Mise à jour le 19 août 2020

Raisonnements mathématiques
Résumé de cours

Rédaction : Samy Abbes, utilisant des notes de René Cori

Université de Paris
L1 Mathématiques,
Mathématiques-Informatique, MIASHS
Année 2020-21

1—Langage mathématique : noms, objets et énoncés

1.1—Les énoncés mathématiques

1.1.1—Les noms d'objets

Le discours mathématique est structuré à partir de *noms* qui désignent des *objets mathématiques*. Un nombre entier, un nombre réel, un nombre complexe, une fonction, un ensemble de points dans un plan, sont des exemples d'objets. Voici des exemples de noms pour désigner des objets :

Nom	Commentaire
1	"Un" est un autre nom pour le même objet. C'est une *constante*.
x	Une variable, dont on doit préciser quel est l'ensemble des valeurs qu'elle peut prendre.
$3/2$	"Trois demis" est un autre nom pour cette fraction. C'est aussi une constante.
$1,5$	Un autre nom pour la constante "trois demis".
$\mathbf{i}$	Une constante complexe imaginaire pure, celle qui a 1 pour partie imaginaire.
$\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$, $\mathbb{N}$	Les noms des ensembles de nombres usuels : les réels, les rationnels, les entiers relatifs, les entiers naturels.
$\{(x,y) \in \mathbb{R}^2 \mid x^2+y^2=1\}$	À lire ainsi : "l'ensemble des couples (x,y) de coordonnées réelles telles que la somme x^2+y^2 est égale à 1". C'est donc un ensemble de points.
π	Le nombre π qui est défini comme le demi-périmètre du cercle ci-dessus. C'est une constante réelle.
$\{(x,y) \in \mathbb{R}^2 \mid x^2+y^2=r^2\}$	Ce nom désigne le cercle de rayon r et centré sur l'origine. Ici, r est une variable qui prend ses valeurs parmi l'ensemble $\mathbb{R}_+$ des réels positifs.
$f : \mathbb{R} \to \mathbb{R}\,, \quad x \mapsto e^x$	La fonction, nommée f, qui est définie sur $\mathbb{R}$ et qui associe e^x à tout réel x. Ici, la variable "f" désigne donc une fonction.

1.1.2—Noms synonymes et variables muettes

On dit que deux noms sont *synonymes* s'ils désignent le *même* objet. Il y a principalement deux façons d'obtenir des noms synonymes :

1. *Par l'égalité des valeurs.* Par exemple, la fraction $3/2$ s'écrit $1,5$ en base dix. En effet, par définition de l'écriture en base dix, on a $1,5 = 1 + \frac{5}{10} = \frac{3}{2}$. Donc $3/2$ et $1,5$ sont deux noms synonymes.
2. *Par substitution de variable muette.* Exemples :
   a) Le cercle de centre $(0,0)$ et de rayon 1 a été décrit ci-dessus ainsi :
   $$\{(x,y) \in \mathbb{R}^2 \mid x^2+y^2=1\}\,.$$
   Dans cette écriture, les variables x et y sont *muettes*. On peut décider d'utiliser d'autres noms de variables pour les coordonnées, par exemple a et b. L'ensemble de points du plan décrit par l'écriture ci-dessous
   $$\{(a,b) \in \mathbb{R}^2 \mid a^2+b^2=1\}$$

est bien le même que celui décrit avec les variables x et y. On a *substitué* les variables a et b aux variables x et y.

b) La fonction $f : \mathbb{R} \to \mathbb{R}\,, \quad x \mapsto e^x$ qui associe e^x à tout réel x peut aussi bien être décrite en substituant la variable y à la variable x :

$$f : \mathbb{R} \to \mathbb{R}\,, \quad y \mapsto e^y\,.$$

Dans l'écriture ci-dessus, la variable y est donc muette.

c) Fixons-nous un entier naturel n, et intéressons-nous à la somme des carrés des entiers compris entre 1 et n. Notons-la S_n. Par convention, nous avons $S_0 = 0$. Si on connaît la valeur de n, et si cette valeur n'est pas trop grande, mettons $n = 5$, on peut écrire explicitement S_n :

$$S_5 = 1^2 + 2^2 + 3^2 + 4^2 + 5^2.$$

Mais si on ne connaît pas la valeur de n, on utilise souvent des points de suspension, laissant au lecteur le soin de deviner ce qu'on a voulu dire :

$$S_n = 1^2 + 2^2 + \cdots + n^2\,.$$

Le lecteur comprend la démarche : on doit prendre une variable *auxiliaire*, lui affecter successivement toutes les valeurs entre 1 et n, et faire la somme des nombres obtenus. L'écriture avec le signe $\sum$ (*sigma* grec) synthétise cette démarche :

$$S_n = \sum_{i=1}^{n} i^2\,,$$

qui se lit ainsi : "*somme des* i^2 *pour* i *variant de* 1 *à* n". On dit que le signe Σ sur lequel est porté l'indice i est le *mutificateur* de la variable i.

La variable i joue un rôle auxiliaire, et on peut lui substituer n'importe quelle autre variable, disons j, ou k ou même une variable nommée x_1 :

$$S_n = \sum_{j=1}^{n} j^2 = \sum_{k=1}^{n} k^2 = \sum_{x_1=1}^{n} x_1^2\,.$$

d) L'écriture des intégrales utilise aussi des variables muettes :

$$\int_0^1 x^2\,dx\,, \qquad\qquad \int_0^1 y^2\,dy$$

sont deux noms synonymes, obtenus l'un de l'autre par substitution de variable muette. Ici, le mutificateur de x est le signe $\int$ avec le symbole dx à la fin.

e) Question : dans l'exemple du cercle ci-dessus, quel est le signe mutificateur des variables x et y ?

Les variables muettes sont toujours mutifiées par un signe qui leur fait référence. C'est pourquoi une autre appellation est celle de *variable liée*.

À retenir Différents noms peuvent désigner le même objet ; ce sont des noms synonymes. Deux noms sont synonymes soit par l'égalité de leurs valeurs, soit parce qu'on a fait une substitution de variable muette, aussi dite variable liée.

1.1.3—Les variables libres et l'utilisation des opérations

Parmi les noms que nous avons vus dans le premier tableau, certains utilisent aussi des variables qui ne sont pas muettes, et qu'on appelle donc *variables parlantes*. On les appelle aussi *variables libres*.

Par exemple, soit C_r le cercle centré sur l'origine d'un plan repéré par coordonnées cartésiennes, et de rayon r :

$$C_r = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = r^2\}\,.$$

Nous avons donc deux noms pour désigner le même objet :

le symbole "C_r", l'écriture $\{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = r^2\}\,.$

Dans chacun des deux noms, on est obligés de conserver une référence à la variable r. Ici, "r" est une variable parlante, on ne peut pas lui substituer une autre variable arbitrairement, car il n'y pas de raison *a priori* pour que C_r et C_q par exemple désignent le même cercle. En fait, on sait par la géométrie qu'on a $C_r = C_q$ si et seulement si $r = q$. Ainsi, si r et q sont juste des variables dont les valeurs ne sont pas fixées, les deux noms C_r et C_q désignent des objets qui doivent être traités comme non nécessairement égaux.

On peut former de nouveaux noms par des opérations mathématiques portant sur d'autres noms, qui utilisent à la fois des variables muettes et des variables parlantes. Par exemple :

$$x + 2y + \int_0^1 f(3t + y)\,dt\,.$$

Le nom ci-dessus comporte 4 variables, qui sont par ordre d'occurrence : x, y, f et t. Sur cet exemple :

— La variable f désigne une fonction de $[0, 1]$ dans $\mathbb{R}$.
— Les variables x, y et t désignent des réels.
— La variable t est muette, mutifiée par le signe dt de l'intégrale.
— Les trois autres variables, x, y et f sont libres.

À retenir Les noms combinent des variables parlantes (ou libres) et des variables muettes (ou liées). On ne peut pas changer les variables parlantes comme on substitue les variables muettes.

1.1.4—Énoncés mathématiques

Nous avons vu que les noms peuvent être formés en combinant :
— des constantes ;
— des noms de variables parlantes (aussi appelées libres) ;
— des noms de variables muettes (aussi appelées liées) ;
— des opérations mathématiques.

Le travail mathématique consiste à démontrer des affirmations qui portent sur ces noms, à partir d'hypothèses bien précises. À la fois les hypothèses et les affirmations ont la même forme, qui est celle d'*énoncés mathématiques*. On les appelle plus simplement des *énoncés* (à ne pas confondre avec l'énoncé d'un exercice).

Considérons une variable x qui prend ses valeurs dans $\mathbb{R}$. Voici deux énoncés mathématiques très simples :

$$(a)\ 2x^2 - x - 1 = 0\,, \qquad (b)\ x \in \left\{-\frac{1}{2}, 1\right\}.$$

Deux remarques importantes, qui s'appliquent à tous les énoncés qu'on rencontrera :

1. Ces deux énoncés ont un sens, *indépendemment de savoir s'ils sont vrais ou faux.*
2. Ces énoncés sont présentés sous forme de *relations entre différents noms* : une relation d'*égalité* pour l'énoncé (a), et une relation d'*appartenance* pour l'énoncé (b).

Lorsqu'on se fixe un énoncé comme *hypothèse*, c'est qu'on envisage toutes les conséquences qu'on peut en déduire s'il est réalisé. Par exemple, si on prend l'énoncé (b) ci-dessus comme hypothèse, c'est qu'on considère que la variable x est restreinte à prendre ses valeurs uniquement parmi les deux valeurs possibles $-\frac{1}{2}$ ou 1. On peut alors *démontrer* d'autres énoncés à partir de cette hypothèse. Par exemple, il est facile de vérifier la véracité de l'énoncé (a) sous l'hypothèse (b) : il suffit d'examiner les deux cas possibles $x = -\frac{1}{2}$ puis $x = 1$, et de vérifier dans chacun des deux cas que l'équation (a) est satisfaite. On dit que (b) *implique* (a) : (b) est *l'hypothèse*, et (a) est la *conclusion.*

Mais on voit aussi que les rôles d'hypothèse et de conclusion peuvent être inversés, et donc qu'il n'y a pas de différence de nature entre hypothèse et conclusion. Sur cet exemple en effet, on peut aussi démontrer que l'hypothèse (a) implique la conclusion (b), d'après ce qu'on connaît sur la résolution des équations du second degré. Lorsque, comme ici, on a à la fois :

$$(a) \text{ implique } (b) \qquad \text{et} \qquad (b) \text{ implique } (a)\,,$$

on dit que (a) *et* (b) *sont équivalents.*

À retenir Les énoncés mathématiques sont des relations entre des noms, par exemple : inégalité, égalité, appartenance. En partant d'un énoncé comme hypothèse, on démontre d'autres énoncés qui sont des conclusions.

1.2—Les booléens

1.2.1—Valeur de vérité d'un énoncé. Ensemble des booléens

Étant donné un énoncé, on a vu que l'énoncé a un sens indépendemment de savoir s'il est effectivement vérifié ou non. Évidemment, nous sommes intéressés à savoir si l'énoncé est vrai ou non.

Cas des énoncés sans variable libre. Lorsque les énoncés portent sur des noms qui n'ont pas de variable libre, alors cet énoncé a une valeur de vérité qui est bien déterminée. Par exemple, l'énoncé

$$1 = 3$$

est faux. On lui attribue la valeur de vérité Faux.

L'énoncé peut comporter des variables muettes, comme par exemple :

$$\int_0^{2\pi} \cos(2t)\, dt = 0$$

qui est vrai. On attribue à cet énoncé la valeur de vérité Vrai.

L'ensemble à deux éléments $\mathcal{B} = \{\text{Vrai}, \text{Faux}\}$ est appelé *ensemble des booléens.* Chaque énoncé *sans variable libre* a une *valeur de vérité* qui est dans $\mathcal{B}$.

Cas des énoncés avec variables libres. Si un énoncé a une ou plusieurs variables libres, la valeur de vérité de l'énoncé ne peut pas être déterminée *a priori*, puisqu'elle

dépend en général des valeurs des variables libres. Par exemple, l'énoncé suivant a pour variable libre la variable n qui prend ses valeurs dans $\mathbb{N}$:

$$\int_0^{2\pi} \cos(nt)\, dt = 0\,. \tag{1}$$

Sa valeur de vérité dépend des valeurs de l'entier n. En effet, l'énoncé est vrai si $n \neq 0$, mais il est faux si $n = 0$. Sa valeur de vérité ne peut donc pas être déterminée *a priori*.

En revanche : *si on fixe les valeurs des variables libres d'un énoncé, alors sa valeur de vérité est bien déterminée.*

En effet, une fois que les valeurs des variables libres d'un énoncé ont été fixées, alors tout se passe comme si l'énoncé n'avait *plus* de variables libres. On est donc ramené au cas des énoncés sans variable libre, dont on a vu qu'ils avaient une valeur de vérité bien déterminée. Par exemple, si on fixe $n = 2$, alors l'énoncé ci-dessus (1) a la valeur de vérité Vrai.

À retenir On attribue à chaque énoncé mathématique *sans* variable libre une valeur de vérité parmi les deux possibles qui sont Vrai et Faux. Les énoncés *avec* variable libre n'ont de valeur de vérité que lorsque les valeurs des variables libres ont été fixées. L'ensemble $\mathcal{B} = \{\text{Vrai}, \text{Faux}\}$ est appelé ensemble des booléens.

1.2.2—Négation, ET et OU logiques

Supposons donné un énoncé mathématique A. On associe à cet énoncé sa *négation*. C'est un nouvel énoncé qu'on note $\neg A$ (prononcer : *non-A*). Par définition, la valeur de vérité de $\neg A$ est l'opposée de celle de A. On établit donc la table de vérité de la négation :

A	$\neg A$
Vrai	Faux
Faux	Vrai

L'énoncé $\neg A$ a les mêmes variables libres que A. Donc la valeur de vérité de $\neg A$ est fixée une fois que toutes les variables libres de A ont été fixées.

Dans la table de vérité ci-dessus, on avait utilisé la variable A pour désigner un énoncé. On peut aussi "oublier" que A désigne un énoncé, pour ne garder que sa *valeur de vérité*. Ce point de vue revient à considérer A comme une variable ne prenant ses valeurs que parmi l'ensemble $\mathcal{B}$ des *booléens*. Alors la table ci-dessus décrit les valeurs d'une fonction $\neg : \mathcal{B} \to \mathcal{B}$, qui est appelée *négation logique*.

On remarque que l'identité suivante est toujours vérifiée :

$$\neg(\neg A) = A$$

On considère maintenant deux énoncés A et B. Il se peut que A et B aient des variables libres en commun, ce n'est pas gênant. Nous considérons alors les deux nouveaux énoncés

$$A \wedge B \qquad\qquad A \vee B$$

à lire "A ET B" et "A OU B". Par définition :

- $A \wedge B$ prend la valeur Vrai si A et B ont *tous les deux* la valeur Vrai, et prend la valeur Faux si ce n'est pas le cas.
- $A \vee B$ prend la valeur Vrai si *l'un au moins* de A ou de B prend la valeur Vrai, et prend la valeur Faux sinon.

