Deuxième partie

Logique ensembliste

Chapitre 10

Structure logique

Résumé -

En mathématiques, on s'intéresse à des objets sur lesquelles on formule des assertions. Si, partant des axiomes ou des définitions on peut, en respectant des règles logiques, démontrer qu'une assertion est vraie, elle prend alors le nom de théoréme (avec un certain nombre de variantes sur ce nom : proposition *(résultat considéré comme un peu moins important qu'un théorème),* lemme *(résultat qui est avant tout une étape intermédiaire pour arriver au résultat final),* corollaire *(conséquence plus ou moins immédiate d'un résultat précédemment démontré).*
Le but de l'activité mathématique est de prouver de nouveaux résultats. Pour éviter les erreurs, il faut : du bon sens (i.e. de la logique), de la méthode, de la rigueur.
Quelques vidéos de youtubers :
— *Canal unisciel - Logique et raisonnement -*

Sommaire

1. Cours mathématiques

1.1. L'énigme mathématique

Pas de réponse, que des questions. Extrait de « l'efficacité des mathématiques est-elle déraisonnable » de D. Lambert.

? Problème 47 - Déraisonnable efficacité des mathématiques

Le développement des sciences physiques contemporaines a clairement manifesté l'efficacité surprenante des mathématiques. Dans un article souvent cité, E. P. Wigner parle à ce propos d'une « efficacité déraisonnable », d'une sorte de « miracle » qui est comme un « don magnifique que nous ne comprenons ni ne méritons ». Einstein lui-même manifeste son étonnement à cet égard ? : « Comment est-il possible que la mathématique, qui est un produit de la pensée humaine et indépendante de toute expérience, puisse s'adapter d'une si admirable manière aux objets de la réalité ? La raison humaine serait-elle capable, sans avoir recours à l'expérience, de découvrir par la pensée seule les propriétés des objets réels » ? Aujourd'hui cet étonnement est encore renforcé par les confirmations expérimentales très précises apportées à la mécanique quantique, à l'électrodynamique quantique, à la théorie unifiée des interactions électro-faibles (qui a permis la découverte effective des bosons vectoriels intermédiaires) ou encore à la théorie cosmologique standard (grâce aux mesures effectuées par le satellite COBE par exemple). De plus, cette efficacité se manifeste également, quoique de manière plus discrète, dans d'autres domaines des sciences. En biologie, par exemple, les mathématiques apportent des résultats surprenants au niveau de la compréhension des dynamiques de populations en écologie...

? Problème 48 - Un simple langage ? Ou plus

Les mathématiques sont-elles un langage ? Est-ce un jeu ? Un aperçu sur la/une vérité ? Autre chose...

? Problème 49 - Inspiration...

Les deux sources d'inspiration pour les mathématiques jusqu'au XXème siècle sont la physique dans sa globalité (mécanique, électricité, chimie...) et l'arithmétique (le calcul avec des nombres entiers). La géométrie a été aussi d'une certaine façon une source d'inspiration.
Il est donc nécessaire en filière mathématique d'étudier la physique et l'arithmétique...
La biologie et l'informatique (quoi que pour cette dernière, il est parfois compliqué de démêler informatique et mathématiques) sont de nouvelles sources d'inspiration...

1.2. Structure de cours

Analyse - Formalisation

Exercice
Pour ces six étapes, donner un pourcentage du temps passé en cours de mathématiques pendant le lycée ?
Reprendre l'exercice en fin d'année pour évaluer le cours de CPGE.

2. Quantificateurs et notations ensemblistes

2.1. Appartenance, éléments

Définition - Ensemble
Un ensemble est une "collection" d'objets appelés éléments. On introduit une relation particulière entre un élément x et un ensemble E, la relation d'appartenance :

$x \in E$, ce qui se lit "x appartient à E" ou "x est un élément de E.

La négation de la relation d'appartenance s'écrit $x \notin E$, ce qui signifie que $x \in E$ est faux.

Proposition - Propriété essentielle
Un ensemble est défini dés que pour tout objet x, on **peut dire** si x est, ou n'est pas, un élément de cet ensemble.

Pour aller plus loin - Propriété essentielle, sinon, c'est la faillite...
Trés vite dans la théorie des ensembles sont apparus quelques paradoxes, ce qui a demandé de faire une théorie plus fine. Ici, on reste au stade naïf, car cela demanderait beaucoup de temps et il serait assez peu productif de prendre ce temps.
La contradiction est de cette forme (en notant catalogue ou lieu d'ensemble) : « Peut-on faire un catalogue des catalogues qui ne se citent pas ?

Définition - Formalisation
On formalise les idées et objets pour signifier un certain type d'appartenance par :
$\forall x$, qui se lit « quel que soit x » ou pour « pour tout x »,
$\exists x$ se lit « il existe x »,
$\exists! x$ se lit « il existe un unique x »,

Attention - Pas d'abus
On n'abuse pas de ce formalisme dans un texte en français.
Seul un « $x \in E$ » peut être toléré.

Histoire - Assez récente...
Depuis la fin du XIXe siècle, la théorie mathématique s'appuie sur la théorie des ensembles. Le premier a les avoir étudier est Cantor (1845-1918).

On commence donc par définir ceux-ci. Parlant de cette théorie des ensembles, le grand mathématicien Hilbert affirmait : « Nul ne doit nous exclure du Paradis que Cantor a créé ».

Exemple - Applications

Exemple - Ensembles classiques

Exercice
Que pensez-vous de l'affirmation suivante ?
On a donc
$$\forall x \in \mathbb{R},\, x^2 \neq -1 \text{ mais } \exists x \in \mathbb{C} \mid x^2 = -1$$

Remarque - Convention de notation
La lettre x peut être remplacée par n'importe quel autre symbole, bien que quelques conventions tacites existent en mathématiques (parfois différentes de la physique) : $n, m, p, i, j, k, \ell, \ldots$ pour des entiers, $x, y, z, s, t, \theta, \epsilon, \ldots$ pour des réels, z pour un complexe...

