iff Q$ l'assertion qui est vraie si P et Q ont la même valeur de vérité et qui est fausse sinon.
On exprime la situation «$P \iff Q$ vraie» en disant indifféremment

- P et Q sont **équivalentes**,
- P **si et seulement si** Q,
- P est une **condition nécessaire et suffisante** de Q.

P	Q	$P \iff Q$
F	F	V
F	V	F
V	F	F
V	V	V

R

1. $(P \iff Q)$ est tautologiquement équivalente à $(Q \iff P)$.
2. $(P \iff Q)$ est tautologiquement équivalente à $(\text{non}\, P \iff \text{non}\, Q)$.
3. $(P \iff Q)$ vraie ne signifie pas que P ou Q soit vraie.
4. $(P \iff Q)$ peut-être vraie alors que P et Q n'ont aucun rapport entre elles :

$$0 = 0 \iff \cos \text{ est continue sur } \mathbb{R}.$$

Ici, $(P \iff 0 = 0)$ est une façon d'écrire que P est vraie.

P *Étant données deux relations P et Q, la relation $(P \iff Q)$ est tautologiquement équivalente à la relation*

$$(P \implies Q) \ \underline{\text{et}}\ (Q \implies P).$$

D Étant données deux relations P et Q. L'**implication réciproque** de $P \implies Q$ est la relation

$$Q \implies P.$$

Si l'implication $(P \implies Q)$ est vraie, cela ne donne *aucune* indication sur la véracité de $(Q \implies P)$.

D Soient R une relation et a un objet mathématique, et x une lettre. On appelle **spécialisation de R pour la valeur a de x**, que l'on désigne par $R[x \leftarrow a]$, la relation obtenue en substituant a à x dans R

Pour indiquer qu'une lettre x figure dans une relation R, on écrit fréquemment celle-ci sous la forme $R(x)$ et on écrit alors fréquemment $R(a)$ au lieu de $R[x \leftarrow a]$.

E À tout réel x, nous pouvons associer l'assertion «x est un entier impair», que nous notons $P(x)$; c'est ainsi que $P(-3)$ est une assertion vraie et que $P(\pi)$ est une assertion fausse.

D Soit $P(x)$ une relation à une variable x appartenant à un ensemble A. La proposition «$\boldsymbol{\forall x \in A, P(x)}$» se lit «Pour tout x appartenant à A, $P(x)$». Cette proposition est vraie si la substitution à x dans la proposition par n'importe quel élément a de A fournit une proposition $P(a)$ vraie.

Il s'agit en quelque sorte d'une conjonction généralisée. (Par exemple si $A = \{a, b, c\}$ la proposition «$\forall x \in A, P(x)$» équivaut à «$P(a)$ <u>et</u> $P(b)$ <u>et</u> $P(c)$».)

D La proposition «$\boldsymbol{\exists x \in A, P(x)}$»se lit «Il existe x appartenant à A tel que $P(x)$». Cette proposition est vraie si l'ensemble A contient au moins un élément, disons a, dont la substitution à x dans la proposition fournit une proposition $P(a)$ vraie.

Il s'agit en quelque sorte d'une disjonction généralisée. (Par exemple si $A = \{a, b, c\}$ la proposition «$\exists x \in A, P(x)$»équivaut à «$P(a)$ <u>ou</u> $P(b)$ <u>ou</u> $P(c)$».

E

1. $\forall x \in \mathbb{R}, x^2 + 1 > 0.$
2. $\exists x \in \mathbb{R}, x^2 + 1 > 0.$
3. $\forall x \in \mathbb{R}, x^2 - 1 > 0$ est une assertion fausse.
4. $\exists x \in \mathbb{R}, x^2 - 1 > 0.$
5. Dire qu'une fonction $f : \mathbb{R} \to \mathbb{R}$ s'annule au moins une fois sur $\mathbb{R}$ s'écrit
$$\exists x \in \mathbb{R}, f(x) = 0.$$
6. Tout nombre réel positif ou nul peut s'écrire comme le carré d'un nombre réel s'écrit
$$\forall x \in \mathbb{R}_+, \exists y \in \mathbb{R}, x = y^2.$$
On peut choisir, par exemple $y = \sqrt{x}$. Remarquez que le y recherché dépend (à priori) du x. Nous verrons plus tard que l'on ne peut pas inverser «$\forall x \in \mathbb{R}_+$» et «$\exists y \in \mathbb{R}, x = y^2$».