On obtient donc les tables de vérité suivantes :

A	B	$A \wedge B$
Vrai	Vrai	Vrai
Vrai	Faux	Faux
Faux	Vrai	Faux
Faux	Faux	Faux

A	B	$A \vee B$
Vrai	Vrai	Vrai
Vrai	Faux	Vrai
Faux	Vrai	Vrai
Faux	Faux	Faux

On remarque que les identités suivantes sont toujours satisfaites :

(symétrie)	$A \wedge B = B \wedge A$	$A \vee B = B \vee A$
(idempotence)	$A \wedge A = A$	$A \vee A = A$
(lois de de Morgan)	$\neg(A \wedge B) = \neg A \vee \neg B$	$\neg(A \vee B) = \neg A \wedge \neg B$
(distributivité de $\vee$ sur $\wedge$)	$A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C)$	
(distributivité de $\wedge$ sur $\vee$)	$A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C)$	

Par exemple, pour illustrer les deux lois de de Morgan :

1. À quelle condition Paul et Amélie n'ont-ils pas tous les deux un pull-over rouge ? Si au moins l'un des deux n'a pas un pull-over rouge.
2. À quelle condition Paul et Amélie n'ont-ils pas à eux deux au moins un pull-over rouge ? Si aucun des deux n'a un pull-over rouge.

Les variables libres de $A \wedge B$ sont toutes les variables libres qui interviennent au moins une fois dans A ou dans B, et de même pour $A \vee B$. Les valeurs de vérités de $A \wedge B$ et de $A \vee B$ sont donc fixées une fois que toutes les variables libres de A *et* de B ont été fixées.

À retenir On peut combiner les énoncés mathématiques en utilisant les opérations logiques suivantes : la négation logique ($\neg$), le ET logique ($\wedge$) et le OU logique ($\vee$). Les tables de vérité de ces opérations logiques correspondent à l'intuition. Attention cependant : le OU logique est *non exclusif*.

1.2.3—Quantificateurs

De nombreuses propriétés démontrées en mathématiques prennent une forme telle que :

1. Pour tout réel x on a $x^2 \geq 0$.
2. Il existe un réel dont le carré vaut 2.
3. Il n'existe pas de rationnel (c'est-à-dire, une fraction p/q avec p et q entiers) dont le carré vaut 2.
4. Pour tout entier naturel $n \neq 1$, il existe un nombre premier p qui divise n.

Les quatre phrases ci-dessus sont sous une forme mixte entre français et mathématiques. Pour les mettre sous une forme entièrement mathématique, on utilise des *quantificateurs*. Les quantificateurs sont au nombre de deux :

1. Le quantificateur *universel*, noté $\forall$, qu'on lit "quel que soit l'élément" ou "pour tout élément".
2. Le quantificateur *existentiel*, noté $\exists$, qu'on lit "il existe un élément [...] tel que".

Tout quantificateur est obligatoirement suivi d'une variable dont on précise l'appartenance avec le symbole $\in$, qui signifie "élément de".

La variable qui suit le quantificateur est dite *quantifiée*. La première phrase est facile à formaliser dans le langage mathématique :

$$\forall x \in \mathbb{R} \quad x^2 \geq 0\,, \tag{2}$$

qu'on peut traduire ainsi, en mettant en gras la traduction du quantificateur : ***Pour tout élément*** x *de* $\mathbb{R}$*, l'énoncé "*$x^2 \geq 0$*" est vrai.*

La deuxième phrase n'est pas difficile non plus :

$$\exists x \in \mathbb{R} \quad x^2 = 2, \tag{3}$$

qu'on peut traduire ainsi : ***Il existe un élément*** x *de* $\mathbb{R}$ ***tel que*** *l'énoncé "*$x^2 = 2$*" est vrai.*

Les deux énoncés ci-dessus, qu'on a numérotés (2) et (3), sont appelés des énoncés *quantifiés* à cause de la présence de quantificateurs. On reconnaît à l'intérieur de ces énoncés quantifiés des énoncés qui ne sont pas quantifiés : $x^2 \geq 0$, et $x^2 = 2$. En particulier, ces sous-énoncés contiennent chacun la variable *parlante* x.

Cependant, dans les énoncés quantifiés (2) et (3), la variable x est visiblement *muette*. En effet, dire "le carré de tout réel x est positif", ou en substituant la variable y à la variable x : "le carré de tout réel y est positif", c'est dire deux fois la même chose. De même, dire "il existe un réel x dont le carré vaut 2", ou dire "il existe un réel y dont le carré vaut 2", c'est dire deux fois la même chose. On reconnaît donc que les quantificateurs ont *une action mutificatrice sur les variables qu'ils quantifient.*

Cette propriété importante des quantificateurs peut se reformuler ainsi : *dans un énoncé quantifié, la variable sur laquelle porte le quantificateur est muette.*

Exercice Donner la formulation entièrement mathématique de la phrase 3 ci-dessus en utilisant le symbole $\mathbb{Q}$ de l'ensemble des nombres rationnels. Même question en n'utilisant pas le symbole $\mathbb{Q}$, mais seulement le symbole $\mathbb{Z}$ de l'ensemble des nombres entiers relatifs.

Exercice Donner la formulation entièrement mathématique de la phrase 4 ci-dessus. Commencer par exprimer les énoncés suivants, en utilisant le symbole $\mathbb{Z}$ pour l'ensemble des nombres entiers relatifs :

1. Deux variables parlantes n et m à valeurs dans $\mathbb{Z}$, et introduire une variable muette : "n est un diviseur de m".
2. (À faire quand vous aurez vu l'implication logique). Une variable parlante p à valeurs entières : "p est un nombre premier".

Les *valeurs de vérité* des énoncés qui comportent des quantificateurs sont définies de la façon suivante :

1. Quantificateur universel $\forall$. Tout énoncé A qui commence par $\forall$ est de la forme :

   $$A = \text{“}\forall x \in W \quad B\text{”}\,,$$

   où W est un ensemble et B est un énoncé qui contient éventuellement x comme variable *parlante*. On décide que la valeur de vérité de A est Vrai si celle de B est Vrai, *pour toutes les valeurs de* x *dans* W. Exemples :

   a) L'énoncé : "$\forall x \in \mathbb{R} \quad x^2 \geq 0$" a la valeur Vrai puisque l'énoncé $x^2 \geq 0$ est vrai quel que soit la valeur du réel x.

   b) L'énoncé : "$\forall x \in \mathbb{R} \quad x^2 \geq 1$" a la valeur Faux puisque l'énoncé $x^2 \geq 1$ n'est pas vrai pour toutes les valeurs du réel x. En effet, pour $x = 0$, l'énoncé $x^2 \geq 1$ a la valeur Faux.

2. Quantificateur existentiel $\exists$. Tout énoncé A qui commence par $\exists$ est de la forme :

$$A = \text{“}\exists x \in W \quad B\text{”}\,,$$

où W est un ensemble et B est un énoncé qui contient éventuellement x comme variable *parlante*. On décide que la valeur de vérité de A est Vrai si celle de B est Vrai pour *au moins une valeur de x dans W*. Exemples :

a) L'énoncé : “$\exists x \in \mathbb{R} \quad x^2 = 2$” a pour valeur de vérité Vrai. En effet, on sait qu'il existe un réel, qu'on note $\sqrt{2}$, qui a pour propriété que son carré vaut 2.

b) L'énoncé : “$\exists x \in \mathbb{Q} \quad x^2 = 2$” a pour valeur de vérité Faux. En effet, on sait qu'il n'existe pas de rationnel dont le carré vaut 2.

Exercice Traduire en français les deux énoncés suivants, et donner leur valeur de vérité :

$$\forall x \in \mathbb{R} \quad \exists y \in \mathbb{R} \quad x < y$$
$$\exists y \in \mathbb{R} \quad \forall x \in \mathbb{R} \quad x < y$$

Exercice Soit A un énoncé qui ne comporte qu'une seule variable parlante a, qui ne peut prendre que deux valeurs, a_1 ou a_2.

Soit A_1 l'énoncé A où on a fixé $a = a_1$ et soit A_2 l'énoncé A où on a fixé $a = a_2$. Montrer que les énoncés suivants ont les mêmes valeurs de vérité :

$$\forall a \in \{a_1, a_2\} \;\; A \qquad \text{et} \qquad A_1 \wedge A_2$$
$$\exists a \in \{a_1, a_2\} \;\; A \qquad \text{et} \qquad A_1 \vee A_2$$

À retenir Les quantificateurs logiques universel et existentiel sont toujours suivis d'une variable avec une appartenance à un ensemble. Cette variable est mutifiée par le quantificateur.

1.2.4—Implication logique

L'*implication logique*, qui est notée $\implies$ et qui se lit “*implique*”, est un connecteur logique, au même titre que les connecteurs logiques $\wedge$ et $\vee$ déjà vus. Il connecte deux énoncés pour en produire un nouveau. Voici un exemple, où x est une variable libre qui prend ses valeurs dans $\mathbb{R}$:

$$x \geq 1 \implies x^2 \geq 1\,, \tag{4}$$

à lire : “x plus grand que 1 implique x^2 plus grand que 1”. C'est toute cette phrase qui constitue l'énoncé (4).

Appelons $C(x)$ l'énoncé (4), et décomposons-le sous la forme :

$$C(x) = \text{“}A(x) \implies B(x)\text{”}\,, \qquad \text{avec } A(x) = \text{“}x \geq 1\text{”} \qquad \text{et } B(x) = \text{“}x^2 \geq 1\text{”}$$

En affirmant la véracité de $A(x) \implies B(x)$, on n'affirme ni la véracité de $A(x)$, ni celle de $B(x)$. En revanche, on affirme la chose suivante :

Si $A(x)$ est vrai, alors $B(x)$ est vrai.

En particulier, l'énoncé $C(x)$ *ne se prononce pas sur la véracité de $B(x)$ dans le cas où $A(x)$ est faux*. Par convention, l'implication $A(x) \implies B(x)$ a la valeur de vérité Vrai dès que $A(x)$ a la valeur de vérité Faux, quelle que soit la valeur de vérité de $B(x)$.

Dans notre exemple, l'énoncé $A(x)$ a la valeur Faux pour tous les x de l'intervalle $]-\infty, 1[$. Donc l'énoncé $C(x)$ a automatiquement la valeur Vrai pour ces valeurs de x. Voici les valeurs de vérité de $A(x)$, $B(x)$ et $C(x)$ pour les réels x de l'intervalle $]-\infty, 1[$:

	$A(x)$	$B(x)$	$C(x)$
$x \in]-\infty, -1]$	Faux	Vrai	Vrai
$x \in]-1, 1[$	Faux	Faux	Vrai

Le véritable travail mathématique pour démontrer l'implication $A(x) \implies B(x)$ ne s'intéresse pas aux valeurs de x pour lesquelles $A(x)$ est faux, puisque dans ce cas, comme on vient de le voir, l'énoncé $A(x) \implies B(x)$ a conventionnellement la valeur de vérité Vrai. Le travail consiste au contraire à : 1° considérer les réels x pour lesquels $A(x)$ est vrai, 2° démontrer que l'énoncé $B(x)$ est vrai avec cette hypothèse supplémentaire sur x. Faisons-le pour l'exemple (4) :

1. *Supposition :* On suppose $x \geq 1$ (noter qu'on ne cherche pas à le démontrer).
2. *Démonstration :* En particulier, $x \geq 0$, et on peut donc multiplier les deux membres de l'inégalité $x \geq 1$ par x : on obtient $x^2 \geq x$. Comme $x \geq 1$ d'après l'hypothèse $A(x)$, on en déduit $x^2 \geq 1$, qui est l'énoncé $B(x)$.
3. *Conclusion :* On vient de *démontrer* $B(x)$ *sous l'hypothèse* $A(x)$: c'est donc qu'on a la validité de l'implication $A(x) \implies B(x)$.

Une façon de comprendre l'implication logique est la suivante : pour que l'implication $A(x) \implies B(x)$ soit prise en défaut, il faut trouver un *flagrant délit de non implication*, c'est-à-dire une valeur de x pour laquelle :

$$A(x) \text{ est vrai, } \textit{et pourtant } B(x) \text{ n'est pas vrai.}$$

Cette remarque nous donne une formulation logique de la négation de l'implication, qui est intuitive et facile à retenir :

$$\neg(A \implies B) = A \wedge (\neg B).$$

Appliquons l'opération de négation aux deux membres de l'équation logique ci-dessus. On obtient :

$$\begin{aligned} (A \implies B) &= \neg(A \wedge (\neg B)) \\ &= \neg A \vee (\neg(\neg B)) && \text{d'après la loi de de Morgan} \\ &= \neg A \vee B && \text{car } \neg(\neg B) = B \end{aligned}$$

On retiendra la formule suivante :

$$\boxed{(A \implies B) = \neg A \vee B}$$

On en déduit la formule :

$$\boxed{(A \implies B) = (\neg B \implies \neg A)}$$

L'énoncé $\neg B \implies \neg A$ s'appelle la *contraposée* de l'énoncé $A \implies B$. Pour démontrer l'égalité des valeurs de vérité de $A \implies B$ et de sa contraposée, on écrit :

$$\begin{aligned} (\neg B \implies \neg A) &= \neg(\neg B) \vee (\neg A) \\ &= \neg A \vee B \\ &= (A \implies B) \end{aligned}$$

Finalement, on obtient aussi la table de vérité de $A \implies B$:

A	B	$A \implies B$
Vrai	Vrai	Vrai
Vrai	Faux	Faux
Faux	X	Vrai

Exercice Soit A et B deux booléens. Montrer que $(A \implies \neg B)$ et $\neg(A \wedge B)$ ont même valeur de vérité.

Exercice Étant donné un ensemble W, comparer les valeurs de vérité des énoncés (a) et (b) suivants :

$$(a)\ \forall x \in W \quad (A(x) \implies B(x)), \qquad (b)\ (\forall x \in W \quad A(x)) \implies (\forall x \in W \quad B(x))$$
$$(a)\ \exists x \in W \quad (A(x) \implies B(x)), \qquad (b)\ (\exists x \in W \quad A(x)) \implies (\exists x \in W \quad B(x))$$

À retenir L'implication logique est un connecteur logique noté $\implies$ dont la valeur de vérité est donnée par $(A \implies B) = (\neg A \vee B)$. La contraposée $\neg B \implies \neg A$ a la même valeur de vérité que $A \implies B$. Si $A \implies B$ est vraie, on ne peut rien dire de la valeur de vérité ni de A ni de B.

1.2.5—Équivalence logique

Nous avons déjà vu que deux énoncés A et B sont dits équivalents dans le cas où, en supposant A, on peut démontrer B, et en supposant B, on peut démontrer A. Avec le langage de l'implication logique, on reformule donc l'équivalence comme un nouveau connecteur logique, noté $\iff$, tel que l'énoncé $A \iff B$ a la même valeur de vérité que l'énoncé suivant :

$$(A \implies B) \wedge (B \implies A).$$

On établit la table de vérité de $A \iff B$ en croisant la table de vérité de $A \implies B$ avec celle de $B \implies A$, et en utilisant la table de vérité du connecteur $\wedge$:

A	B	$A \iff B$
Vrai	Vrai	Vrai
Vrai	Faux	Faux
Faux	Vrai	Faux
Faux	Faux	Vrai

Évidemment, si A et B sont des constantes logiques, la question de l'équivalence $A \iff B$ n'est pas spécialement intéressante. Elle ne devient intéressante que dans le cas où les énoncés A et B contiennent en fait des variables, parlantes ou muettes : voir les exercices ci-dessous.