Proposition - Règle de la théorie des ensembles
Quelques régles régissent les ensembles (dont certaines sont des axiomes de la théorie des ensembles) :
— régle n°1 : Deux ensembles qui ont les mêmes éléments sont égaux.
— régle n°2 : Il existe un ensemble qui n'admet aucun élément, soit
$$\exists E \mid \forall x, x \notin E$$
D'après la règle n°1, cet ensemble est unique, on l'appelle ensemble vide et on le note $\emptyset$.

2.2. Différentes manières d'écrire un ensemble

Descriptions : en extension, en compréhension, par image

Définition - Singleton, paire
Soit a un objet mathématique. L'ensemble dont a est l'unique élément s'appelle un singleton, on le note $\{a\}$.
Soient a et b deux objets distincts. L'ensemble dont ce sont les deux seuls éléments s'appelle la paire formée de a et b. On le note $\{a, b\}$

D'aprés la régle n°1, $\{a, b\} = \{b, a\}$, qu'il ne faut pas confondre avec le couple (a, b).
Si $a = b$, $\{a, b\} = \{a\}$.

Définition - Définition en extension
On dit que l'on définit un ensemble en extension lorsque l'on énumère ses éléments :

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

Cette notation sous-entend que l'on sait interpréter les ... intermédiaires.

Exemple - Ensemble défini en extension

Exercice
$\{1, 2, 3, \dots\} =$, $\{0, 1, -1, 2, -2, \dots\} =$

Définition - Définition en compréhension
On peut définir un ensemble en compréhension, c'est à dire par l'intermédiaire d'une propriété qui le caractérise : soit E un ensemble et $P(x)$ une propriété dépendant d'un objet x de E, alors

$$\{x \in E \mid P(x)\}$$

est l'ensemble des x éléments de E tels que $P(x)$ (sous-entendu "tels que $P(x)$ soit vraie").

Pour aller plus loin - Définition par image
On peut définir un ensemble par image, c'est à dire par l'intermédiaire d'une application qui le caractérise : soit E un ensemble et $f : E \to F$ et enfin $A \subset E$.
Alors

$$f(A) = \{f(x), x \in A\}$$

est le sous-ensemble de F dont les éléments sont des images d'éléments de A par f.

Exercice
$\{x \in \mathbb{R} | x^2 + 1 = 0\} =$
$\{x \in \mathbb{N} | x + 1 = 0\} =$
$\{x \in \mathbb{C} | x^2 + 1 = 0\} =$
$\{x \in \mathbb{Z} | x + 1 = 0\} =$
$\{a^2 + 2 | a \in [\![1, 5]\!]\} =$

Le dernier ensemble de cet exercice est un exemple d'ensemble défini comme image.

Intervalle de $\mathbb{R}$

Définition - Intervalles de $\mathbb{R}$
Pour $a, b \in \mathbb{R}$, $a < b$, on définit les intervalles de $\mathbb{R}$, ce sont les ensembles suivants :

$$[a, b] = \{x \in \mathbb{R} \mid a \leqslant x \leqslant b\} \quad]a, b] = \{x \in \mathbb{R} \mid a < x \leqslant b\} \quad [a, b[,]a, b[\dots$$
$$]-\infty, a] = \{x \in \mathbb{R} \mid x \leqslant a\} \quad]-\infty, a[= \{x \in \mathbb{R} \mid x < a\} \quad [b, +\infty[,]b, +\infty[\dots$$

Les intervalles du type $[a, b],]-\infty, a], [b, +\infty[$ sont des intervalles fermés

Les intervalles du type $]a,b[,]-\infty,a[,]b,+\infty[$ sont des intervalles ouverts
Les intervalles du type $[a,b[$ ou $]a,b]$ sont dits semi-ouverts (ou semi-fermés)
$[a,b]$ s'appelle un segment.

Exemple - Autres exemples

Savoir faire - Montrer que I est un intervalle de $\mathbb{R}$

Il suffit de montrer que pour tout $a,b \in I$, $[a,b] := \{t \in \mathbb{R} \mid a \leqslant t \leqslant b\} \subset I$.
C'est-à-dire :
« Soient $a,b \in I$ (quelconques puis fixés).
Soit $t \in [a,b]$ (i.e. $a \leqslant t \leqslant b$) alors. . . . . et donc $t \in I$. »

Exercice
Montrer que $J = \{x \in \mathbb{R} \mid 1 \leqslant x + e^x \leqslant 10\}$ est un intervalle.

2.3. Utilisation de quantificateurs

Heuristique - Quantificateurs nécessaires

En mathématiques classiques, deux quantificateurs sont essentiels :
- $\forall$, lu « pour tout » ou « quel que soit », pour désigner qu'une propriété a un certain degré d'universalité :
  $\forall\ x, \mathscr{P}(x)$. La propriété $\mathscr{P}$ est donc toujours vraie, puisque vraie pour tout point.
  $\forall\ x \in E, x \in F$. Tous les éléments de E sont dans F. Dans sa totalité : $E \subset F$.
- $\exists$ lu « il existe » est la négation du précédent.

Pour aller plus loin - Motivations
Il y a d'autres motivations.
Nous verrons plus loin l'articulation forte entre ces deux quantificateurs, en particulier pour la négation.
Nous verrons encore plus l'articulation très forte entre ces connecteurs et les opérations ensemblistes $\bigcap_{i\in I} A_i$ et $\bigcup_{i\in I} A_i$

Remarque - Existence ET unicité

Il arrive qu'on ait besoin d'ajouter l'unicité à l'existence (cas des antécédents pour une fonction bijective. . .).
On écrit alors : $\exists\,!x$, pour dire « il existe un unique x qui. . . »

Analyse - Non commutativité des connecteurs

Exemple - Suite majorée, ou rien

Exercice
On considère la suite de Fibonacci : $F_{n+2} = F_{n+1} + F_n$ et $F_0 = F_1 = 1$.
Que pensez-vous des deux assertions suivantes :
- $\forall\ n \in \mathbb{N}, \exists\ A,B \in \mathbb{R}$ tels que $F_n = A\left(\frac{1+\sqrt{5}}{2}\right)^n + B\left(\frac{1-\sqrt{5}}{2}\right)^n$
- $\exists\ A,B \in \mathbb{R}$ tels que $\forall\ n \in \mathbb{N}$, $F_n = A\left(\frac{1+\sqrt{5}}{2}\right)^n + B\left(\frac{1-\sqrt{5}}{2}\right)^n$

Savoir faire - Noter les dépendances

Si l'on écrit $\forall\ a, \exists\ b\dots$, le nombre b en second dépend grandement de a.
On devrait noter $b(a)$ ou b_a.
En revanche, si on écrit $\exists\ b$ tel que $\forall\ a\dots$, le nombre a ne dépend pas (plus particulièrement que les autres) de b. La notation a_b ou $a(b)$ n'aurait pas d'intérêt. Rappelons que cette formulation est la plus forte.
De nombreux problèmes rencontrés en mathématiques en MPSI par les élèves reposent sur la non compréhension de cette (in)dépendance.