R

- une variable qui a été quantifiée devient «muette» : son écriture peut être remplacée par n'importe quel symbole (sauf ceux figurant ailleurs dans l'énoncé).
- L'utilisation des quantificateurs suppose que vous utilisiez les quantificateurs sur toute la proposition considérée : pas de mélange !
- L'emploi des quantificateurs en guise d'abréviations est exclus.

E

Énoncer par des phrases correctes les assertions

$$A : \forall x \in \mathbb{R}_+, \exists y \in \mathbb{R}, x = y^2.$$
$$B : \exists y \in \mathbb{R}, \forall x \in \mathbb{R}_+, x = y^2.$$

Ces deux propositions ont-elles le même sens ?

P

Admis

Considérons deux ensembles X et Y et une relation $P(x, y)$ dépendant des variables $x \in X$ et $y \in Y$.

1. *Les assertions suivantes sont tautologiquement équivalentes.*

$$\forall x \in X, \forall y \in Y, P(x, y) \tag{1}$$
$$\forall y \in Y, \forall x \in X, P(x, y) \tag{2}$$
$$\forall (x, y) \in X \times Y, P(x, y) \tag{3}$$

2. *Les assertions suivantes sont tautologiquement équivalentes.*

$$\exists x \in X, \exists y \in Y, P(x, y) \tag{4}$$
$$\exists y \in Y, \exists x \in X, P(x, y) \tag{5}$$
$$\exists (x, y) \in X \times Y, P(x, y) \tag{6}$$

3. *On a l'implication*

$$(\exists x \in X, \forall y \in Y, P(x, y)) \implies (\forall y \in Y, \exists x \in X, P(x, y)) \tag{7}$$

Quand une proposition «$\forall x \in X, \exists y \in Y, P(x, y)$» est vraie, alors la proposition «$\exists y \in Y, \forall x \in X, P(x, y)$ » *peut* être fausse.

E

- Quelle est la négation de «Tous les triangles sont isocèles» ?
- Quelle est la négation de «Tous les élèves de la classe sont des garçons» ?

E

- Quelle est la négation de «Tous les triangles sont isocèles» ?
- Quelle est la négation de «Tous les élèves de la classe sont des garçons» ?

P

- *La négation de* «$\forall x \in A, P(x)$» *est*

$$\exists x \in A, \text{non } P(x).$$

- *La négation de* «$\exists x \in A, P(x)$» *est*

$$\forall x \in A, \text{non } P(x).$$

E

Pour une application $f : \mathbb{R} \to \mathbb{R}$ et $a \in R$, voici la définition de «f est continue au point a».

$$\forall \epsilon \in]0, +\infty[, \exists \delta \in]0, +\infty[, \forall x \in \mathbb{R}, |x - a| \leq \delta \implies |f(x) - f(a)| \leq \epsilon.$$

Sa négation, en l'occurence la non-continuité de f au point a est

$$\exists \epsilon \in]0, +\infty[, \forall \delta \in]0, +\infty[, \exists x \in \mathbb{R}, |x - a| \leq \delta \text{ et } |f(x) - f(a)| > \epsilon.$$

D La proposition «$\boldsymbol{\exists ! x \in A, P(x)}$» se lit «Il existe un unique x appartenant à A tel que $P(x)$». Cette proposition signifie qu'il y a un, et un seul, élément de A pour lequel $P(x)$ est vraie.

E Il est vrai que

$$\exists ! n \in \mathbb{N}, \frac{1}{2} \leq n < \frac{3}{2}.$$

L'entier n en question est tout simplement 1.

L'axiome fondamental est l'**axiome d'extensionalité** pour les ensembles, qui dit qu'un ensemble est totalement caractérisé par ses éléments.

A

Axiome d'extensionalité

$$(\forall x, x \in E \iff x \in F) \implies E = F. \tag{8}$$

Lire : «deux ensembles qui ont les mêmes éléments sont égaux».

A

Axiome de séparation

Soient X un ensemble et $P(x)$ une propriété des éléments de X. Alors il existe un ensemble A vérifiant

$$\forall x, x \in A \iff (P(x) \text{ et } x \in X)$$

On note cet ensemble $\{\, x \in X \mid P(x) \,\}$, ce qui se lit «l'ensemble des x éléments de E tels que $P(x)$».