Exercice Pour les énoncés suivants A et B, 1° démontrer l'implication $A \implies B$ quelles que soient les valeurs des variables libres, 2° déterminer toutes les valeurs des variables libres pour lesquelles l'équivalence $A \iff B$ a lieu.

Variables libres	A	B
$x \in \mathbb{R}$	$x \geq 1$	$x^2 \geq 1$
$m \in \mathbb{R}$	$\forall x \in \mathbb{R} \quad mx \geq 0$	$m = 0$
$n \in \mathbb{Z}$	n est pair	n^2 est pair
$n \in \mathbb{Z},\ m \in \mathbb{Z}$	n est pair	$n + 2m$ est pair

Exercice Étant donné un ensemble W, comparer les valeurs de vérité des énoncés (a) et (b) suivants :

$$(a)\ \forall x \in W \quad (A(x) \iff B(x)), \qquad (b)\ (\forall x \in W \quad A(x)) \iff (\forall x \in W \quad B(x))$$
$$(a)\ \exists x \in W \quad (A(x) \iff B(x)), \qquad (b)\ (\exists x \in W \quad A(x)) \iff (\exists x \in W \quad B(x))$$

1.2.6—Tautologies

Définition. *Une tautologie est une formule logique composée de variables prenant leurs valeurs dans l'ensemble des booléens et des connecteurs logiques* $\neg$, $\vee$, $\wedge$, $\implies$, $\iff$, *et qui a toujours la valeur vraie, quelles que soient les valeurs des différentes variables.*

Un exemple de tautologie est la formule suivante :

$$(A \implies B) \iff (\neg A \implies \neg B)$$

En effet, on sait que les deux membres de part et d'autre du signe $\iff$ ont toujours même valeur de vérité. Donc les deux membres sont bien équivalents logiquement.

Voici un exemple de formule qui n'est pas une tautologie :

$$(A \implies B) \implies (B \implies A)$$

Pour montrer que cette formule, appelons-la F, n'est pas une tautologie, il faut trouver un assignement des valeurs de A et de B pour lequel la formule est fausse. Et en effet, en fixant $A = \mathsf{Faux}$ et $B = \mathsf{Vrai}$, nous avons $A \implies B = \mathsf{Vrai}$ et $B \implies A = \mathsf{Faux}$ donc $F = \mathsf{Faux}$, ce qui montre que F n'est pas une tautologie.

Au cours d'une démonstration mathématique, l'utilisation d'une tautologie logique permet de clarifier la rédaction. Ainsi, dire "Je vais démontrer l'implication demandée par la contraposée" fait appel à la tautologie $(A \implies B) \iff (\neg B \implies \neg A)$. La nature des objets mathematiques qui sont le sujet des énoncés A et B n'entre aucunement en considération pour cela. Ainsi on sépare bien l'utilisation de la logique pure, de l'étude des propriétés mathématiques des objets.

Comment montrer qu'une formule est une tautologie ? Une méthode qui fonctionne *a priori* quelle que soit la tautologie est d'établir la table de vérité de la formule qu'on cherche à étudier. Comme chaque variable de la formule peut prendre les deux valeurs Vrai ou Faux, l'examen de tous les assignements possibles nécessitera d'écrire une table avec 2^n lignes, où n est le nombre de variables de la formule. Établir la table de vérité d'une formule est donc une tâche rapidement fastidieuse.

Il est souvent plus commode d'utiliser les propriétés des connecteurs logiques qu'on a vues précédemment : définition de l'implication, loi de de Morgan, distributivité, etc (*cf.* ci-dessus).

Exemple. *Montrer que la formule suivante est une tautologie :*

$$(A \implies (B \vee C)) \implies ((A \implies B) \vee (A \implies C))$$

Rappelons qu'une implication $X \implies Y$ est vraie dès que X est faux, il suffit donc d'étudier le cas où X est vrai. Ici, on suppose donc que $X = (A \implies (B \vee C))$ est vraie, et on cherche à montrer que $Y = ((A \implies B) \vee (A \implies C))$ est vrai.

Distinguons les deux cas $A = \mathsf{Vrai}$ et $A = \mathsf{Faux}$. Si $A = \mathsf{Faux}$, alors les deux implications $A \implies B$ et $A \implies C$ sont vraies, donc $Y = \mathsf{Vrai}$ et $F = \mathsf{Vrai}$.

Si $A = \mathsf{Vrai}$, alors comme l'implication X est vraie par hypothèse, nous avons $B \vee C = \mathsf{Vrai}$, donc l'un au moins de B ou de C est vraie. Donc l'implication correspondante $A \implies B$ ou $A \implies C$ est vraie, donc $Y = \mathsf{Vrai}$ et $(X \implies Y) = \mathsf{Vrai}$.

On a montré que $X \implies Y$ est vrai, et ceci quelles que soient les valeurs des variables booléennes A, B et C. Donc $X \implies Y$ est une tautologie, ce qu'on voulait montrer. □

On aurait pu établir la table de vérité de la formule, en prenant soin de considérer les $2^3 = 8$ possibilités pour les valeurs des variables A, B et C.

A	B	C	$B \vee C$	$A \implies (B \vee C)$	$A \implies B$	$A \implies C$	$(A \implies B) \vee (A \implies C)$	F
Vrai	Vrai	Vrai	Vrai	Vrai	Vrai	Vrai	Vrai	Vrai
Vrai	Vrai	Faux	Vrai	Vrai	Vrai	Faux	Vrai	Vrai
Vrai	Faux	Vrai	Vrai	Vrai	Faux	Vrai	Vrai	Vrai
Vrai	Faux	Faux	Faux	Faux	Faux	Faux	Faux	Vrai
Faux	Vrai	Vrai	Vrai	Vrai	Vrai	Vrai	Vrai	Vrai
Faux	Vrai	Faux	Vrai	Vrai	Vrai	Vrai	Vrai	Vrai
Faux	Faux	Vrai	Vrai	Vrai	Vrai	Vrai	Vrai	Vrai
Faux	Faux	Faux	Faux	Vrai	Vrai	Vrai	Vrai	Vrai

On constate que la formule F prend toujours la valeur Vrai, donc c'est une tautologie.

Exercice Vérifier que les formules suivantes sont des tautologies :

$$(A \implies (B \wedge C)) \iff (A \implies B) \wedge (A \implies C)$$
$$(A \vee B) \implies C \iff (A \implies C) \wedge (B \implies C)$$

À retenir Une tautologie est une formule logique qui est vrai quelles que soient les valeurs de ses variables. On peut montrer qu'une formule est une tautologie soit en établissant sa table de vérité, soit en utilisant les propriétés des connecteurs logiques.

1.2.7—Composition des opérations logiques et des quantificateurs

On a déjà vu que la négation logique échange les opérateurs $\wedge$ et $\vee$: ce sont les lois de de Morgan. Ces lois s'étendent aux quantificateurs en échangeant le rôle de "$\forall$" et $\exists$", comme illustré dans le tableau ci-dessous.

Énoncé à la forme affirmative	Traduction de la négation de l'énoncé
$(\forall x \in U \quad A(x))$	$(\exists x \in U \quad \neg A(x))$
$(\exists x \in U \quad A(x))$	$(\forall x \in U \quad \neg A(x))$

Quelques remarques :

1. L'ensemble U dans lequel varie la variable muette x est bien *toujours le même* !
2. La négation de "Tous les ballons sont rouges" est bien "Il existe un ballon qui n'est pas rouge", et non pas "Aucun ballon n'est rouge". C'est le sens de l'échange des quantificateurs par la négation.
3. Le quantificateur $\forall$ peut être vu comme une généralisation du connecteur ET. Par exemple, vérifier que l'énoncé "$\forall x \in U \quad A(x)$" est vraie, c'est comme vérifier un ET logique qui court sur l'ensemble de ces valeurs ; et *idem* pour le quantificateur "$\exists$" qui généralise le connecteur OU. Il n'est donc pas surprenant que les règles de négation ci-dessus généralisent les règles de de Morgan.

Les énoncés mathématiques peuvent comporter plusieurs quantificateurs. Par exemple :

$$\forall x \in \mathbb{R} \quad \exists y \in \mathbb{R} \quad x < y$$

Cet énoncé affirme que, si on fixe un réel x, alors il existe un réel y qui lui est strictement supérieur. Cet énoncé sans variable libre est évidemment vrai.

Examinons le statut de l'énoncé obtenu en échangeant la place des deux quantificateurs, existentiel et universel :

$$\exists y \in \mathbb{R} \quad \forall x \in \mathbb{R} \quad x < y$$

Cet énoncé, toujours sans variable libre, affirme qu'il existe un réel y qui est plus grand que tous les réels. Cet énoncé est évidemment faux. On en déduit que des énoncés obtenus en échangeant la place de $\forall$ et de $\exists$ ne sont pas équivalents en général.

En revanche, on peut toujours échanger deux quantificateurs identiques consécutifs : la formule obtenue est équivalente à celle d'origine. Considérons par exemple l'énoncé suivant :

$$\exists x \in \mathbb{Z} \quad \exists y \in \mathbb{Z} \quad \exists z \in \mathbb{Z} \quad z^2 = x^2 + y^2$$

Cet énoncé affirme qu'on peut choisir un entier x, puis un entier y, puis un entier z, de telle sorte que le triplet (x, y, z) soit solution de $z^2 = x^2 + y^2$. Il est évident que l'ordre dans lequel on a décidé de sélectionner les variables n'intervient pas *in fine* sur l'existence du triplet solution.

Exercice Un nombre $n \in \mathbb{N}$ est dit *premier* s'il vérifie :

$$(n \neq 1) \wedge \big(\forall k \in \mathbb{N} \quad ((\exists j \in \mathbb{N} \quad n = kj) \implies (k = 1 \vee k = n))\big)$$

Exprimer avec des quantificateurs et des connecteurs logiques la propriété pour un nombre de *ne pas être premier*. Expliquer pourquoi la propriété trouvée est bien vérifiée par exemple pour $n = 4$.

Exercice Soit U et V deux ensembles, et soit $P(x, y)$ un énoncé ayant seulement x et y comme variables libre, avec x variant dans U et y variant dans V. Montrer que les deux énoncés suivants ont même valeur de vérité : $\big(\forall x \in U \quad \forall y \in V \quad P(x, y)\big)$ et $\big(\forall y \in V \quad \forall x \in U \quad P(x, y)\big)$.

À retenir La négation échange les quantificateurs universel et existentiel, ce qui généralise les lois de de Morgan. On ne peut pas échanger les places de deux quantificateurs de types différents, l'un existentiel et l'autre universel. Mais on peut échanger les places de deux quantificateurs s'ils sont de même type et consécutifs dans une formule, sans changer sa valeur de vérité.

2—Ensembles et opérations sur les ensembles

On va décrire ici la notion d'ensemble en partant de la notion de *relation d'appartenance*, considéree comme primitive.

2.1—Appartenance. Définition extensive d'un ensemble

Décrivons informellement deux idées-clefs qui sous-tendent la notion d'ensemble ; puis nous verrons la forme mathématique que prennent ces deux idées.

1. Chaque ensemble est une *boîte* pouvant contenir n'importe quels objets, de toute nature et sans limite de place.
2. Chaque boîte-ensemble est étiquetée par son contenu. Il y a donc autant de boîtes que de contenus possibles différents.

Mathématiquement, on a des objets mathématiques appelés *ensembles*, et une relation dite *relation d'appartenance* notée "$a \in B$" et qui se lit de manière équivalente :

"a appartient à B" ou "a est un élément de B" ou "B contient a"

Ceci traduit l'idée 1. On traduit la deuxième idée en disant que *deux ensembles sont égaux si et seulement si ils ont les mêmes éléments.*

À retenir Un ensemble est une "boîte" contenant des objets mathématiques, et qui est entièrement identifiée par son contenu, c'est-à-dire par les objets que cette boîte contient.

Puisqu'un ensemble est identifié par les objets qu'il contient, le plus simple pour construire des ensembles est d'énumérer des collections d'objets. On utilise la notation suivante : on met entre accolades tous les éléments de l'ensemble, et on les sépare par des virgules. Par exemple : $\{1, 2, 3\}$ est l'ensemble qui contient les éléments 1, 2 et 3. Cette description est appelée *définition extensive* de l'ensemble.

Notez que *l'ordre des éléments ne compte pas.* Par exemple :

$$\{1, 2, 3\} = \{1, 3, 2\}$$

Par convention, on ne répète jamais un même élément : le symbole $\{1, 1\}$ n'a pas de sens.

Enfin, le symbole $\emptyset$ désigne l'ensemble qui ne contient aucun objet. Cet ensemble est appelé *ensemble vide.*

À retenir La définition extensive d'un ensemble consiste à faire la liste de tous les éléments qu'il contient, sans répétition et sans tenir compte de l'ordre.

2.2—Inclusion et ensemble des parties d'un ensemble

Définition. *On dit qu'un ensemble A est une* partie *d'un ensemble B si tous les éléments de A sont éléments de B. On le note ainsi : $A \subseteq B$. On a donc :*

$$(A \subseteq B) \iff (\forall x \in A \quad x \in B)$$

De manière synonyme, on dit que A est un *sous-ensemble* de B, ou que A est *inclus* dans B, ou que A est *contenu* dans B.

Nous avons deux remarques immédiates.

1. Puisque deux ensembles sont égaux si et seulement si ils ont les mêmes éléments, l'égalité de deux ensembles se décompose comme une double inclusion :

$$A = B \iff (A \subseteq B \wedge B \subseteq A).$$

2. Si A est un ensemble, il y a toujours parmi ses parties au moins $\emptyset$ et lui-même :

$$\emptyset \subseteq A \qquad\qquad A \subseteq A.$$

Si on se donne un ensemble "petit", par exemple $A = \{1, 2, 3\}$, on peut facilement trouver toutes ses parties :

$$\emptyset, \quad \{1\}, \quad \{2\}, \quad \{3\}, \quad \{1, 2\}, \quad \{1, 3\}, \quad \{2, 3\}, \quad \{1, 2, 3\}$$

Définition. *On appelle* ensemble des parties d'un ensemble A*, et on note* $\mathcal{P}(A)$*, l'ensemble dont les éléments sont tous les sous-ensembles de* A*.*

Ainsi, les éléments de $\mathcal{P}(A)$ sont eux-mêmes des ensembles. On peut encore utiliser la notation avec des accolades pour décrire $\mathcal{P}(A)$ si A n'est pas trops gros. Ainsi, pour l'exemple précédent avec $A = \{1, 2, 3\}$, on a :

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

Conceptuellement, on ne fait pas de différence entre les ensembles finis et les ensembles infinis. On peut donc parler de l'ensembles des parties d'un ensemble infini tel que $\mathbb{N}$ ou $\mathbb{R}$. En fait, en arrivant en Licence, on a déjà été fortement habitué à manipuler des parties d'ensembles infinis. Par exemple, en géométrie, on considère les droites d'un plan donné, et chaque droite est bien elle-même une partie de ce plan. Ou bien on considère l'ensemble $\mathbb{R}$ des nombres réels, et on étudie certaines de ses parties comme $\mathbb{N}$, $\mathbb{Z}$ ou $\mathbb{Q}$.