Une autre stratégie est de faire comme en Python, des indentations dans la démonstration.
A chaque paramètre introduit, on fait apparaître un petit retrait dans l'écriture de la démonstration qui permet de voir comme ces paramètres dépendent mutuellement les uns des autres...

2.4. Parties d'un ensemble

Définition - Partie d'un ensemble (sous ensemble)
On dit qu'un ensemble F est inclus dans un ensemble E, ce que l'on note $F \subset E$, si tous les éléments de F sont éléments de E.
On dit aussi que F est une partie ou un sous-ensemble de E.

Savoir faire - Montrer que $F \subset E$

Pour montrer que $F \subset E$, on démontre :
$$F \subset E \Leftrightarrow (\forall x,\ x \in F \Rightarrow x \in E).$$

Proposition - Relation d'ordre
Quelques propriétés :
- $\emptyset \subset E$ pour tout ensemble E
- $E \subset E$ (l'inclusion est une relation réflexive)
- Si on a $E \subset F$ et $F \subset G$ alors on a aussi $E \subset G$ (l'inclusion est une relation transitive)
- Si on a $E \subset F$ et $F \subset E$ alors $E = F$ (l'inclusion est une relation antisymétrique)

Savoir faire - Prouver l'égalité de deux ensembles

La dernière propriété sert souvent à prouver l'égalité de deux ensembles.

Exercice
A quelle condition a-t-on : $\{a\} \subset E$? $\{a,b\} \subset E$? $\{a\} \subset \{b\}$?

Définition - Ensemble des partes de E
$\mathscr{P}(E)$ est l'ensemble des parties de E : $X \in \mathscr{P}(E)$ signifie donc à $X \subset E$.

Exemple - Singleton...

2.5. Produit cartésien

Définition - Produit cartésien de deux ensembles
Soient E et F deux ensembles. On appelle produit cartésien de E et F, et on note $E\times F$, l'ensemble dont les éléments sont les couples formés d'un élément de E et d'un élément de F (dans cet ordre) :

$$E\times F=\{x|\exists a\in E,\exists b\in F;\ x=(a,b)\}=\{(a,b)|a\in E \text{ et } b\in F\}.$$

Remarque - Rôle de la ponctuation
Le ";" dans la définition en compréhension peut être remplacé par " :", "tels que".
Plus généralement,

Définition - Produit cartésien de n ensembles
Soit $n\in\mathbb{N}$, si $E_1,\dots,E_n$ sont n ensembles, on définit le produit cartésien $E_1\times\cdots\times E_n$ comme l'ensemble des n-uplets $(a_1,\dots,a_n)$ formés d'éléments $a_1\in E_1,\dots,a_n\in E_n$.
Si les E_i désignent un même ensemble E, on note $E_1\times\cdots\times E_n=E^n$ $(\mathbb{R}^2,\mathbb{R}^3\dots)$

Remarque - Associativité du produit cartésien
A priori $E\times(F\times G)\neq(E\times F)\times G$, mais on les identifie fréquemment à $E\times F\times G$.

2.6. Opérations sur les ensembles

Définition - Réunion, intersection, différence d'ensembles
Pour E et F deux ensembles on définit :
- la réunion (ou union) de E et F : $E\cup F=\{x|x\in E \text{ ou } x\in F\}$ (le "ou" est inclusif : on peut avoir les deux simultanément)
- l'intersection de E et F : $E\cap F=\{x|x\in E \text{ et } x\in F\}$
- la différence de E et de F : $E\setminus F=\{x|x\in E \text{ et } x\notin F\}$

Remarque - Interprétation avec une table de vérité
En d'autres termes on a :

$x\in E$	$x\in F$	$x\in E\cup F$	$x\in E\cap F$	$x\in E\setminus F$
V	V	V	V	F
V	F	V	F	V
F	V	V	F	F
F	F	F	F	F

Définition - Complémentaire d'un ensemble (dans un ensemble plus gros)
Lorsque $F\subset E$, l'ensemble $E\setminus F$ est appelé complémentaire de F dans E et noté $\complement_E F$.
On ne peut parler de complémentaire de l'ensemble F que relativement à un ensemble "contenant" ce dernier. Toutefois, en l'absence d'ambiguïté sur E, on peut noter $\complement F$ ou F^c ou $\overline{F}$ (cette dernière notation ayant cependant différents sens suivant le domaine des mathématiques...)

Attention - Le verbe contenir
Attention également à l'ambiguïté du verbe "contenir", parfois utilisé pour dire que x est élément de E, parfois pour dire que F est une partie de E.

Exercice
Soit $A = \{x \in \mathbb{N} \mid x/2 \in \mathbb{N} \text{ et } x \geqslant 10\}$. Que représente A ? Ecrire cet ensemble différemment.
Ecrire en extension $\complement_{2\mathbb{N}} A$ puis déterminer $\complement_{\mathbb{N}} A$.
Déterminer les sous-ensembles X de $\mathbb{N}$ tels que $A \cup X = \mathbb{N}$.

Exercice
Soit E un ensemble. Que peut-on dire de deux parties A et B de E vérifiant $A \cap B = A \cup B$?

Pour aller plus loin - Probabilité
Nous reprenons ces notions lors du cours de probabilité. Il y aura quelques modifications de vocabulaire

Exercice
On définit la différence symétrique de deux ensembles E et F par

$$E \Delta F = (E \setminus F) \cup (F \setminus E).$$

Ecrire $E \Delta F$ à l'aide de $E \cup F$ et $E \cap F$.