E

$$\{\, n \in \mathbb{N} \mid n \text{ est pair} \,\}, \qquad \left\{\, x \in \mathbb{Q}_+ \,\middle|\, x^2 > 2 \,\right\}.$$

Un même ensemble peut être défini de plusieurs manières différentes.

$$\left\{\, x \in \mathbb{R} \,\middle|\, x^2 = 2 \,\right\} = \left\{\, -\sqrt{2}, \sqrt{2} \,\right\} = \left\{\, \sqrt{2}, -\sqrt{2} \,\right\} = \left\{\, \epsilon\sqrt{2} \,\middle|\, \epsilon = 1 \text{ \underline{ou} } \epsilon = -1 \,\right\}$$

$$\{\, -1, 1 \,\} = \{\, 1, -1 \,\} = \{\, 1, 1, 1, 1, -1 \,\} = \left\{\, x \in \mathbb{R} \,\middle|\, x^2 = 1 \,\right\}$$

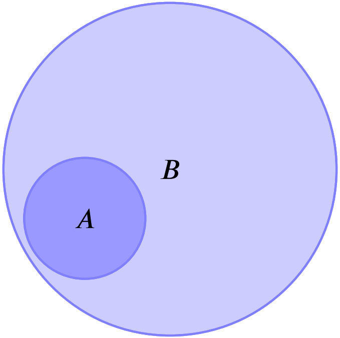
D Soit A et B deux ensembles. On écrit que $A \subset B$ et dit que A est une **partie** de B, ou que A est un **sous-ensemble** de B, ou encore que A est **inclu** dans B pour signifier que tous les éléments de A sont contenus dans B.

$$A \subset B \iff (\forall x, x \in A \implies x \in B)$$

Ou abbréviativement,

$$A \subset B \iff (\forall x \in A, x \in B)\,.$$

$A \subset B$



D Soit A et B deux ensembles. On écrit que $A \subset B$ et dit que A est une **partie** de B, ou que A est un **sous-ensemble** de B, ou encore que A est **inclu** dans B pour signifier que tous les éléments de A sont contenus dans B.

$$A \subset B \iff (\forall x, x \in A \implies x \in B)$$

Ou abbréviativement,

$$A \subset B \iff (\forall x \in A, x \in B)\,.$$

E L'ensemble vide est un sous-ensemble de tout ensemble. Tout ensemble est sous-ensemble de lui même. L'ensemble $\{\, x \in X \mid P(x) \,\}$ est un sous-ensemble de X.

En anticipant un peu sur les définitions ultérieures, on voit que la relation d'inclusion est réflexive, transitive et antisymétrique : l'inclusion est donc une relation d'ordre.

P

1. *L'inclusion est réflexive, c'est-à-dire, quel que soit l'ensemble* A,
$$A \subset A.$$
2. *L'inclusion est transitive, c'est-à-dire, quels que soient les ensembles* A, B *et* C,
$$(A \subset B \ \underline{\text{et}}\ B \subset C) \implies A \subset C.$$
3. *L'inclusion est antisymétrique, c'est-à-dire, quels que soient les ensembles* A, B,
$$(A \subset B \ \text{ et } \ B \subset A) \implies A = B. \qquad \text{(Règle de la double inclusion)}$$

A

Soit E un ensemble. La relation $x \subset E$ est collectivisante et définit l'**ensemble des parties de E**, noté $\mathcal{P}(E)$. On a donc

$$\forall x, (x \in \mathcal{P}(E) \iff x \subset E) .$$

E

- On a toujours $\emptyset \subset E$.
- Si $E = \{ 0, 1 \}$, alors $\mathcal{P}(E) = \left\{ \emptyset, \{ 0 \} , \{ 1 \} , \{ 0, 1 \} \right\}$.
- Si $E = \{ a, b, c \}$, alors

$$\mathcal{P}(E) = \left\{ \emptyset, \{ a \} , \{ b \} , \{ c \} , \{ a, b \} , \{ a, c \} , \{ b, c \} , \{ a, b, c \} \right\} .$$

- $\mathcal{P}(\emptyset) = \{ \emptyset \}$.
- $\mathcal{P}\left(\mathcal{P}(\emptyset)\right) = \left\{ \emptyset, \{ \emptyset \} \right\}$.