De façon générale, on a donc un "gros ensemble" qui sert de cadre, et tous les ensembles sur lesquels on raisonne en sont des sous-ensembles. C'est ce cadre extrèmement général qui sera suffisant pour toutes les mathématiques de la Licence. Dans ce cadre, il est facile d'utiliser les quantificateurs logiques pour traduire les propriétés des ensembles. Voici un exemple. Soit U un ensemble, et A et B deux parties de U. Alors (exercice) :

$$A = B \iff (\forall x \in U \quad x \in A \iff x \in B)$$

À retenir Les parties de A sont les ensembles qui sont inclus dans A. Les parties de A sont regroupées dans l'ensemble des parties de A, qui est un nouvel ensemble noté $\mathcal{P}(A)$. Les éléments de $\mathcal{P}(A)$ sont les ensembles inclus dans A.

2.3—Définition d'un ensemble par compréhension

Nous avons vu une première façon de décrire un ensemble : par l'énumération de ses éléments. Une deuxième façon, extrèmement utile en pratique, est la définition par *compréhension.*

Un exemple typique est l'ensemble des entiers naturels pairs. Pour le définir, on considère d'abord l'ensemble $\mathbb{N}$ de tous les entiers naturels. Puis on sélectionne parmi ceux-ci tous ceux qui ont la propriété qui nous intéresse, ici la parité. On le note de la façon suivante, qui diffère de la notation en extension bien qu'on utilise aussi les accolades :

$\{x \in \mathbb{N} \mid x \text{ est pair}\}$ à lire : l'ensemble des x de $\mathbb{N}$ tels que : "x est pair"

Cette démarche est très générale, et se résume ainsi : *étant donné un ensemble* U *et étant donné un énoncé* $\Phi(x)$ *ayant une seule variable libre prenant ses valeurs dans* U*, on note :*

$$U_\Phi = \{x \in U \mid \Phi(x)\}$$

l'ensemble des éléments de U pour lesquels $\Phi(x)$ est vrai. C'est donc une partie de U.

Ce type de définition d'un ensemble vous est en fait très familier. Par exemeple, une droite donnée par son équation est de ce type :

$$D = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid ax + by + c = 0\}$$

Ici, Φ s'applique au couple (x, y), et est donnée par l'énoncé $ax + by + c = 0$. Pour un autre exemple, le cercle C dans un plan P, de centre O et de rayon r est défini par $C = \{M \in P \mid d(O, M) = r\}$. Dans ce cas, la formule Φ s'applique au point M et est donnée par l'énoncé $d(O, M) = r$.

Quelques remarques :

1. La définition qu'on a donnée de U_Φ utilise une variable muette. Donc la construction $\{\bullet \in U \mid \cdots\}$ *mutifie* la variable qui apparaît en premier, à la place de $\bullet$. Nous pouvons donc substituer une autre variable muette, et on décrit le même ensemble :

$$U_\Phi = \{y \in U \mid \Phi(y)\}$$

2. Les relations logiques entre énoncés Φ se traduisent par des relations entre ensembles U_Φ , de la façon suivante (exercice) :
   a) Si $\forall x \in U \quad \Phi(x) = \mathsf{Faux}$, alors $U_\Phi = \emptyset$
   b) Si $\forall x \in U \quad \Phi(x) = \mathsf{Vrai}$, alors $U_\Phi = U$
   c) Soit Φ et Ψ deux énoncés avec x comme variable libre, prenant ses valeurs dans U. Alors :

$$\begin{aligned} (\forall x \in U \quad \Phi(x) &\implies \Psi(x)) &&\iff U_\Phi \subseteq U_\Psi \\ (\forall x \in U \quad \Phi(x) &\iff \Psi(x)) &&\iff U_\Phi = U_\Psi \end{aligned}$$

3. L'ensemble U joue un rôle fondamental. Il serait tentant, étant donné un énoncé Φ ayant une variable libre x, de considérer "l'ensemble des x satisfaisant $\Phi(x)$". En fait, on ne peut pas donner de sens à un tel ensemble. C'est le sujet du célèbre *paradoxe de Russel* illustré dans l'encadré 2.1, qui est indiqué à titre de complément.

La définition des ensembles par compréhension est implicitement utilisée pour définir de nombreux ensembles familiers. Par exemple l'intervalle $[1, 3]$ correspond à la propriété $1 \leq x \leq 3$ pour un nombre réel x. On a donc :

$$[1, 3] = \{x \in \mathbb{R} \mid 1 \leq x \leq 3\}$$

On peut parfois utiliser des points de suspension à la place de la variable muette. Par exemple :

$$\{1, 2, \ldots, k\} = \{x \in \mathbb{N} \mid 1 \leq x \leq k\}.$$

En voyant la notation du membre de gauche, il faut comprendre que cette notation renvoie à une définition par compréhension, qui est celle explicitée dans le membre de droite.

Enfin, insitons sur l'importance d'une utilisation rigoureuse de la notation pour un ensemble défini par compréhension : chaque symbole a place et une signification précises.

Supposons que, pour tout énoncé $\Phi(x)$, il existe un ensemble constitué de tous les objets x pour lesquels $\Phi(x)$ est vrai, sans restriction ; on noterait naturellement un tel ensemble de la façon suivante : $\{x \mid \Phi(x)\}$. Prenons alors pour $\Phi(x)$ l'énoncé $x \notin x$, et posons $B = \{x \mid x \notin x\}$.

Le problème surgit lorsqu'on se pose la question « est-ce que $B \in B$? » :

— si la réponse est oui (c'est à dire que $B \in B$), alors B doit satisfaire la propriété caractéristique des éléments de B, c'est-à-dire qu'on doit avoir $B \notin B$;

— si la réponse est non (c'est à dire que $B \notin B$), alors c'est que B ne satisfait pas la propriété caractéristique des éléments de B, donc $B \notin B$ est faux et on a $B \in B$.

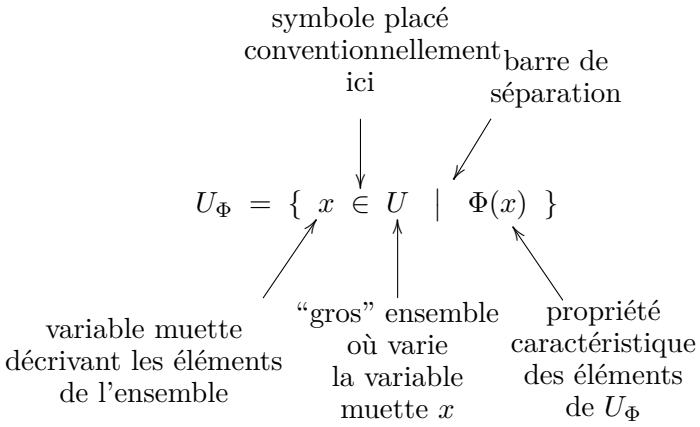
En conclusion, on a $B \in B$ si et seulement si $B \notin B$, ce qui est contradictoire.

On en déduit que la notion d'ensemble ne permet pas de définir *sans restriction* la collection des objets qui satisfont un énoncé donné.

Dans la pratique, ce n'est pas un problème : on s'intéresse à l'ensemble des *nombres* vérifiant une certaine propriété, à l'ensemble des *fonctions* $\mathbb{R} \to \mathbb{R}$ vérifiant une certaine propriété, etc. Ainsi, on travaille toujours parmi les éléments d'un "gros" ensemble, et ceci évite les problèmes comme ceux soulevés par le paradoxe de Russel.

ENCADRÉ 2.1 – À propos du paradoxe de Russell. Bertrand Russel (1872-1970) : philosophe et mathématicien anglais.

Revoyons-les à nouveau :



À retenir Étant donnés un ensemble U et un énoncé $\Phi(x)$ portant sur les éléments de U, la définition par compréhension $\{x \in U \mid \Phi(x)\}$ définit la partie de U constituée des éléments de U vérifiant la propriété $\Phi(x)$. La notation utilise une variable muette.

2.4—Couples et produit cartésien

Définition. *Soit A et B deux ensembles. Pour chaque élément a de A et pour chaque élément b de B, on peut former le* couple (a, b). *L'ensemble des couples ainsi formés est appelé le* produit cartésien *de A et de B, et on le note $A \times B$.*

Les couples ont la propriété fondamentale suivante : $(a, b) = (a', b')$ si et seulement si $a = a'$ et $b = b'$. En particulier, les couples (a, b) et (b, a) diffèrent, sauf si $a = b$.

Il est utile de penser au produit cartésien $A \times B$ comme à un ensemble "rectangulaire". Ses éléments correspondent à des coordonnées généralisées, l'une indexée par A et l'autre indexée par B. Le point important est qu'il n'y a pas de contrainte d'une coordonnée sur

l'autre, puisque étant donné $a \in A$ ou $a' \in A$, toutes les paires correspondantes (a, b) et (a', b) sont autorisées.

On utilise souvent la définition par compréhension pour rajouter des contraintes. Par exemple, soit le cercle :

$$C = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x^2 + y^2 = 1\}.$$

Si $|x| > 1$, il n'y a pas de y tel que $(x, y) \in C$. Si $|x| = 1$ il y a seulement $y = 0$ tel que $(x, y) \in C$, et si $|x| < 1$ il y a deux éléments distincts $y = \pm\sqrt{1 - x^2}$ tels que $(x, y) \in C$.

On note souvent A^2 au lieu de $A \times A$.

À retenir Le produit cartésien $A \times B$ de deux ensemble A et B est l'ensemble des couples qu'on peut former à partir d'éléments de A et de B.

2.5—Union et intersection. Passage au complémentaire

Définition. *Soit A et B deux ensembles.* L'union *de A et B est l'ensemble des éléments qui appartiennent à A ou à B, on le note $A \cup B$.* L'intersection *de A et de B est l'ensemble des éléments qui appartiennent à A et à B, on le note $A \cap B$.*

Proposition. *Quels que soient les ensembles A, B et C, les énoncés suivants sont vrais :*

$$\begin{aligned} A \cup A &= A & A \cap A &= A \\ A \cup \emptyset &= A & A \cap \emptyset &= \emptyset \\ A \cup B &= B \cup A & A \cap B &= B \cap A \\ (A \cup B) \cup C &= A \cup (B \cup C) & (A \cap B) \cap C &= A \cap (B \cap C) \\ A \cap (B \cup C) &= (A \cap B) \cup (A \cap C) & A \cup (B \cap C) &= (A \cup B) \cap (A \cup C) \end{aligned}$$

On se fixe maintenant un ensemble U. Si A et B sont deux parties de U, il est clair que $A \cup B$ et $A \cap B$ sont encore des parties de U. Autrement dit, les opérations d'union et d'intersection sont *internes aux parties de U*.

Les connecteurs logiques OU et ET correspondent aux opérations d'union et d'intersection des ensembles. En effet, soit Φ et Ψ deux énoncés ayant une unique variable libre x, et considérons les parties de U_Φ et U_Ψ définies par compréhension. Alors :

$$U_\Phi \cup U_\Psi = U_{\Phi \vee \Psi} \qquad U_\Phi \cap U_\Psi = U_{\Phi \wedge \Psi}$$

Si on part de parties A et B au lieu d'énoncés Φ et Ψ, on obtient :

$$A \cup B = \{x \in U \mid x \in A \text{ OU } x \in B\} \qquad A \cap B = \{x \in U \mid x \in A \text{ ET } x \in B\}$$

Définition. *Soit U un ensemble, et soit A une partie de U. Alors le* complémentaire *de A dans U est l'ensemble des éléments de U qui ne sont pas éléments de A. On le note $U \setminus A$.*

Il est important de noter que l'ensemble U est essentiel pour définir le complémentaire.

Il est clair que le passage au complémentaire correspond à la négation logique :

$$U_{\neg\Phi} = U \setminus U_\Phi$$

Proposition. *Soit U un ensemble. Soit A et B des parties de U. Alors les énoncés suivants sont vrais.*

$$U \setminus (U \setminus A) = A$$
$$A \cup (U \setminus A) = U \qquad A \cap (U \setminus A) = \emptyset$$
$$U \setminus \emptyset = U \qquad U \setminus U = \emptyset$$
$$U \setminus (A \cup B) = (U \setminus A) \cap (U \setminus B) \qquad U \setminus (A \cap B) = (U \setminus A) \cup (U \setminus B)$$

On voit ainsi qu'il y a une correspondance entre les opérations de passage au complémentaire, d'intersection et de réunion et, respectivement, les connecteurs logiques « non », « et » et « ou » :

Opération ensembliste	*Connecteur logique correspondant*
passage au complémentaire	négation ($\neg$)
intersection ($\cap$)	conjonction ($\wedge$)
réunion ($\cup$)	disjonction ($\vee$)

2.6—Suites d'ensembles

Soit E un "gros" ensemble, et supposons donné, pour chaque entier $n \geq 0$, une partie de E qu'on note A_n. De même que vous avez déjà vu la notion de suite $(x_n)_{n\geq 0}$ avec par exemple $x_n \in \mathbb{R}$, on a maintenant la notion de *suites d'ensembles*, qu'on va noter $(A_n)_{n\geq 0}$ dans ce cas. Remarquer que n est ici une variable muette.

On peut alors définir les notions d'*intersection* et d'*union* pour la suite d'ensembles $(A_n)_{n\geq 0}$, de la façon suivante :

$$\bigcap_{n\geq 0} A_n = \{x \in E \mid \forall n \geq 0 \quad x \in A_n\} \qquad \bigcup_{n\geq 0} A_n = \{x \in E \mid \exists n \geq 0 \quad x \in A_n\}$$

Exercice Soit $A_n = [0, n]$. Prouver : $\bigcup_{n\geq 0} A_n = \mathbb{R}$ et $\bigcap_{n\geq 0} A_n = \{0\}$.

Exercice On suppose que $(A_n)_{n\geq 0}$ est une suite *croissante* d'ensembles, c'est-à-dire $A_n \subseteq A_{n+1}$ pour tout entier $n \geq 0$. Montrer que $\bigcap_{n\geq 0} A_n = A_0$. Retrouver ainsi le résultat de l'exercice précédent.

3—Fonctions et applications. Cardinalité des ensembles

3.1—Fonctions, applications, images et antécédents

La notion de *fonction* a été plusieurs fois évoquée depuis le début de ce cours.

Définition. *Une* fonction $f : E \to F$ *est caractérisée par les éléments suivants :*

1. *Un* ensemble de départ E.
2. *Un* ensemble d'arrivée F.
3. *L'*association *d'au plus un élément de F à chaque élément de E. S'il est défini, l'élément de F associé à x appartenant à E est noté $f(x)$.*

Si $y = f(x)$ est défini, on dit que y est l'image *de x. Il y a donc* au plus une *image pour chaque élément x.*

Le domaine de définition *de la fonction f est l'ensemble des éléments $x \in E$ pour lesquels $f(x)$ est défini. On le note D_f . Si $D_f = E$, c'est-à-dire si chaque élément a une image, on dit que f est une* application.