Proposition - Quelques règles de calcul
E, F et G désignent trois ensembles quelconques.

$$\begin{aligned}
E \cup F &= F \cup E && \text{(commutativité de la réunion)}\\
E \cup (F \cup G) &= (E \cup F) \cup G && \text{(associativité de la réunion)}\\
\emptyset \cup E = E \cup \emptyset &= E && \text{(l'ensemble vide est neutre pour la réunion)}\\
E \cap F &= F \cap E && \text{(commutativité de l'intersection)}\\
E \cap (F \cap G) &= (E \cap F) \cap G && \text{(associativité de l'intersection)}\\
\emptyset \cap E = E \cap \emptyset &= \emptyset && \text{(l'ensemble vide est absorbant pour l'intersection)}\\
E \cap (F \cup G) &= (E \cap F) \cup (E \cap G) && \text{(distributivité de l'intersection par rapport à la réunion)}\\
E \cup (F \cap G) &= (E \cup F) \cap (E \cup G) && \text{(distributivité de la réunion par rapport à l'intersection)}
\end{aligned}$$

Pour A et B deux parties de E :

$$\begin{aligned}
A \cap E &= A\\
A \cup E &= E\\
\complement_E(\complement_E A) &= A\\
\complement_E(A \cup B) &= (\complement_E A) \cap (\complement_E B)\\
\complement_E(A \cap B) &= (\complement_E A) \cup (\complement_E B)
\end{aligned}$$

Les deux dernières formules sont connues sous le nom de lois de Morgan.

Pour la démonstration, on lie ces résultats aux affirmations correspondantes.
On peut aussi faire une table exhaustive de vérité

Démonstration

3. Vocabulaire sur les assertions

3.1. Définitions

Définition - Assertion (proposition) et prédicat
Dans ce paragraphe une proposition, ou assertion est un énoncé qui peut prendre deux valeurs logiques : V (vrai) ou F (faux).
Si cette assertion dépend d'une variable x on parle alors de prédicat.

Exemple - Propositions

Comme on peut le voir dans les parties suivantes, à partir de deux assertions A et B, on en définit d'autres dont la valeur logique est donnée par une table de vérité.

Exercice

Que pensez-vous de $\mathscr{P}_n$ dans l'énoncé formel suivant ?

Notons, $\forall\ n \in \mathbb{N}, \mathscr{P}_n$: « $\exists\ k \in E$ tel que $a_n = k$ »

Pour aller plus loin - Logique floue (1)
Formalisée en 1965, la logique floue élargie ce point de vue : on associe un nombre entre 0 et 1 pour mesurer la véracité de chaque proposition. Une proposition de valeur 0 est fausse. Une proposition de valeur $\frac{1}{2}$ est à moitié fausse. L'arithmétique qui en découle est comparable à celle des probabilités d'événements.
Cela s'appuie sur les ensembles floues avec des degré d'appartenance entre le $\in$ et le $\notin$.
On l'utilise en automatique ou en médecine...

3.2. Négation

Définition - Négation d'une assertion
Considérons une assertion A.
On appelle négation de A l'assertion qui dit le contraire de A, c'est à dire qui est vraie exactement lorsque A est fausse, on la note "non$A$" (ou $\neg A$ en logique).
Latable de vérité de non$A$:

A	non A
V	F
F	V

Exercice

La négation de « L'hiver dernier il a plu tous les jours à Toulouse » est :
La négation de « Chaque hiver, il neige au moins un jour en Aveyron » est :

Soit I un intervalle de $\mathbb{R}$.
La négation de « $0 \in I$ » est
La négation de « $\forall x \in I, x > 0$ » est
La négation de « $\exists x \in I \mid x \geqslant 0$ » est

D'une manière plus générale il faut savoir nier une proposition écrite avec des quantificateurs :

Exercice

P désignant une propriété dépendant de x ou de x, y suivant les cas, écrire la négation des assertions suivantes :

1. $\forall x \in E, P(x)$;
2. $\exists x \in E | P(x)$;
3. $\forall x \in E, \exists y \in E | P(x, y)$;
4. $\exists x \in E | \forall y \in E, P(x, y)$;
5. $\exists r \in \mathbb{R}, \exists s \in \mathbb{R} | \forall x \in \mathbb{R}, x \leqslant r$ et $s \leqslant r$.

L'exercice suivant permet de revoir également la table de vérité d'une conjonction (« et ») ou disjonction (« ou ») d'assertions.

Exercice

Compléter le tableau suivant :

A	B	A et B	A ou B	non (A et B)	non (A ou B)	non A	non B	
V	V	V	V					
V	F	F	V					
F	V	F	V					
F	F	F	F					

On a laissé une colonne pour des « tests ». Quelle relation remarquez-vous ?

3.3. Implications et équivalence d'assertions

Définition - Implication d'assertions
Considérons deux assertions A et B.
Si, lorsque l'assertion A est vraie, alors, nécessairement, l'assertion B l'est également, on dit que A implique B et l'on écrit $A \Rightarrow B$
(ce qui se lit donc "A implique B" ou "si A alors B").
Plus précisément, la table de vérité de $A \Rightarrow B$ est donnée par :

A	B	$A \Rightarrow B$
V	V	V
V	F	F
F	V	V
F	F	V

Remarque - Et si A est fausse
On remarquera qu'en logique, dés que A est fausse, $A \Rightarrow B$ est évaluée vraie, en bref, vous pouvez construire sans problème une démonstration juste avec une hypothèse fausse, mais finalement c'est sans intérêt parce que vous n'avez aucun résultat à énoncer à la fin...c'est la raison pour laquelle usuellement "prouver $A \Rightarrow B$" sous entend "prouver A vraie $\Rightarrow B$ vraie ".
Et donc si $E = \emptyset$, tout énoncé "$\forall x \in E, P(x)$" (ou "$x \in E \Rightarrow P(x)$") a la valeur logique V...

Exercice
Quelle est l'assertion qui a même table de vérité que « non($A \Rightarrow B$)' » ?