A

Soit A et B deux ensembles. Il existe alors un ensemble noté $A \cup B$, appelé **réunion** ou **union** de A et B, tel que

$$\forall x, (x \in A \cup B \iff (x \in A \text{ ou } x \in B)).$$

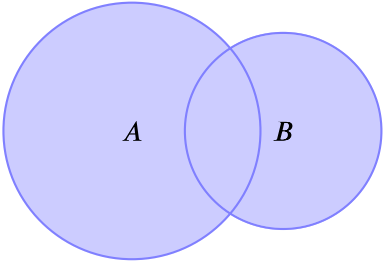
A

Soit A et B deux ensembles. Il existe alors un ensemble noté $A \cap B$, appelé **intersection** de A et B, tel que

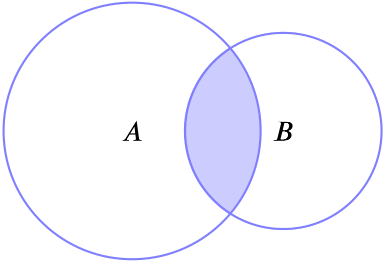
$$\forall x, (x \in A \cap B \iff (x \in A \text{ et } x \in B)).$$

On dit que A et B sont **disjoints** lorsque $A \cap B = \emptyset$.

$A \cup B$



$A \cap B$



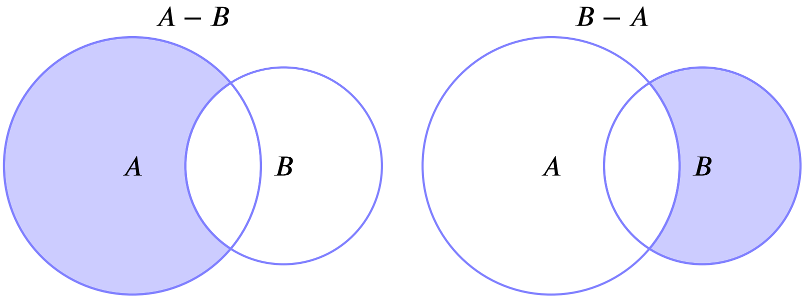
D Soit A et B deux ensembles.

- On appelle **différence** de A et B l'ensemble des éléments de A qui n'appartiennent pas à B. On le note $A \setminus B$, qui se lit «A privé de B» ou «A moins B».

$$\forall x, (x \in A \setminus B \iff (x \in A \text{ et } x \notin B)).$$

Ainsi $A \setminus B = \{ x \mid x \in A \text{ et } x \notin B \}$.

- Si $B \subset A$, on définit le **complémentaire** de B dans A l'ensemble $A \setminus B$. On le note $\complement_A B$.



D Soit A et B deux ensembles.

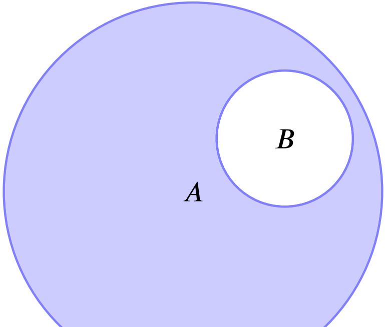
- On appelle **différence** de A et B l'ensemble des éléments de A qui n'appartiennent pas à B. On le note $A \setminus B$, qui se lit «A privé de B» ou «A moins B».

$$\forall x, (x \in A \setminus B \iff (x \in A \text{ et } x \notin B)).$$

Ainsi $A \setminus B = \{ x \mid x \in A \text{ et } x \notin B \}$.

- Si $B \subset A$, on définit le **complémentaire** de B dans A l'ensemble $A \setminus B$. On le note $\complement_A B$.

$$\complement_A B = A - B$$



P

Soit E, A, B trois ensembles. On a alors

1. $E \setminus (E \setminus A) = E \cap A$.
2. $E \setminus (A \cap B) = (E \setminus A) \cup (E \setminus B)$.
3. $E \setminus (A \cup B) = (E \setminus A) \cap (E \setminus B)$.

P

Soit E un ensemble, et A et B deux parties de E. On a alors

1. $\complement_E \left(\complement_E A\right) = A$.
2. $\complement_E (A \cap B) = \left(\complement_E A\right) \cup \left(\complement_E B\right)$.
3. $\complement_E (A \cup B) = \left(\complement_E A\right) \cap \left(\complement_E B\right)$.

Ces deux dernières propriétés sont parfois appelée loi de De Morgan pour les ensembles.