Prenons $E = F = \mathbb{R}$. Une fonction $f : \mathbb{R} \to \mathbb{R}$ est souvent défini par la *formule* qui exprime $f(x)$ en fonction de x (c'est de là que vient le nom de *fonction*). Par exemple, la fonction $f : \mathbb{R} \to \mathbb{R}$ telle que

$$f(x) = \frac{1}{\sqrt{2x-1}}$$

a comme ensemble de définition :

$$D_f = \{x \in \mathbb{R} \mid 2x - 1 > 0\} = \left]\frac{1}{2}, +\infty\right[$$

Mais la notion de fonction est plus générale que juste la donnée d'une formule analytique exprimant $f(x)$ en fonction de x. Ainsi, on peut considérer la fonction suivnate $f : \mathbb{R} \to \mathbb{R}$ définie par :

$$f(x) = \begin{cases} 1, & \text{si } x \in \mathbb{Q} \\ 0, & \text{si } x \in \mathbb{R} \setminus \mathbb{Q} \end{cases}$$

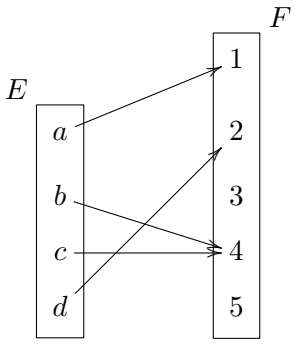
Ce denier exemple illustre la définition d'une fonction *par cas*. Une telle définition est valide du moment que les différents cas ne se chevauchent pas. Si les différents cas couvrent tous les éléments de l'ensemble de départ, il s'agit alors d'une application. Par exemple, la définition par cas suivante *n'est pas* valide :

$$f : \mathbb{N} \to \mathbb{N} \qquad f(x) = \begin{cases} 2, & \text{si } x \text{ est multiple de } 2 \\ 7, & \text{si } x \text{ est multiple de } 3 \end{cases}$$

En effet les deux cas "x multiple de 2" et "x multiple de 3" ne sont pas disjoints, et il y a ambiguité dans la définition par exemple pour $x = 6$.

Un autre exemple de fonction qui n'est pas donnée par une formule est celui des fonctions entre des ensembles finis. On peut alors représenter une fonction $f : \{a, b, c, d\} \to \{1, 2, 3, 4, 5\}$ sous la forme d'un shéma comme ci-dessous, pour $f(a) = 1$, $f(b) = 4$, $f(c) = 4$

et $f(d) = 2$:



Il est pratique de disposer de la définition suivante.

Définition. *Soit $f : E \to F$ une fonction. On dit que $x \in E$ est un* antécédent *de $y \in F$ si $f(x) = y$. On appelle* image de f *l'ensemble des éléments de F qui ont au moins un antécédent. On le note $f(E)$.*

Attention : les définitions d'image et d'antécédent *ne sont pas* symétriques. En effet, par définition d'une fonction, un élément $x \in E$ a *au plus* une image. Tandis qu'un élément $y \in F$ peut très bien avoir *plusieurs* antécédents, comme le montre l'élément 4 dans l'exemple ci-dessus puisque $f(b) = f(c) = 4$.

L'exemple ci-dessus est celui d'une *application* puisque tous les éléments de E ont une image. Mais certains éléments de F n'ont pas d'antécédents : ici 3 et 5.

Attention à la notation $f(E)$ pour l'image de f. Dans cette notation, E n'est bien sûr pas un élément de E lui-même ! On peut définir $f(E)$ par compréhension :

$$f(E) = \{y \in F \mid \exists x \in E \quad y = f(x)\}$$

C'est donc l'ensemble des éléments de F qui sont atteints par f. Dans l'exemple ci-dessus, on a : $f(E) = \{1, 2, 4\}$.

Exercice Donner la définition d'une fonction. Donner la définition d'une application. Donner un exemple de fonction $f : E \to F$ où tous les éléments $x \in E$ ont la même image. Dans le cas d'une *application*, à quelle condition tous les éléments de F peuvent-ils avoir le même antécédent ? Qu'en est-il dans le cas général d'une fonction ?

3.2—Image directe et image réciproque des sous-ensembles

L'attention des lecteurs est attirée dans cette section sur les *notations* qui peuvent entrainer certaines confusions.

Définition. *Soit $f : E \to F$ une fonction. On appelle* image *d'une partie A de E l'ensemble des images d'éléments de A, et on le note $f(A)$. Par compréhension :*

$$f(A) = \{y \in F \mid \exists x \in A \quad y = f(x)\}. \quad \textit{Notez : } f(A) \subseteq F.$$

On appelle image réciproque *d'une partie B de F l'ensemble des antécédents d'éléments de B, et on le note $f^{-1}(B)$. Par compréhension :*

$$f^{-1}(B) = \{x \in E \mid f(x) \in B\}. \quad \textit{Notez : } f^{-1}(B) \subseteq E.$$

Quelques remarques :

1. Attention aux notations ! Ici, $f^{-1}(B)$ ne doit pas être confondu avec la notion de réciproque d'une fonction bijective (voir plus loin). La notation $f^{-1}(B)$ est seulement une convention pour désigner l'ensemble décrit par compréhension ci-dessus.
2. La notion d'image directe $f(A)$ généralise la notion d'image de la fonction f, définie ci-dessus avec la notation $f(E)$. Vérifiez que c'est bien la même notion pour $A = E$.
3. La notion d'image directe permet donc, à partir d'une fonction f, de définir une nouvelle fonction cette fois $\mathcal{P}(E) \to \mathcal{P}(F)$, qui agit sur les *parties de E*. C'est en fait une application : car si f n'est pas définie sur A, alors son image est pourtant bien définie : $f(A) = \emptyset$.
4. Il en est de même pour les images réciproques, qui définissent une nouvelle application, mais cette fois dans le sens inverse, $\mathcal{P}(F) \to \mathcal{P}(E)$.

Exercice Soit $f : E \to F$. Montrer que si $A \subseteq B \subseteq E$ alors $f(A) \subseteq f(B)$. Si $A \subseteq B \subseteq F$, montrer que $f^{-1}(A) \subseteq f^{-1}(B)$.

3.3—Applications bijectives

Définition. *Soit $f : E \to F$ une application. On dit que f est* bijective*, ou que f est une* bijection*, si tout élément $y \in F$ possède un unique antécédent par f.*

Comme f est supposée être une application, chaque élément $x \in E$ a par définition une unique image. En supposant f bijective, on rétablit la symétrie entre E et F puisqu'alors chaque élément de F a un unique antécédent.

Supposons $f : E \to F$ bijective. Puisque chaque élément $y \in F$ a un unique antécédent, on définit une nouvelle application $g : F \to E$, qui à $y \in F$ associe son unique antécédent $x \in F$, c'est-à-dire l'unique élément $x \in E$ tel que $f(x) = y$. Pour cette paire (x, y), on a donc $x = g(y)$.

Définition. *Soit $f : E \to F$ une application bijective. On appelle* bijection réciproque de f *l'application $g : F \to E$ vérifiant :*

$$\forall y \in E \quad f(g(y)) = y. \tag{5}$$

On la note souvent : $g = f^{-1}$.

Remarquez l'importance des deux ingrédients pour définir $g(y)$: à la fois l'*existence* d'au moins un antécédent de y, mais aussi son *unicité* car sinon g ne serait même pas une fonction.

Dans l'écriture (5) ci-dessus, on part d'un élément $y \in F$, on lui applique g puis f, dans cet ordre, et on retrouve y. Ceci suggère de procéder dans l'ordre inverse, pour savoir si, partant d'un élément $x \in E$, en appliquant d'abord f puis g, on retrouve x. Le théorème suivant répond à cette question par l'affirmative.

Théorème. *Soit $f : E \to F$ une application. Alors les propriétés suivantes sont équivalentes :*

(i) f est bijective

(ii) Il existe une fonction $h : F \to E$ vérifiant :

$$(\forall y \in F \quad f(h(y)) = y) \wedge (\forall x \in E \quad h(f(x)) = x)$$

Dans ce cas, la fonction h est unique et coïncide avec la fonction réciproque de f.

Démonstration. □

3.4—Applications injectives et surjectives

Soit $f : E \to F$ une application. Dire que f est bijective revient à affirmer, pour chaque élément $y \in F$, une double propriété : premièrement, il existe un antécédent de y, et deuxièmement, cet antécédent est unique.

Lorsqu'on examine ces deux propriétés séparément, on aboutit aux notions d'application surjective et d'application injective, définies ci-dessous.

Définition. *Soit $f : E \to F$ une application.*

1. *f est surjective si $f(E) = F$.*
2. *f est injective si elle vérifie la propriété suivante :*

$$\forall x \in E \quad \forall x' \in E \quad f(x) = f(x') \implies x = x'$$

Remarques.

1. On a toujours l'inclusion évidente $f(E) \subseteq F$. Donc l'égalité $f(E) = F$ a lieu si et seulement si l'inclusion réciproque $F \subseteq f(E)$ a lieu. On en déduit la caractérisation suivante (à retenir) de f surjective :

$$\forall y \in F \quad \exists x \in E \quad f(x) = y.$$

2. Reprenons la définition de f injective en utilisant la contraposée de l'implication (ce sera donc une définition équivalente, *cf.* 1.2.4) :

$$\forall x \in E \quad \forall x' \in E \quad x \neq x' \implies f(x) \neq f(x').$$

   Ainsi, f est injective lorsque deux éléments distincts de l'ensemble de départ n'ont jamais la même image. C'est une autre façon de dire qu'un élément de y a au plus un antécédent.

Exemples.

1. Soit $f : \{1, 2, 3, 4\} \to \{1, 2, 3\}$ définie par $f(1) = 2$, $f(2) = 1$, $f(3) = 3$, $f(4) = 4$. Alors f est surjective car on vérifie, en les examinant l'un après l'autre, que les trois éléments de l'ensemble d'arrivée ont chacun au moins un antécédent. Mais f n'est pas injective puisque 3 et 4 ont la même image.
2. Soit $f : \{1, 2, 3\} \to \{1, 2, 3, 4\}$ définie par $g(1) = 1$, $g(2) = 2$, $g(3) = 3$. Alors g est injective puisaue deux éléments distincts parmi $\{1, 2, 3\}$ sont envoyés sur deux éléments distincts. Mais g n'est pas surjective puisque 4 n'a pas d'antécédent par g.
3. L'application $h : \mathbb{R}^* \to \mathbb{R}$ définie par $h(x) = 1/x$ est injective. Pour le voir, prenons la formulation directe de la définition. Soit $x, x' \in \mathbb{R}^*$ tels que $h(x) = h(x')$. Alors $1/x = 1/x'$ donc $x = x'$, ce qui montre que h est injective. Mais h n'est pas surjective puisque 0 n'a pas d'antécédent.
4. L'application $p : \mathbb{R}^* \to \mathbb{R}^*$ définie par $p(x) = 1/x$ est à la fois injective et surjective (notez qu'on a juste modifié l'ensemble d'arrivée). En effet, p est injective pour les mêmes raisons faisant que h est injective. Pour montrer que h est surjective, soit $y \in \mathbb{R}^*$, on cherche $x \in \mathbb{R}^*$ tel que $h(x) = y$, et pour cela il suffit de prendre $x = 1/y$, qui existe puisque $y \neq 0$ par hypothèse.

Le théorème suivant établit le lien entre applications bijective, injectives et surjectives.

Théorème. *Soit $f : E \to F$ une application. Alors f est bijective si et seulement si f est surjective et injective.*

En pratique, on a donc deux méthodes, essentiellement équivalentes pour montrer qu'une application est bijective : soit on montre tour à tour qu'elle est injective et surjective ; soit on exhibe explicitement la bijection réciproque.

Démonstration. □

À retenir Les définitions d'application injective et d'application surjective, par cœur. Le théorème faisant le lien avec les applications bijectives. Comment faire pour démontrer qu'une application est injective, ou surjective, ou bijective.

3.5—Composition des applications

Définition. *Soit $f : E \to F$ et $g : F \to G$ deux applications. La composition de g et f est l'application avec E pour ensemble de départ et G pour ensemble d'arrivée, qu'on note $g \circ f$ et qu'on définit ainsi :*

$$\forall x \in E \quad g \circ f(x) = g\big(f(x)\big)$$

Pour que cette définition ait un sens, il faut que l'ensemble d'arrivée de f coïncide avec l'ensemble de départ de g. La composition $g \circ f$ est symbolisée par le diagramme suivant :

$$E \xrightarrow{f} F \xrightarrow{g} G \qquad (g \circ f : E \to G)$$

Donc, pour connaître l'image d'un élément $x \in E$ par $g \circ f$, on fait d'abord agir f, ce qui donne $f(x)$, auquel on applique g, ce qui donne le résultat final $g\big(f(x)\big)$.

Remarquez que l'ordre est important. En général, avec f et g définies comme précédemment, la composition $f \circ g$ n'est tout simplement pas définie.

Supposons maintenant données trois applications :

$$E \xrightarrow{f} F \qquad F \xrightarrow{g} G \qquad G \xrightarrow{h} H$$

Par composition, il y a alors deux façons de définir une application de E vers H, correspondant aux deux chemins, supérieur et inférieur, dans le diagramme ci-dessous :

$$E \xrightarrow{f} F \xrightarrow{g} G \xrightarrow{h} H \qquad (g \circ f : E \to G,\ h \circ g : F \to H)$$

En fait, ces deux façons de procéder donnent le même résultat, comme le spécifie le théorème suivant. On interprète ce résultat comme une propriété d'*d'associativité*, analogue à l'associativté de l'addition :

$$x + (y + z) = (x + y) + z$$

Notez que cette propriété d'associativité permet l'écriture $x+y+z$ sans parenthèses : sans l'associativité, cette écriture est ambigüe puisqu'elle peut correspondre à deux calculs *a priori* différents, consistant à faire d'abord l'addition de $y + z$ puis celle avec x, ou bien à faire d'abord l'addition $x + y$ puis celle avec z. C'est donc une propriété fondamentale, d'usage permanent, même si on l'utilise sans y prêter attention. Son analogue pour la composition des applications est tout aussi fondamentale.

Théorème. *Soit $f : E \to F$, $g : F \to G$ et $h : G \to H$ trois applications. Alors les deux applications suivantes sont égales :*

$$h \circ (g \circ f) = (h \circ g) \circ f$$

Dans l'égalité ci-dessus, le membre de gauche correspond au chemin du haut dans le diagramme précédent, et le membre de droite correspond au chemin du bas. Au vu de ce théorème, on peut se permettre d'écrire sans parenthèse l'expression $h \circ g \circ f$, qui correspond à l'un quelconque des deux membres de l'égalité $h \circ (g \circ f) = (h \circ g) \circ f$.

Démonstration. □

À retenir La composition de deux applications $f : E \to F$ et $g : F \to G$ est une application $g \circ f : E \to G$. La composition vérifie une loi d'associativité qui permet l'écriture sans parenthèse de plusieurs compositions enchaînées.

3.6—Applications d'un ensemble dans lui-même

Un cas particulier important est celui où ensembles de départ et d'arrivée des applications coïncident. On considère donc des applications $E \to E$ pour un certain ensemble E. L'application identité est définie ci-dessous.