Pour aller plus loin - Logique floue (2)
A la place de V et F, on peut respectivement écrire 1 et 0.
Dans ce cas si p_i est une proposition et $v(p_i)$ sa valeur ($v(p_i) = 0$, si p_i est fausse...).
On a donc $v(p_1 \cap p_2) = v(p_1) \times v(p_2)$, $v(non(p_1)) = 1 - v(p_1)$ et $v(p_1 \cup p_2) = v(p_1) + v(p_2) - v(p_1)v(p_2)$.
Cet arithmétique se transpose aisément en logique floue.

Avec deux implications, on a exactement une équivalence :

Définition - Equivalence d'assertions
Considérons deux assertions A et B.
On dit que A et B sont équivalentes si elles signifient la même chose, mais dite différemment, c'est à dire si, simultanément, A implique B et B implique A;
on note alors $A \Leftrightarrow B$.
Plus précisément, la table de vérité de $A \Leftrightarrow B$ est donnée par :

A	B	$A \Leftrightarrow B$
V	V	V
V	F	F
F	V	F
F	F	V

Exemple - Deux assertions équivalentes

Exercice
Comparer la table d'équivalence de $A \Leftrightarrow B$ avec celle de [($A \Rightarrow B$) et ($B \Rightarrow A$)]

Attention - A démontrer ?
Certaines équivalences correspondent en fait à la définition d'un objet mathématique, d'autres en revanche nécessitent une démonstration.

Attention - Ne pas abuser de $A \Longleftrightarrow B$
Les étudiants écrivent TROP souvent $A \Longleftrightarrow B$, en faisant un calcul dans leur tête (ou une démonstration) qui permet de passer de A à B, SANS vérifier si l'on passe aussi de B à A.
Il est important de ne pas faire cette erreur, surtout si l'on demande qu'une implication.... Il ne faut pas en faire trop, si c'est faux !

4. Principales méthodes de démonstration

4.1. Démonstration d'une implication

Démonstration directe

Considérons deux assertions A et B. On veut démontrer que $A \Rightarrow B$.

Savoir faire - $A \Rightarrow B$. Raisonnement direct
On suppose A vraie, par une succession d'implications connues (calculs, résultats de théorèmes...), on prouve qu'alors B est vraie.

Exercice
Montrer que si (x, y) est élément de $]0,2[\times]-2,0[$ alors $\frac{1}{x}-\frac{1}{y}>1$

Exercice
Soit f la fonction définie sur $\mathbb{R}$ par $f(x)=|x+\frac{3}{2}|-\frac{1}{2}$. Montrer que

$$x \geqslant -1 \Rightarrow f(x) \geqslant 0$$

On peut-être amené à faire une disjonction de cas :
Exercice
Compléter l'énoncé suivant pour que la démonstration nécessite l'étude de deux cas séparés.
Soit f la fonction définie par ...
Montrer que $x \geqslant -1 \Rightarrow f(x) \geqslant 0$.

Le chemin de la démonstration

Heuristique - Démontrer que ...
Lorsqu'on cherche à démontrer un résultat, il y a fondamentalement deux attentes :

1. Trouver la (une) démonstration,
   satisfaisante i.e. qui donne la certitude du fait
2. Ecrire la démonstration,
   de sorte que toute personne qui lise la démonstration soit également persuadé du fait

Avec le temps du passage de 1 à 2, il faut donc trois temps dans la recherche d'une démonstration.

Attention - Premier piège

Le temps 1 est le temps de l'analyse.
Le temps 2 est le temps de la synthèse.
Ce sont deux choses très différentes. Lorsque vous lisez une démonstration d'un théorème faite par un professeur, un corrigé dans un livre… vous ne voyez que le second temps, celui de la synthèse. Après la lecture, vous pouvez vous dire : « et oui, je vois que c'est vrai », mais vous n'avez pas appris *comment on trouve* la démonstration!!!
La seule solution est de chercher, chercher, chercher… et de ne pas se précipiter sur la (une) solution.
De même, si pour vous écrire une démonstration de cours lors d'une colle est uniquement un exercice de mémoire, alors c'est que vous n'avez pas compris le premier point, ni le point $1 \to 2$ de la démonstration du fait considéré. *Pouvez-vous donner un exemple d'une telle situation rencontrée ?*

Analyse - La métaphore du petit poucet

Exemple - Exercice « de base »

On suppose que $f : E \to E$ est surjective, montrer que $f^2 (= f \circ f)$ est surjective.
Si l'on n'écrit pas ce que l'on veut obtenir i.e. le point B : « f^2 est surjective », on ne peut s'en sortir uniquement en dérivant du point A : « f est surjective ».
Pour préparer la démonstration, il faut donc laisser des espaces et compléter au fur et à mesure.
Le temps joue un rôle important, or il n'y parait plus lorsque la démonstration est écrite. Pour le voir à l'oeuvre, nous allons présenter la démonstration comme succession de photos prises de son écriture.

Pour aller plus loin - f surjective, injective

On verra plus loin les définitions. A ce stade, il suffit de savoir que par définition f est surjective de E sur F si $\forall y \in F, \exists x \in E$ tel que $y = f(x)$.
Et par définition f est injective de E (sur F) si $\forall x_1, x_2 \in E, f(x_1) = f(x_2) \Leftrightarrow x_1 = x_2$.

1er 2eme 3eme 4eme 5eme 6eme 7eme

Soit $y \in E$

f est surjective donc $\forall\ b \in E, \exists\ a \in E$ tel que $b = f(a)$

ainsi $\exists\ x_1$ tel que $y = f(x_1)$

et $\exists\ x_2$ tel que $x_1 = f(x_2)$

donc $\exists\ x(= x_2)$ tel que $f^2(x) = f(x_1) = y$

$\forall\ y \in E, \exists\ x \in E$ tel que $y = f^2(x)$

donc f^2 est surjective

Cela s'écrit ensuite :
Soit $y \in E$
  f est surjective donc $\forall\ b \in E, \exists\ a \in E$ tel que $b = f(a)$.
    ainsi $\exists\ x_1$ tel que $y = f(x_1)$
    et $\exists\ x_2$ tel que $x_1 = f(x_2)$
    donc $\exists\ x(= x_2)$ tel que $f^2(x) = f(x_1) = y$
Donc : $\forall\ y \in E, \exists\ x \in E$ tel que $y = f^2(x)$ et finalement : f^2 est surjective

Exercice

Soit E un ensemble et $f : E \to E$, une application sur E.
On suppose que $f^3 = f$. Montrer que si f est injective alors f est surjective. Et réciproquement.