A On suppose que l'on sait former à partir de deux objets a et b un **couple** (a, b) de manière à satisfaire la règle suivante :

$$\forall a, \forall b, \forall c, \forall d, (a, b) = (c, d) \iff (a = c \text{ et } b = d).$$

Les éléments a et b sont respectivement appelés **première** et **seconde composante** (ou encore **coordonnée**) du couple (a, b).

Si $x = (a, b)$, on écrit parfois $a = p_1(x)$ et $b = p_2(x)$.

A

Soit A et B deux ensembles. Le **produit cartésien** de A par B est l'ensemble $A \times B$ des **couples** (x, y) tels que $x \in A$ et $y \in B$. On a

$$A \times B = \{ \, x \mid \exists a \in A \ \text{ et } \ \exists b \in B, x = (a, b) \, \}$$

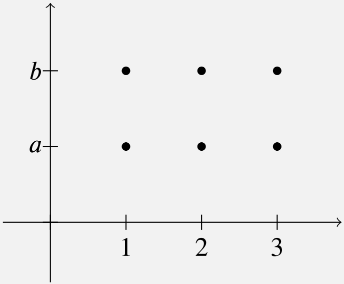
ou de manière équivalente

$$A \times B = \{ \, (a, b) \mid a \in A \ \text{ et } \ b \in B \, \} \, .$$

E L'ensemble $\{ 1, 2, 3 \} \times \{ a, b \}$ est l'ensemble de couples

$$\{ (1, a), (1, b), (2, a), (2, b), (3, a), (3, b) \}$$

Une représentation cartésienne est donnée par



On définit de même des triplets (a, b, c), des quadruplets (a, b, c, d) et plus généralement, à partir de n éléments $a_1, \dots, a_n$, on peut former le ***n*-uplet** $x = (a_1, \dots, a_n)$. On a la règle

$$\forall a_1, \dots, \forall a_n, \forall b_1, \dots, \forall b_n, \big(a_1, \dots, a_n\big) = \big(b_1, \dots, b_n\big) \iff \big(a_1 = b_1 \text{ et } \dots \text{ et } a_n = b_n\big).$$

Les n-uplets $(a_1, \dots, a_n)$ formés d'éléments $a_1 \in A_1, \dots a_n \in A_n$ forment un ensemble, le **produit cartésien** $A_1 \times \cdots \times A_n$.

N Si $A = B$, on note simplement $A^2 = A \times A$. Plus généralement, on définit

$$A^n = \underbrace{A \times \cdots \times A}_{n \text{ fois}} = \left\{ (x_1, \dots, x_n) \,\middle|\, x_1 \in A, \dots, x_n \in A \right\}.$$

E $(1, \sqrt{2}, \pi, -8.23)$ est un élément de $\boldsymbol{R}^4$.

On a sert à affirmer que quelque chose est vrai.

E On a $\sqrt{2} \in \mathbb{R} \setminus \mathbb{Q}$.

Donc, d'où, on en déduit, ainsi, par conséquent,... s'intercale entre une affirmation et sa conséquence.

E La fonction f est impaire donc $f(0) = 0$.

Pour tout... Quel que soit... «Pour tout $x \in A$, on a $P(x)$» signifie que tous les x de A vérifient P. À la fin de la phrase, on ne sait plus ce que désigne x.

E

- Exemple incorrect. Pour tout $x \in \mathbb{R}$, $x^2 \geq 0$. Donc $x^2 + 1 \geq 1$.
- Exemple correct. Pour tout $x \in \mathbb{R}$, $x^2 \geq 0$, donc $x^2 + 1 \geq 1$.

Soit $x \in A$. On se donne x dans l'ensemble E (n'importe quel x). À partir de maintenant, x désigne cet élément. On ne peut plus écrire dans une même démonstration «$\forall x \in A \ \ldots$» ou «$\exists x \in A \ \ldots$».
Pour démontrer un énoncé de la forme

$$\forall x \in A, P(x),$$

le réflexe est une rédaction du type.

- Soit $x \in A$
- ... (Maintenant, vous avez un x fixé entre les mains et vous pouvez commencer à le disséquer et tenter de montrer que x a la propriété P. Si vous y parvenez, c'est terminé)......
- donc $P(x)$ est vraie.
- *Conclusion :* $\forall x \in A, P(x)$.

En effet, travailler avec un $x \in A$ fixé mais quelconque revient à travailler avec tous les éléments de A.