Définition. *Étant donné un ensemble E, on appelle application identité l'application avec E comme ensemble de départ et comme ensemble d'arrivée, qu'on note* Id_E *et qui est définie par :*

$$\forall x \in E \quad Id_E(x) = x$$

Nous pouvons alors reformuler le théorème vu en 3.3 de la façon suivante.

Théorème. *Soit $f : E \to F$ une application. Alors f est une bijection si et seulement si il existe une application $h : F \to E$ telle que :*

$$f \circ h = \mathrm{Id}_F \quad \textit{et} \quad h \circ f = \mathrm{Id}_E$$

Dans ce cas, la fonction h est unique et coïncide avec la fonction réciproque de f.

Dans le théorème ci-dessus, les *deux* égalités sont nécessaires. Par exemple, soit $E = \{0, 1\}$ et $F = \{0, 1, 2\}$, et considérons la fonction $f : E \to F$ définie par $f(0) = 0$ et $f(1) = 1$ est injective mais non surjective, et donc non bijective. Pourtant, la fonction $h : F \to E$ définie par $h(0) = 0$, $h(1) = 1$ et $h(2) = 0$ vérifie $h \circ f = \mathrm{Id}_E$. On vérifie bien sûr que $f \circ h \neq \mathrm{Id}_F$ puisque $f \circ h(2) = f(0) = 0$.

Soit E un ensemble, et définissons $\mathcal{F}(E)$ comme l'ensemble des fonctions de E dans E. Il est clair que pour deux fonctions $f, g \in \mathcal{F}(E)$, la composition $g \circ f$ est toujours bien définie. De plus, la composition $g \circ f$ est à nouveau une fonction de E dans E, c'est-à-dire $g \circ f \in \mathcal{F}(E)$.

La composition définit donc ce qu'on appelle une loi de composition entre éléments de $\mathcal{F}(E)$, c'est-à-dire une application :

$$\mathcal{F}(E) \times \mathcal{F}(E) \to \mathcal{F}(E) \qquad (g, f) \mapsto g \circ f$$

qui est un peu analogue avec la loi du produit entre nombres réels :

$$\mathbb{R} \times \mathbb{R} \to \mathbb{R} \qquad (x, y) \mapsto x \times y$$

Examinons les analogies et les différences entre la composition dans $\mathcal{F}(E)$ et le produit dans $\mathbb{R}$.

1. La composition est associative : $f \circ (g \circ h) = (f \circ g) \circ h$
2. La composition *n'est pas* commutative en général, contrairement au produit dans $\mathbb{R}$. En effet, il est facile de trouver deux applications $f, g \in \mathcal{F}(E)$ telles que $f \circ g \neq g \circ f$. Par exemple, prenons $E = \{0, 1, 2\}$ et f et g décrites par les tableaux suivants :

x	0	1	2
$f(x)$	1	0	2

x	0	1	2
$g(x)$	0	2	1

   Alors :

$$\begin{aligned} f \circ g(0) &= f\big(g(0)\big) && \text{par définition de } f \circ g \\ &= f(0) && \text{d'après le tableau de } g \\ &= 1 && \text{d'après le tableau de } f \end{aligned}$$

   et de même : $g \circ f(0) = g(1) = 2$ donc $f \circ g \neq g \circ f$.
3. Pour le produit dans $\mathbb{R}$, l'élément 1 est neutre : $1 \times x = x$. Le rôle de 1 est joué dans $\mathcal{F}(E)$ par l'identité :

$$\forall f \in F \quad (f \circ \mathrm{Id}_E = f) \wedge (\mathrm{Id}_E \circ f = f)$$

   Comme la composition n'est pas commutative, il est important de spécifier les *deux* égalités ci-dessus.
4. Les nombres non nuls sont inversibles : pour $x \neq 0$, il existe $y \in \mathbb{R}$ tel que $x \times y = 1$. Adaptons cette définition à $\mathcal{F}(E)$. En tenant compte de la non commutativité, on s'intéresse aux applications $f \in \mathcal{F}(E)$ telles que, pour un certain $g \in \mathcal{F}(E)$, on ait : $f \circ g = \mathrm{Id}_E$ et $g \circ f = \mathrm{Id}_E$. Mais d'après le théorème précédent, c'est équivalent à dire que f est bijective, et alors g est la bijection réciproque de f.

Exercice Soit $h \in \mathcal{F}(E)$ vérifiant la propriété suivante :

$$\forall f \in F \quad (f \circ h = f) \wedge (h \circ f = f)$$

Montrer que $h = \mathrm{Id}_E$.

Exercice Soit $r_\theta : \mathbb{R}^2 \to \mathbb{R}^2$ la rotation d'angle $\theta \in [0, 2\pi[$ autour de l'origine, définie par :

$$\forall (x, y) \in \mathbb{R}^2 \quad r_\theta(x, y) = (x \cos\theta - y \sin\theta, x \sin\theta + y \cos\theta)$$

Soit $t : \mathbb{R}^2 \to \mathbb{R}^2$ la translation de vecteur $(1, 0)$, définie par :

$$\forall (x, y) \in \mathbb{R}^2 \quad t(x, y) = (x + 1, y)$$

Montrer que t est une bijection. Montrer que r_θ est une bijection quel que soit θ. Déterminer quelles sont la, ou les variables libres dans l'énoncé suivant :

$$r_\theta \circ t = t \circ r_\theta$$

Déterminer l'ensemble des valeurs du paramètre θ pour lesquelles t et r_θ commutent.

À retenir Si ensembles de départ et d'arrivée coïncident, la composition des applications définit une loi de composition associative mais non commutative dans $\mathcal{F}(E)$. L'application identité est l'élément neutre et les bijections correspondent aux inversibles pour la composition des applications.

3.7—Cardinalité des ensembles finis

Énonçons la définition.

Définition. *Si A est un ensemble fini, le cardinal de A est le nombre d'éléments qu'il contient. On le note $|A|$ ou $\#A$ ou* $\mathrm{Card}(A)$.

L'ensemble vide est le seul ensemble de cardinal 0. Par définition, les singletons sont les ensembles de cardinal 1.

La combinatoire énumérative est la branche des mathématiques qui étudie le cardinal des ensembles finis. Le théorème suivant regroupe deux résultats élémentaires que vous connaissez déjà.

Théorème. *Si A et B sont deux ensembles disjoints, alors $|A \cup B| = |A| + |B|$. Si A et B sont deux ensembles quelconques, alors $|A \times B| = |A| \times |B|$.*

Les applications sont des outils à la base de nombreuses techniques énumératives. Il est important de connaître le résultat suivant, qu'on admettra.

Théorème. *Soit E et F deux ensembles finis. Alors :*

1. *$|A| \leq |B|$ si et seulement si il existe une application injective de A dans B.*
2. *$|A| \geq |B|$ si et seulement si il existe une application surjective de A dans B.*
3. *$|A| = |B|$ si et seulement si il existe une application bijective de A dans B.*

Une application typique de ce théorème est la suivante. Pour calculer le cardinal d'un ensemble A, on montre qu'il y a une bijection entre A et un ensemble B, dont on sait calculer le cardinal. On en déduit que $|A| = |B|$. Le théorème suivant et son corollaire, dont il est important de retenir les résultats, en sont des exemples d'application.

Théorème. *Soit E et F deux ensembles finis. Soit $\mathcal{F}(E, F)$ l'ensemble des applications de E dans F. Alors :*

$$|\mathcal{F}(E, F)| = |F|^{|E|}$$

Remarque. Le théorème est vrai pour $E = \emptyset$, avec la convention qu'il n'existe qu'une seule application de $\emptyset$ dans F pour tout ensemble F. On s'intéressera uniquement au cas $n \geq 1$.

Démonstration. Soit $P(n)$ la propriété suivante, définie pour tout entier $n \geq 1$:

$$\text{pour tout ensemble finis } E \text{ et } F \text{ avec } |E| = n : \quad |\mathcal{F}(E, F)| = |F|^n$$

On va montrer par récurrence la propriété $\forall n \geq 1 \quad P(n)$ (*cf.* 4.5 pour des rappels sur la récurrence).

Initialisation. Pour $n = 1$, on considère un singleton $E = \{*\}$ et un ensemble fini F. Alors une application $f : E \to F$ est entièrement déterminée par l'image de l'unique élément $*$ de E. Il y a donc une bijection entre $\mathcal{F}(E, F)$ et F, donc $|\mathcal{F}(E, F)| = |F|$. Ceci montre la propriété $P(1)$.

Hérédité. Supposons la propriété $P(n)$, et montrons $P(n + 1)$. Pour cela, soit F un ensemble fini et soit E un ensemble de cardinal $n + 1$. Choisissons un élément $*$ dans E, et posons $E' = E \setminus \{*\}$. Nous avons donc $|E'| = n$.

On va définir une application Φ entre $\mathcal{F}(E, F)$ et $\mathcal{F}(E', F) \times F$. L'application Φ est définie ainsi. Pour $f \in \mathcal{F}(E, F)$, on pose $\Phi(f) = (f', x)$ où $x = f(*)$ et $f' : E' \to F$ est

définie par $f'(y) = f(y)$ pour tout $y \in E'$. Alors on laisse en exercice de montrer que Φ est une bijection.

Il s'ensuit que :

$$\begin{aligned} |\mathcal{F}(E,F)| &= |\mathcal{F}(E',F)| \times |F| && \text{à cause de la bijection } \Phi \\ &= |F|^n \times |F| && \text{par hypothèse de récurrence } P(n) \text{ puisque } |E'| = n \\ &= |F|^{n+1} \end{aligned}$$

ce qui montre $P(n+1)$.

Ceci montre $\forall n \in \mathbb{N} \quad P(n)$, et donc le résultat. □

Corollaire. *Soit E un ensemble fini. Alors l'ensemble $\mathcal{P}(E)$ des parties de E a pour cardinal $2^{|E|}$.*

Démonstration. Soit $D = \{0,1\}$. À tout sous-ensemble U de E on associe l'application $f_U : E \to D$ définie par :

$$\forall x \in E \quad f_U(x) = \begin{cases} 1, & \text{si } x \in U \\ 0, & \text{sinon} \end{cases}$$

Ceci définit une application $\Phi : \mathcal{P}(E) \to \mathcal{F}(E,D)$, qui associe à une partie $U \in \mathcal{P}(E)$ l'application $f_U \in \mathcal{F}(E,D)$. On laisse comme exercice de montrer que cette application est bijective. On a donc égalité des cardinaux :

$$|\mathcal{P}(E)| = |\mathcal{F}(E,D)|$$

Or $|D| = 2$. D'après le résultat du théorème précédent, on en déduit $|\mathcal{P}(E)| = 2^{|E|}$, ce qu'on voulait montrer. □

Exercice Soit E un ensemble fini de cardinal $n \geq 0$. Montrer que l'ensemble des bijections de E dans lui-même est de cardinal $n!$.

4—Démonstrations et techniques de preuve

Nous allons aborder ici certaines techniques de démonstration fréquemment utilisées. Il ne s'agit pas de décrire une méthode universelle pour prouver les théorèmes : une telle méthode n'existe pas ! En revanche, nous allons passer en revue un certain nombre d'automatismes auxquels se référer lorsqu'on est face à un énoncé mathématique à prouver. Il faut toujours essayer ces méthodes avant de se dire « je n'y arrive pas ».

Dans un premier temps, on revient rapidement sur les notions de théorème et de définition mathématique. On verra en particulier que ces deux notions sont fortement reliées l'une à l'autre.

Puis on analyse les techniques de démonstration usuelles liées uniquement à *la forme syntaxique* de l'énoncé à prouver, avant d'analyser des techniques qui sont spécifiques des objets utilisés dans l'énoncé à prouver.

4.1—Théorèmes et définitions

4.1.1—Théorèmes, lemmes, propositions : du pareil au même

Les résultats de mathématiques sont données sous forme de *théorèmes* : ce sont des résultats connus de tous, qui sont démontrés dans les livres ou en cours, et auxquels on peut se référer pour faire d'autres démonstrations. Il est donc essentiel pour l'étudiant de connaître *par cœur* le contenu des théorèmes, ce qui inclut les hypothèses du théorème d'une part, et sa conclusion d'autre part.

Au lieu de les appeler « théorème », certains résultats sont appelés *lemme*, d'autres sont appelés *proposition*, d'autres encore *corollaire*. Du point de vue de la validité mathématique, il n'y a aucune hiérarchie entre tous ces termes ; il n'y aurait pas d'inconvénient à tous les appeler *théorèmes*. On utilise ces différents termes pour mieux appréhender l'organisation des résultats entre eux.

Pour être complet, voici un lexique des plus courants.

Théorème (n.m.) Résultat central d'une théorie ou d'un chapitre.

Proposition (n.f.) Résultat à retenir et utile en soi, même s'il n'est pas le plus important.

Lemme (n.m.) Résultat préliminaire pour en démontrer un autre à venir. Le lemme pouvant servir à plusieurs occasions, il est très utile de le retenir.

Corollaire (n.m.) Résultat qui découle presque immédiatement d'un résultat précédent.

4.1.2—Instances d'un théorème : démonstration et utilisation

Si on se réfère aux théorèmes qu'on connait déjà, on verra qu'ils sont tous énoncés dans une ceratine généralité. Prenons l'exemple du théorème de Pythagore : il est valable pour *tout* triangle rectangle.

Ceci a deux conséquences, qu'on explique sur ce même exemple du théorème de Pythagore :

1. *Du point de vue de l'utilisation.* On peut appliquer le résultat du théorème à n'importe quel triangle rectangle. Il s'agit alors d'une *instanciation particulière* du théorème.
2. *Du point de vue de la démonstration du théorème.* Le théorème doit être démontré en toute généralité, quel que soit le triangle rectangle particulier qu'on considère. Ceci est vrai pour tout résultat mathématique, y compris pour les exercices à résoudre. Constater la véracité d'un énoncé sur quelques exemples ne *peut en aucun cas* constituer une démonstration.

Comme il y a une infinité de triangles rectangles, il ne s'agit pas de vérifier l'énoncé pour tous les triangles rectangle *l'un après l'autre*. Par les outils de la logique, on peut se convaincre de la véracité de l'énoncé quel que soit le triangle rectangle.

4.1.3—Les définitions cachent souvent des théorèmes

Les théorèmes portent sur des objets mathématiques qui ont été préalablement définis. Il semblerait donc au premier abord que la séparation entre théorèmes et définitions soit parfaitement claire. En fait, il n'en est rien : les définitions les plus intéressantes sont elles-mêmes fondées sur des théorèmes.

Pour l'illustrer, prenons l'exemple de la racine carrée des nombres réels positifs. Le cas de zéro ne présentant aucune difficulté, on se restreint au cas des réels strictement positifs. Si l'on posait *a priori* comme définition de racine carrée de $x > 0$ un nombre y tel que $y^2 = x$, cette définition n'aurait pas de sens. Premièrement, comment sait-on qu'un tel nombre y existe ? Deuxièmement, y en a-t-il plusieurs, au cas où il en existe au moins un ? On voit donc que la notion de racine carrée ne peut être *définie* qu'après avoir répondu à ces deux questions.