Contraposée

Proposition - Contraposée
(non $B \Rightarrow$ non A) s'appelle la contraposée de $(A \Rightarrow B)$.
Il est équivalent de prouver l'une ou l'autre de ces deux implications

Démonstration

Savoir faire - $A \Rightarrow B$. Raisonnement par contraposée
On suppose donc B fausse et on prouve qu'alors A est fausse, comme précédemment

Le résultat de l'exercice suivant sera fréquemment exploité en analyse :

Exercice

On considére un nombre réel $x \geqslant 0$. Montrer que

$$(\forall \epsilon > 0, 0 \leqslant x \leqslant \epsilon) \Rightarrow x = 0.$$

4.2. Démonstration d'une équivalence

Deux possibilités pour prouver l'équivalence $A \Leftrightarrow B$:

Savoir faire - $A \Leftrightarrow B$. On procède en deux temps

1. On montre $A \Rightarrow B$
2. On montre $B \Rightarrow A$

Exercice
On considère une fonction f définie sur $\mathbb{R}$ à valeurs dans $\mathbb{R}$. Montrer que

$$(f \text{ est une fonction paire et impaire }) \Leftrightarrow (f \text{ est la fonction nulle }).$$

Savoir faire - $A \Leftrightarrow B$. On procède par équivalences connues successives.
Cette méthode est surtout utilisée pour des résolutions calculatoires.
Attention de ne pas en abuser : *il faut à chaque étape être sûr que l'on peut « remonter » les équivalences.*

Exercice
Montrer que

$$\begin{cases} 2x+y=2 \\ 3x+4y=3 \end{cases} \Longleftrightarrow (x,y)=(1,0)$$

Insistons :

Truc & Astuce pour le calcul - Ne pas abuser de $\Leftrightarrow$
Il faut éviter le plus possible d'écrire $\Leftrightarrow$ comme un tic de langage.

1. Si il n'est pas utile, on ne le note pas !
2. Si on choisit de le noter, on vérifie bien à chaque étape le sens $\Leftarrow$ tout particulièrement.

4.3. Raisonnement par l'absurde

Savoir faire - Raisonnement par l'absurde
Pour démontrer un certain énoncé, on fait l'hypothèse qu'il est faux et on aboutit à une contradiction.

Exercice
Montrer que le réel $\sqrt{2}$ est irrationnel (i.e. n'est pas rationnel)

Remarque - Différence avec la contraposée
Pour la contraposée, on suppose non$B$ et on aboutit à non$A$.
Pour l'absurde, on suppose non$B$ et A ensemble et on montre qu'il y a une contradiction. Dans ce second cas, on exploite plus d'hypothèses !

Pour aller plus loin - Raisonnement par l'absurde, à accepter ?
Certaine axiomatique de mathématique refuse le raisonnement par l'absurde, en effet la notion d'existence qui en découle est quelque peut frustrante.
On sait que $\sqrt{2}$ n'est pas un nombre rationnel, c'est un nombre algébrique de degré 2 (quadratique).
Notons $a=\sqrt{2}^{\sqrt{2}}$. Alors il existe un nombre transcendant à la puissance $\sqrt{2}$ (transcendant) qui est algébrique (contraire de transcendant).
En effet, si a est algébrique, alors $\sqrt{2}$, à la puissance $\sqrt{2}$ est algébrique.
Si tel n'est pas le cas alors a est transcendant et $a^{\sqrt{2}}=\sqrt{2}^{\sqrt{2}^{\sqrt{2}}}=\sqrt{2}^{\sqrt{2}\times\sqrt{2}}=\sqrt{2}^2=2$. Donc c'est a qui résout le problème.
Et pourtant...
On ne sait toujours pas aujourd'hui lequel des deux nombres $\sqrt{2}$ ou $\sqrt{2}^{\sqrt{2}}$ répond à la question !

4.4. Conditions nécessaire, suffisante

Il s'agit simplement *d'un peu de bon sens* sur la signification des mots « nécessaire » et « suffisant ».

Exemple - A : « x est le carré d'un entier » et B : « $x \geqslant 0$ »

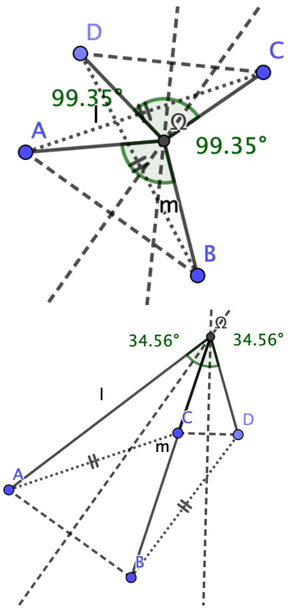
Définition - Condition nécessaire. Condition suffisante
Plus généralement $A \Rightarrow B$ peut se dire :
- B est une condition nécessaire (**CN**) pour avoir A (puisque si on A, nécessairement on a B)
- A est une condition suffisante (**CS**) pour avoir B (puisqu'il suffit d'avoir A pour avoir B

Rechercher une condition nécessaire et suffisante (**CNS**) pour avoir A revient donc à chercher B tel que $A \Leftrightarrow B$.

Savoir faire - Analyse-Synthèse
Certaines démonstrations, difficiles à gérer par équivalences, ou lorsque le résultat n'est pas donné, se font en deux phases :
1. phase d' "analyse" : on obtient une condition nécessaire (par implications successives par exemple) pour qu'une première hypothèse soit vérifiée
2. phase de "synthèse", ou phase de vérification : la condition précédemment obtenue est-elle suffisante ?

Exercice
Montrer que toute fonction définie sur $\mathbb{R}$ à valeurs dans $\mathbb{R}$ s'écrit de manière unique comme somme d'une fonction paire et d'une fonction impaire.
On procédera de la manière suivante :
Première étape (analyse) : supposons qu'il existe deux fonctions f et g telles que ..., alors $f =\quad , g =$
Deuxième étape (synthèse) : on vérifie que les solutions trouvées à la première étape conviennent

Représentation - Deux configurations de l'exercice



Exercice
Soit A, B, C et D quatre points du plan tel que $AC = BD$ et (AB) non parallèle à (CD).
Alors il existe une unique rotation du plan r tel que $r(A) = B$ et $r(C) = D$.
Donner ses caractérisations

On appliquera ce résultat dans le cours sur les nombres complexes.