Soit $x \in A$. On se donne x dans l'ensemble E (n'importe quel x). À partir de maintenant, x désigne cet élément. On ne peut plus écrire dans une même démonstration «$\forall x \in A$ ... » ou «$\exists x \in A$ ... ».

E $\forall (a,b) \in \mathbb{R}^2, ab \leq \frac{a^2+b^2}{2}$.

Démonstration. Soit $(a,b) \in \mathbb{R}^2$. Montrons que $ab \leq \frac{a^2+b^2}{2}$.
On sait que $(a-b)^2 \geq 0$, c'est-à-dire, $a^2 - 2ab + b^2 \geq 0$, donc $a^2 + b^2 \geq 2ab$ et enfin

$$ab \leq \frac{a^2+b^2}{2}.$$

Conclusion : $\forall (a,b) \in \mathbb{R}^2, ab \leq \frac{a^2+b^2}{2}$. ∎

On pose $x = ...$ Soit $x = ...$ sert à définir un nouvel objet (nombre, ensemble...) à partir d'objets déjà connus.
Attention à ne pas confondre «Soit $x = \dots$» avec «Soit $x \in \dots$».

E

1. On considère des réels a, b, c. On pose $\Delta = b^2 - 4ac$.
2. On considère des réels a, b, c. Soit $\Delta = b^2 - 4ac$.

Il existe. «Il existe $x \in A$ tel que $P(x)$» signifie qu'il y a au moins un x dans A tel que la propriété $P(x)$ est vraie. On peut l'employer même si on ne sait pas quels x de A vérifient P.

E Il existe $x \in \mathbb{R}$ tel que $x^7 + x + 1 = 0$.

Pour démontrer un énoncé de la forme

$$\exists x \in A, P(x),$$

il faut exhiber un élément x de A qui vérifie la propriété P. Le réflexe est une rédaction du type.

- Posons $x = \dots$.
- On vérifie $x \in A$ et $P(x)$.
- *Conclusion :* $\exists x \in A, P(x)$.

E $\forall x \in \mathbb{R}, \forall y \in \mathbb{R}, \exists z \in \mathbb{R}, z > x + y.$

Démonstration. Soient $x \in \mathbb{R}$ et $y \in \mathbb{R}$. [a]
Posons $z = x + y + 1$. On a bien $z \in \mathbb{R}$ et puisque $1 > 0$, on a $z = x + y + 1 > x + y$.
Conclusion : $\forall x \in \mathbb{R}, \forall y \in \mathbb{R}, \exists z \in \mathbb{R}, z > x + y$. ∎

[a] Ici, n'importe quel réel strictement plus grand que $x + y$ convient. Néanmoins, il faut en expliciter un.

Si ..., alors ... Si l'on fait une supposition qui ne dure que le temps d'une phrase.

E Si $x \geq 0$, alors $\sqrt{x^2} = x$.

Un théorème se présente souvent sous la forme $P \implies Q$, où P sont les hypothèses et Q la conclusion. Lorsque l'on «applique» un théorème, on utilise la règle si dessous :

M **Règle du modus ponens**

Étant données des relations P et Q, si la relation $(P \implies Q)$ est vraie, et si la relation P est vraie, alors la relation Q est vraie.

E

- La lampe est allumée, (P),
- or, si la lampe est allumée, alors l'interrupteur est fermé, $(P \implies Q)$,
- donc l'interrupteur est fermé. (Q).

Supposons P vraie. Sert à faire une hypothèse. Cette supposition (P vraie) est valable dans la suite de la démonstration jusqu'au terme (conclusion, nouveau tiret,...).
Pour démontrer

$$P \implies Q$$

on commence par *supposer* (ce n'est qu'une hypothèse) que P est vraie (c'est le seul cas que nous devons considérer car si P est faux, alors $P \implies Q$ est automatiquement vraie), puis on démontre d'une manière ou d'une autre que Q est vraie.

E $\forall x > 0, \forall y > 0, x < y \implies x^2 < y^2.$

Démonstration. Soit deux réels strictement positifs x et y, montrons [a]

$$x < y \implies x^2 < y^2.$$

- Supposons que $x < y$.
- On a donc $x^2 < xy$ car $x > 0$. On a également $xy < y^2$ car $y > 0$.
- Par conséquent, on a $x^2 < xy < y^2$. D'où $x^2 < y^2$.

∎

[a] Ici $P : x < y$ et $Q : x^2 < y^2$.