En fait, l'étude de la fonction carrée montre que $x \mapsto x^2$ est une fonction continue et strictement croissante qui tend vers $+\infty$ en $+\infty$. En appliquant en particulier le théorème des valeurs intermédiaires, on peut alors démontrer le résultat suivant : *pour tout nombre $x > 0$ il existe exactement deux réels y tels que $y^2 = x$. Ces deux réels sont opposés l'un de l'autre.*

On peut alors formuler la définition suivante : on appelle *racine carrée* d'un nombre $x > 0$ l'unique réel strictement positif y tel que $y^2 = x$.

Ainsi, la racine carrée de x est définie par sa propriété caractéristique, à savoir $y^2 = x$ et $y > 0$. Mais cette définition a nécessité une étude préalable pour en montrer la validité.

Enfin, il est important de noter la différence entre justifier la validité d'une définition d'une part, et introduire une notation d'autre part. Ci-dessus, on a introduit la notion de racine carrée sans jamais mentionner le symbole $\sqrt{}$. Ce n'est qu'une fois la *définition* de la racine carrée établie qu'on peut introduire la notation de la façon suivante : *pour $x > 0$, on note $\sqrt{x}$ l'unique réel $y > 0$ tel que $y^2 = x$.*

Pour souligner la différence entre définition et notation, voici un deuxième exemple. (inverse complexe).

4.2—Stratégies de preuve en fonction de la forme de l'énoncé à prouver

Nous allons examiner une manière d'organiser sa réflexion en vue de la démonstration d'énoncés mathématiques. Une démonstration est toujours un *chemin logique* menant d'un point de départ que sont les hypothèses, à un point d'arrivée qui est la conclusion.

Pour faciliter les explications, nous allons traiter nos exemples avec un tableau à deux colonnes, la colonne de gauche comportant le point de départ, et la colonne de droite comportant le point d'arrivée. Les techniques de preuves qu'on va exposer consistent en des manipulations élémentaires qu'il faut maîtriser concernant ces tableaux.

Exemple. *Soit a et b deux réels. Montrer que si $0 < a < b$ alors $a^2 < b^2$.*

La première étape consiste à *lire* et *bien comprendre* l'énoncé. Ici, on reconnait que la question posée consiste à démontrer une implication (*si ... alors ...*). C'est ce qu'on indique dans le tableau ci-dessous.

Tableau de départ :

Données	But
$a, b \in \mathbb{R}$	$0 < a < b \implies a^2 < b^2$

Puisqu'il faut ici prouver une implication, nous allons commencer par ce premier exemple.

4.2.1—Implication : preuve directe d'un énoncé de la forme $A \implies B$

La première chose à essayer pour prouver une implication de la forme $A \implies B$ est la démonstration dite *directe*. On rajoute A dans nos données, et maintenant on essaye de prouver B. Attention, il faut bien se rappeler que prouver $A \implies B$ n'est pas du tout la même chose que prouver B : la grande différence est qu'on rajoute A dans les hypothèses.

On continue l'exemple ci-dessus. On modifie le tableau en faisant passer à gauche l'hypothèse de l'implication et en ne conservant à droite que la conclusion de l'implication. On s'est ainsi débarassé du signe $\implies$.

Tableau modifié :

Données	But
$a, b \in \mathbb{R}$	$a^2 < b^2$
$0 < a < b$	

Puisqu'on s'est débarassé du signe d'implication, on est ramenés à de simples manipulations sur les inégalités. On les fait d'abord au brouillon : puisque $a > 0$, je peux multiplier les deux membres de l'inégalité $a < b$ par a et obtenir $a^2 < ab$. De même, puisque $b > 0$, je peux multiplier par b l'inégalité $a < b$ pour obtenir $ab < b^2$. J'ai donc $a^2 < ab < b^2$ d'où je déduis $a^2 < b^2$.

On passe maintenant à l'étape de rédaction. En voici un exemple ci-dessous.

Rédaction. Soit $a, b \in \mathbb{R}$, et supposons $0 < a < b$. Alors, en multipliant les deux membres de l'inégalité $a < b$ par a, on trouve $a^2 < ab$ puisque $a > 0$. De même, on trouve $ab < b^2$ puisque $b > 0$ et donc $a^2 < b^2$. Ceci montre l'implication $0 < a < b \implies a^2 < b^2$. □

4.2.2—Implication : preuve par contraposée d'un énoncé de la forme $A \implies B$

On a vu que la valeur de vérité d'une implication $A \implies B$ est la même que celle de sa contraposée $\neg B \implies \neg A$. En pratique, pour prouver $A \implies B$, il peut s'avérer plus judicieux d'appliquer la technique de preuve directe non pas à $A \implies B$ mais à sa contraposée $\neg B \implies \neg A$. Ce sera le cas en particulier si l'un des énoncés A ou B comporte des négations.

Exemple. *Soit a, b, c trois réels avec $a \neq 0$, et posons $\Delta = b^2 - 4ac$. Montrer que si $\Delta < 0$ alors l'équation $ax^2 + bx + c = 0$ n'a pas de solution réelle.*

Traduisons cet énoncé dans un tableau, en repérant l'implication contenue dans l'énoncé.

Tableau de départ :

Données	But
$a, b, c \in \mathbb{R},\ a \neq 0$	$(\Delta < 0 \implies \neg(\exists x \in \mathbb{R} \quad ax^2 + bx + c = 0))$

Transformons l'implication à prouver par sa contraposée :

Tableau modifié :

Données	But
$a, b, c \in \mathbb{R},\ a \neq 0$	$((\exists x \in \mathbb{R} \quad ax^2 + bx + c = 0) \implies \Delta \geq 0)$

À présent, on transforme l'implication comme dans le cas de la preuve directe, en faisant passer l'hypothèse de l'implication à gauche et en ne conservant à droite que la conclusion de l'implication.

	Données	But
Tableau modifié :	$a, b, c \in \mathbb{R},\ a \neq 0$	$\Delta \geq 0$
	$\exists x \in \mathbb{R} \quad ax^2 + bx + c = 0$	

Puisque nous avons maintenant un énoncé avec un quantificateur existentiel comme données de départ, nous pouvons instancier ce quantificateur. Autrement dit, on fixe un $x_0 \in \mathbb{R}$ solution de l'équation $ax_0^2 + bx_0 + c = 0$, ce qui est possible puisque notre hypothèse nous dit précisément qu'un tel réel existe. On se débarasse donc du quantificateur existentiel et on récupère à la place un "vrai" x_0, d'où le tableau suivant.

	Données	But
Tableau modifié :	$a, b, c \in \mathbb{R},\ a \neq 0$	$\Delta \geq 0$
	$x_0 \in \mathbb{R}$ tel que $ax_0^2 + bx_0 + c = 0$	

Remarquez que x_0 est maintenant une variable qui renferme une certaine constante réelle qu'on a fixée. Tandis que dans le tableau précédent avec le quantificateur existentiel, x était une variable muette. C'est très différent : maintenant on peut faire toutes les manipulations algébriques qu'on souhaite sur notre constante x_0.

Pour finir la démonstration, il reste à mettre en place les calculs habituels sur les polynômes du second degré. Pour résumer, on aboutit à une rédaction comme celle-ci.

Rédaction. On procède par contraposée. Soit donc a, b, c trois réels avec $a \neq 0$ et tels que l'équation $ax^2 + bx + c = 0$ a une solution réelle, et montrons que $\Delta \geq 0$. Soit x_0 une solution rélle de l'équation. Alors on a :

$$\begin{aligned} 0 &= ax_0^2 + bx_0 + c \\ &= a\Big(x_0 + \frac{b}{2a}\Big)^2 + c - \frac{b^2}{4a} \qquad \text{car } a \neq 0 \\ &= a\Big(x_0 + \frac{b}{2a}\Big)^2 - \frac{1}{4a}\Delta \end{aligned}$$

On en déduit : $\Delta = 4a^2\Big(x_0 + \frac{b}{2a}\Big)^2$ donc $\Delta \geq 0$, ce qu'on voulait prouver. □

4.2.3—Énoncés quantifiés universellement (∀)

La plupart des théorèmes du cours sont des énoncés quantifiés universellement : un théorème donne une propriété de tous les nombres entiers, ou de tous les nombres complexes non nuls, ou de toutes les fonctions continues. Il en est de même pour de nombreux exercices.

Soit un énoncé de la forme $\forall x \in W \quad P(x)$, où W est un ensemble et $P(x)$ est un énoncé dans lequel x apparaît comme variable libre. La méthode la plus couramment utilisée pour démontrer un tel énoncé consiste à montrer que l'énoncé $P(x)$ est vrai quel que soit la valeur substituée à la variable libre x, pourvu que cette valeur soit prise dans W.

En pratique, on procède ainsi :

1. On fixe une valeur $x \in W$.
2. On démontre l'énoncé $P(x)$ pour cette valeur de x. Insistons : la valeur x est fixée pour toute la durée de la démonstration de $P(x)$.

Sous forme de tableaux, on obtient le shéma suivant :

Tableau de départ :	Données	But
	X	$\forall x \in W \quad P(x)$

Tableau modifié :	Données	But
	X	$P(x)$
	$x \in W$	

Remarquer le changement de statut de la variable x entre le tableau de départ et le tableau modifié.

Exemple. *Montrer l'inégalité triangulaire :* $\forall (x, y) \in \mathbb{R} \times \mathbb{R} \quad |x + y| \leq |x| + |y|$.

Ici, la quantification universelle porte sur les éléments de $\mathbb{R} \times \mathbb{R}$. On se fixera donc un couple $(x, y) \in \mathbb{R} \times \mathbb{R}$, sur lequel on va travailler. Pour se débarasser des valeurs absolues, on distingue plusieurs cas, suivant les signes de x et de y. Ceci nous amène à la rédaction suivante.

Rédaction. Soit $(x, y) \in \mathbb{R} \times \mathbb{R}$. Quitte à échanger le rôle de x et de y, on suppose que $|x| \leq |y|$.

Étudions les valeurs des différents termes de l'inégalité, suivant le signe de x et de y. On remarque que $x+y$ est toujours du même signe que y puisqu'on a supposé que $|x| \leq |y|$. On obtient donc le tableau suivant.

		$\lvert x+y\rvert$	$\lvert x\rvert + \lvert y\rvert$
$x \geq 0$	$y \geq 0$	$x + y$	$x + y$
$x \geq 0$	$y < 0$	$-(x + y)$	$x - y$
$x < 0$	$y \geq 0$	$x + y$	$-x + y$
$x < 0$	$y < 0$	$-(x + y)$	$-x - y$

Les lignes 1 et 4 sont des cas d'égalité. Pour la ligne 2, l'inégalité découle de $-x \leq x$, qui est vraie puisque $x \geq 0$. Pour la ligne 3, l'inégalité découle de $x \leq -x$, qui est vraie puisque $x < 0$ cette fois. Ainsi, l'inégalité a lieu dans tous les cas. □

À retenir Pour prouver un énoncé universellement quantifié de la forme $\forall x \in A \quad P(x)$, il est fréquent de commencer par introduire une nouvelle variable, x par exemple, et on prouve ensuite l'énoncé $P(x)$ avec x "fixé".

4.2.4—Énoncés quantifiés existentiellement (∃)

Les énoncés commençant par un quantificateur existentiel sont appelés théorèmes d'existence, et ils peuvent être parmi les résultats mathématiques les plus difficiles et les plus profonds.

Pour prouver un énoncé de la forme $\exists x \in W \quad P(x)$, la première méthode qui vient à l'esprit est de trouver un certain élément x de W pour lequel la propriété $P(x)$ est vraie.

Exemple. *Montrer qu'il existe un nombre premier supérieur à* 10000.

On vérifie que 10007 est premier. Pour ce faire, on prend une variable i variant entre 2 et 10006, et on applique l'algorithme de division euclidienne pour vérifier que i ne divise jamais 10007. Donc 10007 est premier.

Cette démarche est légitime : on nous demande de montrer l'existence d'un certain objet avec une certaine propriété, et on en trouve un explicitement. Cependant, en général, la mener à bien peut être très ardu. Par exemple, dans l'énoncé précédent, remplaçons le nombre 10000 par une variable n. L'énoncé devient le suivant.

Exemple. *Montrer que pour tout entier n, il existe un nombre premier supérieur à n.*

Traduisons cet énoncé avec des quantificateurs. Appelons P l'ensemble des nombres premiers. L'énoncé s'écrit :

$$(E) \ : \ \forall n \in \mathbb{N} \quad \exists p \in P \quad p \geq n$$

Puisque (E) commence par un quantificateur universel, on fixe un entier $n \in \mathbb{N}$ et on cherche à montrer l'existence d'un nombre premier $p \geq n$. Or, essayer de généraliser la démarche précédente, qui marchait pour $n = 10000$, n'aboutit pas dans le cas général. En fait, on ne connait pas de formule générale qui donnerait un nombre premier supérieur à n.

Alors on adpote une autre démarche. On va déduire l'énoncé (E) d'un autre énoncé :

$$(E') \ : \ \text{il existe une infinité de nombres premiers}$$

Notre entier n étant toujours fixé, raisonnons par l'absurde en supposant qu'il n'existe pas de nombre premier $p \geq n$. Ceci implique que tous les nombres premiers sont situés entre 2 et $n-1$. Ils seraient donc en nombre fini, ce qui contredit l'énoncé (E').

Il reste bien sûr à démontrer l'énoncé (E'). Nous l'admettrons ici : nous renvoyons les lecteurs curieux à un cours d'Arithmétique pour la preuve.

L'important est de bien saisir la différence entre ces deux exemples. Dans le premier exemple, on a donné *explicitement* un des objets recherchés. Tandis que, dans le deuxième exemple, on a utilisé un argument qui montrait *l'existence* de l'objet, sans le décrire explicitement.

La première démarche est préférable si elle est possible, mais elle peut être hors de portée. Voici deux autres exemples où on prouve l'existence d'un objet sans le caractériser explicitement. Dans le deuxième exemple, on peut le caractériser explictement si on le souhaite, ou juste se contenter de la preuve de l'existence.

Exemple. *Montrer que l'équation $x^7 - \frac{47592}{987103}x^2 + \sqrt{31}x - 1 = 0$ a au moins une solution réelle.*

Plus généralement, grâce au théorème des valeurs intermédiaires, on sait que tout polynôme de degré impair s'annule au moins une fois sur $\mathbb{R}$. C'est un exemple classique pour lequel nous renvoyons au cours d'Analyse.

Exemple. *Soit $f : \mathbb{R}^3 \to \mathbb{R}^2$ donnée par :*

$$f(x, y, z) = (2x + 3y - x, \ -x + 5y + z)$$

Montrer qu'il existe un triplet $(x, y, z) \neq (0, 0, 0)$ tel que $f(x, yz) = (0, 0)$.

On reconnaît que f est une application linéaire. D'après la théorie de la dimension, f ne peut pas être injective, donc son noyau est non réduit à $\{(0, 0, 0)\}$, d'où l'existence d'un vecteur $(x, y, z) \neq (0, 0, 0)$ tel que $f(x, y, z) = (0, 0)$. Évidemment, on pourrait très bien ici résoudre le système linéaire $f(x, y, z) = (0, 0)$ et caractériser entièrement toutes les solutions. La théorie de la dimension nous dit à l'avance que ce système a des solutions non identiquement nulles.