4.5. Exploiter un contre-exemple dans une démonstration

Savoir faire - Utilisation d'un contre-exemple
Lorsque l'on veut prouver qu'une implication est fausse, on cherche un exemple vérifiant l'hypothèse mais pas la conclusion, ce que l'on appelle un contre-exemple.

Exercice
Soit f la fonction définie sur $\mathbb{R}$ par $f(x) = |x + \frac{3}{2}| - \frac{1}{2}$. Montrer que $(x \geqslant -1)$ et $(f(x) \geqslant 0)$ ne sont pas équivalents.

4.6. Démonstration par récurrence

Proposition - Principe admis (axiome)
Soit $P(n)$ (parfois notée $\mathscr{P}_n$) une propriété portant sur l'entier n.
Si on a
$$\begin{cases} P(0) \text{ vraie} \\ \forall n \in \mathbb{N}, (P(n) \text{ vraie } \Rightarrow P(n+1) \text{ vraie }) \end{cases}$$
alors $P(n)$ est vraie pour tout entier n.

Savoir faire - Rédaction d'un raisonnement par récurrence

• Pour $n = 0$, $P(0)$ est vérifiée, avec vérification effective! (souvent deux simples calculs)
• Supposons la propriété vérifiée pour **un certain** $n \geqslant 0$ (et surtout pas "pour tout", parce que là, ce n'est plus la peine de faire une démonstration!).
  $\Rightarrow$ Montrons que $P(n+1)$ est vraie.
Conclusion : $\forall n \in \mathbb{N}$, $P(n)$ est vraie.

Remarque - Démarrer à un autre nombre

On peut aussi démarrer à une valeur de n autre que 0.

Exercice

Montrer que $\forall n \in \mathbb{N}$, $n < 2^n$.

Exercice

Y a-t-il des erreurs dans les raisonnements suivants ? Où sont-elles ?

1. On a : $10^{n+1} + 1 = 10 \times 10^n + 1 = (9+1) \times 10^n + 1 = 9 \times 10^n + 10^n + 1$
   Donc, si $10^n + 1$ est divisible par 9, il en est de même de $10^{n+1} + 1$, ce qui prouve que pour tout entier naturel n, $10^n + 1$ est divisible par 9.
2. Prouvons que tout ensemble fini a tous ses éléments égaux :
   Si dans tout ensemble E_n à n éléments, tous les éléments sont égaux, alors, soit E_{n+1} un ensemble à $n+1$ éléments :
   $$E_{n+1} = \{x_1, x_2, \dots, x_n, x_{n+1}\}.$$
   Avec l'ensemble de n éléments $\{x_1, x_2, \dots, x_n\}$, on a, par hypothése de récurrence : $x_1 = x_2 = \cdots = x_n$.
   Avec l'ensemble de n éléments $\{x_2, x_3, \dots, x_{n+1}\}$, on a, par hypothése de récurrence : $x_2 = x_3 = \cdots = x_{n+1}$.
   Donc $x_1 = x_2 = \cdots = x_{n+1}$.
   Comme la propriété est vraie pour $n = 1$ (cas d'un singleton), il en résulte que tout ensemble de n éléments a tous ses éléments égaux.

Histoire - Citation de Henri Poincaré, La science et l'hypothèse, 1902

« Le caractère du raisonnement par récurrence est qu'il contient, condensés, pour ainsi dire en une formule unique, une infinité de syllogismes.
Pour qu'on s'en puisse mieux rendre compte, je vais énoncer les uns après les autres ces syllogismes qui sont, si l'on veut me passer l'expression, disposés en cascade.
Ce sont bien entendu des syllogismes hypothétiques.
Le théorème est vrai du nombre 1.
Or si il est vrai de 1, il est vrai de 2.
Donc il est vrai de 2.
Or si il est vrai de 2, il est vrai de 3.
Donc il est vrai de 3, et ainsi de suite… »

Savoir faire - Récurrence à plusieurs pas (ou plusieurs termes)

Suivant la façon dont est énoncée la propriété de récurrence $P(n)$ il peut être nécessaire
• d'initialiser la récurrence avec plusieurs (k) valeurs de n
• de supposer $P(n), \dots, P(n+k-1)$ (il y en a aussi k) vraies pour un certain $n \geqslant 0$
• de prouver que ces k propriétés exactes entraînent $P(n+k)$ vraie

Savoir faire - Récurrence forte

• Pour $n = 0$, $P(0)$ est vérifiée (avec vérification effective!)
• Supposons la propriété vérifiée **jusqu'à** un certain $n \geqslant 0$ (i.e $P(0), P(1), \dots, P(n)$ vraies)
• Montrons que $P(n+1)$ est vraie.

On parle parfois alors de « récurrence à plusieurs pas » ou de « récurrence forte », par opposition à la récurrence du théorème dite « récurrence simple (ou faible) »).

Exercice

Soit (u_n) la suite définie par $u_0 = \dfrac{2}{5}$, $u_1 = 1$ et pour tout entier naturel n,

$$u_{n+2} = 5u_{n+1} - 6u_n.$$

Démontrer que pour tout $n \in \mathbb{N}$, $u_n = \dfrac{2^n + 3^n}{5}$.

Exercice

Montrer que tout entier $n \geqslant 2$ se décompose en produit de nombres premiers.

Exercice

Montrer qu'un changement d'hypothèse de récurrence ramène une récurrence à plusieurs pas ou une récurrence forte à une récurrence faible.

Exercice

Montrer par récurrence forte que toute suite décroissante d'entiers est stationnaire (i.e. constante à partir d'un certain rang).