Une autre méthode de démonstration fréquemment utilisée dans la pratique est celle de la **disjonction de cas** ; elle repose sur l'énoncé suivant :

P

Soient P, Q, R trois relations ; si les trois relations

$$P \ \underline{\text{ou}}\ Q, \quad P \implies R, \quad Q \implies R$$

sont vraies, alors R est vraie.

Dans la pratique, on utilise surtout l'énoncé précédent en prenant pour Q la négation de P.

E

$\forall x \in \mathbb{R}, \max(-x, x) = |x|$.

Démonstration. Soit $x \in \mathbb{R}$.

- On suppose $x > 0$. Alors $x > -x$. Donc $\max(-x, x) = x = |x|$.
- On suppose $x \leq 0$. Alors $-x \geq x$. Donc $\max(-x, x) = -x = |x|$.

Conclusion : $\forall x \in \mathbb{R}, \max(-x, x) = |x|$. ∎

L'assertion $(P \implies Q)$ et l'assertion $(\text{non}\, Q \implies \text{non}\, P)$ sont tautologiquement équivalentes. Autrement dit, il revient au même de démontrer une implication ou de démontrer sa contraposée.

E $\forall n \in \mathbb{N}, (n^2 \text{ impair}) \implies (n \text{ impair})$.

Démonstration. Raisonnons par contraposition. Il s'agit d'établir que pour tout entier n, $(n \text{ pair}) \implies (n^2 \text{ pair})$. Soit $n \in \mathbb{N}$ fixé quelconque. Supposons n pair. Il existe alors $m \in \mathbb{N}$ tel que $n = 2m$. Ainsi $n^2 = 4m^2 = 2 \times 2m^2$ et n^2 est donc pair.
Ici, la contraposée est plus facile à prouver. L'hypothèse «$\text{non}\, Q$» portant sur n, il suffit d'élever au carré pour obtenir un renseignement su n^2. ∎

E Montrer

$$\forall n \in \mathbb{N}, (n^2 \text{ pair}) \implies (n \text{ pair}).$$

P

Étant données deux relations P et Q, la relation $(P \iff Q)$ est tautologiquement équivalente à la relation

$$(P \implies Q)\ \underline{\text{et}}\ (Q \implies P).$$

P

Étant données des relations P, Q et R, si les relations $P \iff Q$ et $Q \iff R$ sont vraies, alors la relation

$$P \iff R$$

est vraie.

Pour montrer

$$P \iff Q,$$

on peut procéder de plusieurs manières :

1. Montrer que $(P \implies Q)$ est vraie, puis montrer que sa réciproque $(Q \implies P)$ est vraie. En fait, dès que vous écrivez une équivalence, vous devez être capable de montrer ces deux implications. Par exemple,

$$\forall x \in \mathbb{R}, \forall y \in \mathbb{R}, \left\{ \begin{array}{ccc} x & +y & = 2 \\ x & -y & = 3 \end{array} \right. \iff \left\{ \begin{array}{ccc} x & +y & = 2 \\ 2x & & = 5 \end{array} \right.$$

est vraie car on conserve la première ligne et on modifie la seconde :

- pour passer de gauche à droite ($\implies$), on additionne les deux équations.
- pour passer de droite à gauche ($\impliedby$), on soustrait la première à la seconde.

Pour montrer

$$P \iff Q,$$

on peut procéder de plusieurs manières :

2. Aller de P à Q par une succession d'équivalences :

$$P \iff P_1 \iff P_2 \iff \cdots \iff P_n \iff Q$$

C'est souvent le cas dans des phases calculatoires, par exemple, la résolution d'un système d'équations. Pour $(x, y) \in \mathbb{R}^2$,

$$\begin{cases} x & +y & = 2 \\ x & -y & = 3 \end{cases} \iff \begin{cases} x & +y & = 2 \\ 2x & & = 5 \end{cases}$$

$$\iff \begin{cases} & y & = 2 - \frac{5}{2} \\ x & & = \frac{5}{2} \end{cases} \iff (x = \frac{5}{2} \text{ et } y = -\frac{1}{2}).$$

Pour montrer

$$P \iff Q,$$

on peut procéder de plusieurs manières :