4.7. Démonstration par algorithme

Algorithme

Heuristique - Exploitation d'un algorithme

Un algorithme peut permettre de démontrer, constructivement, l'existence d'un certain objet (ou d'une certaine fonction).
La difficulté est plutôt de démontrer que l'algorithme :

- se termine bien
- réalise bien ce que l'on désire

Définition - Algorithme

Un algorithme est une suite finie de règles à appliquer dans un ordre déterminé à un nombre fini de données pour arriver avec certitude (c'est-à-dire sans indétermination ou sans ambiguïté), en un nombre fini d'étapes, à un certain résultat et cela indépendamment des données.

Terminaison de l'algorithme

Pour démontrer que l'algorithme termine (que le nombre d'étapes est fini), on exploite un variant de boucle, en règle général, en suite d'entiers décroissante. Pour des boucles `for`, la terminaison de boucle est en règle générale immédiate.

Savoir faire - Démontrer qu'une boucle se termine

On identifie une expression (variable) qui :

- est entière
- décroît strictement à chaque étape de la boucle

Alors, nécessairement, la boucle se termine.

Exemple - Division euclidienne

Exercice

On considère le bout de programme suivant :

```
c=0
while p>0 :
        if c==0 :
                p=p-2
                c=1
        else :
                p=p+1
                c=0
```

1. Que fait ce programme ?
2. Les variables `p` et `c` sont-elles décroissantes, strictement ?
3. Montrer que la variable `t=2p+3c` est entière, strictement décroissante.
   En déduire la terminaison de l'algorithme.

Correction de l'algorithme

Il faut aussi savoir **démontrer** que le programme (avec de nombreuses répétitions de la boucle) réalise se que l'on souhaite.
On utilise alors pour cela des *invariant de boucles*.
Comme son nom l'indique il s'agit d'identifier (créer) une expression-variable qui ne change pas de valeur tout au long du programme.
Puis lorsque le programme se termine, en exploitant cette expression, nous pourrons démontrer que l'on obtient bien le résultat attendu.

Savoir faire - Utilisation d'un invariant de boucle pour démontrer le résultat attendu

Pour démontrer qu'une boucle réalise bien le résultat attendu,

1. on cherche une expression qui reste constante tout au long des calculs de la boucle ;
2. on calcule sa valeur initiale (avant le début de la boucle) ;
3. on en déduit sa valeur finale ;
4. enfin connaissant les valeurs finales des variables du système (testées pour la sortie de boucle), on en déduit la valeur de la variable retournée par le programme.

Exemple - Retour sur la division euclidienne

Exercice

Montrer que le programme

```
def somme2(n) :
    S=0
    for i in range(1,n+1):
        S=S+i**2
    return(S)
```

calcule bien $\sum_{i=1}^{100} i^2$

Exercice

On cherche à écrire un programme qui calcul $n!$.

1. Ecrire un programme avec une boucle `while`.
2. **Démontrer** que le programme se termine bien.
3. **Démontrer** que le programme effectue bien ce que l'on souhaite.

Proposition - Plus petit élément d'un ensemble fini
Considérons E un ensemble muni d'une relation d'ordre totale.
Un ensemble A de n éléments de E admet un plus petit élément.

Nous allons faire la démonstration par algorithme

Démonstration

5. Bilan

Synthèse

- ⇝ En mathématiques, les raisonnements se fondent sur une vision ensembliste des objets ou des propositions. Nous faisons un premier passage, *de bon sens*, sur ce qu'est un ensemble et ce que signifie appartenir à un ensemble ou en être une partie; ce qu'est un intervalle ou un produit cartésien d'ensembles.
- ⇝ Naturellement, apparait fréquemment dans les affirmations mathématiques ensemblistes deux notions : une notion d'universalité *pour tout* et une notion d'exception *il existe*. La formalisation qui est le langage écrit des mathématiques, réserve donc deux symboles pour ces notions : $\forall$ et $\exists$. On les retrouve tout le temps.

$\rightsquigarrow$ Les mathématiques donnent des relations (de vérité ?) entre les assertions. Nous voyons différentes méthodes exploitées dans *l'artisanat de la démonstration* : table de vérité (cas par cas), implication ou équivalence, analyse-synthèse, contraposée, raisonnement par l'absurde, contre-exemple ou récurrences...

Savoir-faire et Truc & Astuce du chapitre

- Savoir-faire - Montrer que I est un intervalle de $\mathbb{R}$
- Savoir-faire - Noter les dépendances
- Savoir-faire - Montrer que $F \subset E$
- Savoir-faire - Prouver l'égalité de deux ensembles
- Savoir-faire - $A \Rightarrow B$. Raisonnement direct.
- Savoir-faire - $A \Rightarrow B$. Raisonnement par contraposée.
- Savoir-faire - $A \Leftrightarrow B$. On procède en deux temps.
- Savoir-faire - $A \Leftrightarrow B$. On procède par équivalences connues successives.
- Truc & Astuce pour le calcul - Ne pas abuser de $\Leftrightarrow$
- Savoir-faire - Raisonnement par l'absurde
- Savoir-faire - Analyse-Synthèse
- Savoir-faire - Utilisation d'un contre-exemple
- Savoir-faire - Rédaction d'un raisonnement par récurrence
- Savoir-faire - Récurrence à plusieurs pas (ou plusieurs termes)
- Savoir-faire - Récurrence forte
- Savoir-faire - Démontrer qu'une boucle termine
- Savoir-faire - Utilisation d'un invariant de boucle pour démontrer le résultat attendu

Notations

Notations	*Définitions*	*Propriétés*	*Remarques*
$\forall$ - $\exists$	Pour tout (ou quel que soit) - Il existe	Les affirmations mathématiques exploitent très souvent uniquement ces deux symboles	Attention, on a n'a pas : $\forall\, a \exists\, b \Leftrightarrow \exists\, b \forall\, a$
$A \Longrightarrow B \equiv B \Longleftarrow A$	Implication de A vers B	A est suffisante pour B et B est nécessaire à A	Ex : $\exists\, b \forall\, a \Rightarrow \forall\, a \exists\, b$
$A \Longleftrightarrow B$	A et B sont équivalentes	Identique à $A \Rightarrow B \& B \Rightarrow A$	Ne pas en abuser.

Retour sur les problèmes

47. Quoi dire...
48. Ce n'est probablement pas qu'un langage, mais...
49. Ce n'est pas un problème