3. Montrer que $(P \implies Q)$ est vraie, puis montrer que $(\text{non}\, P \implies \text{non}\, Q)$ est vraie. Par exemple, nous avons déjà montré que pour tout entier n, $(n^2 \text{ pair}) \implies (n \text{ pair})$ et $(n^2 \text{ impair}) \implies (n \text{ impair})$. Nous avons donc montré

$$\forall n \in \mathbb{N}, (n^2 \text{ pair}) \iff (n \text{ pair})$$

Pour montrer l'unicité d'un élément de A vérifiant la propriété P, on montre

$$\forall x \in A, \forall x' \in A, \left(P(x) \ \underline{\text{et}}\ P(x')\right) \implies x = x'.$$

Cela montre qu'il ne peut y avoir deux objets distincts possédant la propriété P.
L'unicité d'un élément ne prouve pas son existence, on montre qu'*il existe au plus* un $x \in A$ tel que P. «**Au plus un**» signifiant zéro ou un.
Pour démontrer la proposition «$\exists! x \in A, P(x)$», on le fait en deux étapes

- pour l'existence, on fait comme si on travaillait avec la proposition «$\exists x \in A, P(x)$»,
- pour l'unicité, on montre qu'il existe *au plus* un $x \in A$ tel que P. On suppose donc que deux éléments x et x' de A ont la propriété P et on montre alors que $x = x'$.

On peut également utiliser un raisonnement par « condition nécessaire» et « condition suffisante» (appelé également raisonnement par « Analyse» et « Synthèse»).

P

Soit P une assertion. Supposons que

$$\text{non } P \implies Q$$

où Q est une assertion fausse. Alors P est vraie.

Démonstration. Si non $P \implies Faux$ par contraposée, $vrai \implies P$, c'est-à-dire P vraie.
Ou formellement,

$$\big((\text{non } P \implies Q) \ \underline{\text{et}}\ (\text{non } Q)\big) \implies P$$

∎

E Montrer que $\sqrt{2} \notin \mathbb{Q}$.

Démonstration. Rappel : $\forall n \in \mathbb{N}, (n^2 \text{ pair}) \implies (n \text{ pair})$
On suppose $\sqrt{2} \in \mathbb{Q}$.
Alors, il existe deux entiers p et q, premiers entre eux, tels que $\sqrt{2} = \frac{p}{q}$.
On a donc $p^2 = 2q^2$, d'où p^2 est pair. Par conséquent p est aussi pair. Il existe donc un entier p' tel que $p = 2p'$.
De $4p'^2 = p^2 = 2q^2$, on déduit que $q^2 = 2p'^2$ est pair. Ainsi q est aussi pair.
Les entiers p et q étant tous les deux pairs, ils ne sont pas premiers entre eux. D'où la contradiction.
Conclusion : $\sqrt{2} \notin \mathbb{Q}$. ∎

Le raisonnement par condition nécessaire et condition suffisante (ou analyse-synthèse) est souvent employé pour prouver une existence-unicité.

E Déterminer l'unique fonction $f : \mathbb{R} \to \mathbb{R}$ telle que

$$\forall x \in \mathbb{R}, \forall y \in \mathbb{R}, f\,(x - f(y)) = 4 - 2x - 4y.$$

Démonstration. (CN) Soit $f : \mathbb{R} \to \mathbb{R}$ une fonction. On suppose

$$\forall x \in \mathbb{R}, \forall y \in \mathbb{R}, f\,(x - f(y)) = 4 - 2x - 4y.$$

En particulier, pour tout $x \in \mathbb{R}$,

$$f(x) = f\,((x + f(0)) - f(0)) = 4 - 2\,(x + f(0)) - 0 = 4 - 2f(0) - 2x.$$

L'application f est donc de la forme $f : x \mapsto \lambda - 2x$ où $\lambda \in \mathbb{R}$.
(CS) Soit $\lambda \in \mathbb{R}$ et $f : x \mapsto \lambda - x$. Alors pour tous $x, y \in \mathbb{R}$,

$$f\,(x - f(y)) = f\,(x - (\lambda - 2y)) = f(x + 2y - \lambda) = \lambda - 2(x + 2y - \lambda) = 3\lambda - 2x - 4y.$$

Ce calcul prouve que la seule valeur de λ pour laquelle f satisfait la condition donnée est $\lambda = \frac{4}{3}$.
Conclusion : La fonction $f : x \mapsto \frac{4}{3} - 2x - 4y$ est l'unique fonction pour laquelle,

$$\forall x \in \mathbb{R}, \forall y \in \mathbb{R}, f\,(x - f(y)) = 4 - 2x - 4y.$$

∎