À retenir Les énoncés quantifiés existentiellement sont typiquement ceux pour lesquels il n'y a pas de "recette miracle" qui marcherait à tous les coups. Tout dépend du contexte. Si on le peut, le mieux est d'exhiber l'objet recherché.

4.2.5—Prouver un énoncé de la fome $A \vee B$

Pour prouver un énoncé de la forme $A \vee B$, il faut trouver un chemin qui parte des données de départ et qui arrive soit à A soit à B. Attention : le point d'arrivée peut tout à fait *dépendre* des données de départ.

Exemple. *Soit n un entier. Montrer que n est soit de la forme $2k$, soit de la forme $2k+1$, avec k entier.*

En traduisant l'énoncé avec des quantificateurs, et en les plaçant dans un tableau comme précédemment, on obtient donc le tableau suivant :

Tableau de départ :	Données	But
	$n \in \mathbb{N}$	$(\exists k \in \mathbb{N} \quad n = 2k) \vee (\exists k \in \mathbb{N} \quad n = 2k+1)$

Une façon de faire consiste à *éliminer des cas* en voyant la démonstration de manière dynamique. Posons A et B les énoncés :

$$A = \text{“}\exists k \in \mathbb{N} \quad n = 2k\text{”} \qquad\qquad B = \text{“}\exists k \in \mathbb{N} \quad n = 2k+1\text{”}$$

En partant de $n \in \mathbb{N}$, si A est vérifée, alors on a gagné et donc la démonstration s'arrête. Sinon, c'est que A n'est pas vérifiée. On peut rajouter l'hypothèse $\neg A$ dans nos données, à charge maintenant de montrer que B est vraie. On a donc échangé un peu de souplesse (montrer A ou montrer B) contre une hypothèse supplémentaire : on part de $\neg A$ mais il faut montrer B. Ceci s'interprète facilement à l'aide de l'implication :

$$A \vee B = (\neg(\neg A) \vee B) = (\neg A \implies B)$$

Notre tableau de départ est donc équivalent au tableau suivant :

Tableau modifié :	Données	But
	$n \in \mathbb{N}$	$\neg A \implies B$

Appliquons la technique de démonstration directe pour l'implication :

Tableau modifié :	Données	But
	$n \in \mathbb{N}$	B
	$\neg A$	

Pour notre exemple, en remplaçant les lettres A et B par les énoncés qu'ils représentent :

Tableau modifié :	Données	But
	$n \in \mathbb{N}$	$\exists k \in \mathbb{N} \quad n = 2k+1$
	$\neg(\exists k \in \mathbb{N} \quad n = 2k)$	

La logique ne peut pas tout... Il faut maintenant travailler avec les outils mathématiques pour démontrer la conclusion de la colonne de droite en partant des données de la colonne de gauche. Voici un exemple de rédaction qui recopie sans le dire la démonstration du théorème de la division euclidienne (ce qui n'est pas très surprenant puisque le résultat devient évident avec la notion de division euclidienne par 2).

Rédaction. Soit $n \in \mathbb{N}$, et supposons que n ne s'écrit pas sous la forme $2k$ avec $k \in \mathbb{N}$. On va montrer que n s'écrit sous la forme $2k+1$ pour un certain entier k. Pour cela, considérons l'ensemble suivant :

$$K = \{j \in \mathbb{N} \mid 2j > n\}.$$

On voit que l'ensemble K est non vide puisque, par exemple, $n+1 \in K$, ce qui montre que $K \neq \emptyset$.

On sait que tout ensemble d'entiers non vide admet un plus petit élément : on pose donc $j_0 = \min K$. En particulier $j_0 \in K$ et donc $j_0 \neq 0$ puisque $0 \notin K$. Donc $j_0 - 1$ est un entier naturel, et puisque j_0 est le plus petit élément de K, $j_0 - 1 \notin K$. Or, ceci s'écrit : $2(j_0 - 1) \leq n$. Par ailleurs $j_0 \in K$ s'écrit $n < 2j_0$, donc les seules valeurs possibles pour n sont $2(j_0 - 1)$ et $2j_0 - 1$. Or $n = 2(j_0 - 1)$ est exclu d'après notre hypothèse, donc :

$$n = 2j_0 - 1 = 2(j_0 - 1) + 1$$

Comme on a déjà remarqué que $k = j_0 - 1$ est un entier naturel, on obtient bien $n = 2k+1$, ce qu'on voulait prouver. □

4.2.6—Prouver un énoncé de la fome $A \wedge B$

Partant des données X, prouver un énoncé de la forme $A \wedge B$ c'est montrer qu'il existe un chemin logique de X à A d'une part, et un chemin logique de X à B d'autre part. Ainsi, le tableau regroupant les données de départ est équivalent à deux tableaux séparés :

Données	But
X	A

Données	But
X	B

Cependant, imaginons qu'on ait déjà fait la preuve de A sous les hypothèses X. Il peut arriver que A soit utile pour démontrer B. Or, puisqu'on a déjà démontré la validité de A sous les hypothèses X, il est loisible d'utiliser A comme hypothèse supplémentaire. On peut donc tout aussi bien s'intéresser aux deux tableau suivants :

Données	But
X	A

Données	But
X	B
A	

Exemple. *Soit z un nombre complexe $\neq 1$ et tel que $z^3 = 1$. Montrer que $|z| = 1$ et $\mathrm{Im}(z) < 0$.*

Deux tableaux de départ :

Tableau n° 1		Tableau n° 2	
Données	But	Données	But
$z \in \mathbb{C}$	$\lvert z\rvert = 1$	$z \in \mathbb{C}$	$\mathrm{Im}(z) < 0$
$z \neq 1,\ z^3 = 1$		$z \neq 1,\ z^3 = 1$	

Il est facile de montrer dans un premier temps $|z| = 1$ en partant de $z^3 = 1$ puis en passant aux modules. On peut donc se concentrer sur la deuxième assertion à prouver, en rajoutant maintenant l'hypothèse que z est de module 1. On aboutit donc au tableau suivant :

Tableau modifié :

Données	But
$z \in \mathbb{C}$	$\mathrm{Im}(z) < 0$
$z \neq 1,\ z^3 = 1$	
$\lvert z\rvert = 1$	

Pour finir la démonstration, il reste à utiliser le calcul sur les nombres complexes.

Rédaction. Soit z un complexe tel que $z \neq 1$ et $z^3 = 1$. Alors, en passant aux modules dans $z^3 = 1$ on obtient $|z|^3 = 1$, et comme $|z|$ est un réel positif, il s'ensuit que $|z| = 1$. Ceci prouve la première assertion.

Prouvons maintenant que $\mathrm{Im}(z) < 0$. Comme $|z| = 1$, on peut poser $z = \cos(\theta) + \mathbf{i}\sin(\theta)$ pour un unique réel $\theta \in [0, 2\pi[$. D'après la formule d'Euler, on a alors $z^3 = \cos(3\theta) + \mathbf{i}\sin(3\theta)$ et donc $\sin(3\theta) = 0$ et $\cos(3\theta) = 1$ puisque $z^3 = 1$ par hypothèse. Raisonnons par équivalences, en utilisant que $\theta \in [0, 2\pi[$:

$$\begin{cases} \cos(3\theta) = 1 \\ \sin(3\theta) = 0 \end{cases} \iff \exists k \in \mathbb{Z} \quad 3\theta = 2k\pi \iff \exists k \in \mathbb{Z} \quad \theta = \frac{2k\pi}{3} \iff \theta \in \left\{0, \frac{2\pi}{3}, \frac{4\pi}{3}\right\}$$

Or $\theta = 0$ est exclu car ce cas correspond à $z = 1$, donc les deux seules possibilités restantes sont $\theta = 2\pi/3$ et $\theta = 4\pi/3$. Dans les deux cas, on a $\mathrm{Im}(z) = -1/2 < 0$, ce qu'on voulait montrer. □

4.2.7—Prouver la négation d'un énoncé

Il arrive qu'on veuille prouver qu'un énoncé est faux, ce qui correspond à prouver sa négation. Par ailleurs, l'usage de la contraposée introduit des négations en général, comme on l'a vu en 4.2.2.

Pour prouver un énoncé de la forme $\neg P$, la première chose à faire est de développer la négation, autant que possible, pour *in finie* se débarasser entièrement du signe $\neg$. On procède en deux temps :

1. On fait "rentrer" le symbole de négation à l'intérieur des énoncés en utilisant les lois de de Morgan (*cf.* 1.2.2) et leur généralisation aux quantificateurs (*cf.* 1.2.7).
2. Lorsque la négation ne peut pas aller plus loin à l'intérieur, on examine sa signifcation mathématique. Par exemple, la négation "$x < 10$" pour $x \in \mathbb{R}$ est équivalente à "$x \geq 10$", la négation de "n est pair" pour $n \in \mathbb{Z}$ est équivalente à "n est impair" (c'est ce qu'on a vu en 4.2.5).

On est maintenant ramené à un énoncé sans négation, et on peut donc procéder à son analyse comme on l'a vu jusqu'à maintenant.

Exemple. *Montrer que l'énoncé suivant est faux : tout nombre premier est impair.*

Soit P l'énoncé "tout nombre premier est impair". Avec des quantificateurs, l'énoncé P se traduit par :

$$P \ : \quad \forall n \in \mathbb{N} \quad (n \text{ premier} \implies n \text{ impair})$$

On développe $\neg P$ en faisant rentrer la négation à l'intérieur :

$$\begin{aligned} \neg P \ : \quad & \neg\big(\forall n \in \mathbb{N} \quad (n \text{ premier} \implies n \text{ impair})\big) \\ & \exists n \in \mathbb{N} \quad \neg(n \text{ premier} \implies n \text{ impair}) \\ & \exists n \in \mathbb{N} \quad (n \text{ premier} \wedge \neg(n \text{ impair})) \end{aligned}$$

L'analyse logique s'arrête là car on ne peut pas faire rentrer le signe $\neg$ plus loin à l'intérieur. Il faut maintenant analyser la signification de "$\neg(n \text{ impair})$", et on sait d'après l'arithmétique (*cf.* 4.2.5) que c'est équivalent à "n pair". Finalement, $\neg P$ s'écrit donc :

$$\neg P \ : \quad \exists n \in \mathbb{N} \quad (n \text{ premier} \wedge n \text{ pair}).$$

Il nous reste à determiner si on peut trouver un tel entier n, qui soit à la fois premier et pair, et bien sûr $n = 2$ convient, c'est d'ailleurs l'unique entier à la fois premier et pair. La rédaction peut donc être la suivante.

Rédaction. La négation de l'énoncé "tout nombre premier est impair" est équivalente à l'existence d'un entier n à la fois premier et non impair, c'est-à-dire pair. Or $n = 2$ convient. Donc l'énoncé "tout nombre premier est impair" est faux.

Exercice Montrer que l'énoncé suivant est vrai : "tout entier divisible par 4 est divisible par 2", mais que sa réciproque est fausse. Est-il vrai qu'aucun entier divisible par 2 n'est divisible par 4 ?

4.2.8—Raisonnement par équivalences

L'utilisation d'équivalences logiques est l'un des premiers modes de raisonnements qu'on rencontre en mathématiques. Résoudre une équation par exemple, c'est trouver un équivalent "plus simple" de l'équation. Ainsi, lorsqu'on écrit : "les solutions réelles de l'équation $2x^2 - x - 1 = 0$ sont $-1/2$ et 1", on affirme *deux* choses :

1. Toute solution de $2x^2 - x - 1 = 0$ est parmi $\{-1/2, 1\}$.
2. Tout élément de $\{-1/2, 1\}$ est solution de $2x^2 - x - 1 = 0$.

Avec des symboles logiques, on a donc l'énoncé suivant :

$$\forall x \in \mathbb{R} \quad 2x^2 - x - 1 = 0 \iff x \in \left\{-\frac{1}{2}, 1\right\}$$

Remarque sur la terminologie. L'expression "A si et seulement si B" est synonyme de "A est équivalent à B", et est synonyme de "$A \iff B$". Si $A \implies B$, on dit que B est une condition *nécessaire* pour A, et si $B \implies A$ on dit que B est une condition *suffisante* pour B. C'est pourquoi un autre synonyme de $A \iff B$ est l'expression "B est une condition nécessaire et suffisante pour A".

L'utilisation d'équivalences est rendue aisée par la règle logique évidente suivante : les équivalences se composent. Autrement dit, quels que soient les énoncés A, B et C, on a :

$$\text{si } A \iff B \text{ et si } B \iff C, \text{ alors } A \iff C$$

D'autre part, les manipulations algébriques sur les équations sont généralement données dans le cours sous forme d'équivalences. Par exemple, on sait que :

$$\forall a \in \mathbb{R} \setminus \{0\} \quad \forall (b, c) \in \mathbb{R} \times \mathbb{R} \quad \forall x \in \mathbb{R} \quad ax + b = c \iff x = \frac{c - b}{a}$$

L'enchaînement d'équivalences peut donc être un moyen rapide et efficace de raisonner et de résoudre des équations.

Attention, cependant : la rédaction n'en est pas aussi simple qu'il y parait. C'est un défaut très répandu, qui vire à l'habitude, voire à l'automatisme non réfléchi, que de placer un signe « $\iff$ » au début de chaque ligne, pour signifier une suite d'énoncés équivalents sans même prêter attention à la *signification* de ce signe $\iff$. En général les équivalences ainsi énoncées ne sont pas prouvées, ou bien la présentation ne permet pas de comprendre quels sont les énoncés qui sont dits être équivalents. Mieux vaut rédiger plus précisément et plus explicitement.

Une règle utile à adopter est la suivante : faites les calculs *d'abord*, *puis* introduisez les équivalences lorsque vous en avez besoin, comme dans l'exemple suivant.

Exemple. *Cas d'égalité de l'inégalité triangulaire : montrer que, quels que soient $x, y \in \mathbb{R}$, on a $|x + y| = |x| + |y|$ si et seulement si x et y ont même signe.*

On se fixe $x, y \in \mathbb{R}$. Puisque les deux membres de l'équation qui nous intéresse sont des nombres positifs, on sait qu'ils sont égaux si et seulement si leurs carrés sont égaux. L'avantage des carrés est qu'ils permettent de se débarasser des valeurs absolues. En effet, on sait que pour tout nombre réel a, on a $|a|^2 = a^2$, ce qui donne en particulier :

$$\begin{aligned} |x+y|^2 &= (x+y)^2 \\ &= x^2 + y^2 + 2xy \\ (|x| + |y|)^2 &= |x|^2 + |y|^2 + 2|x||y| \\ &= x^2 + y^2 + 2|x||y| \end{aligned}$$

On raisonne à partir de maintenant par équivalences :

$$\begin{aligned} |x+y| = |x| + |y| &\iff |x+y|^2 = (|x| + |y|)^2 && \text{car ces nombres sont } \geq 0 \\ &\iff x^2 + y^2 + 2xy = x^2 + y^2 + 2|x||y| && \text{d'après les calculs précédents} \\ &\iff xy = |xy| \\ &\iff xy \geq 0 \end{aligned}$$

Or un produit de deux nombres est positif si et seulement si ces deux nombres ont même signe. Donc $|x+y| = |x| + |y|$ si et seulement si x et y ont même signe. □

Remarque. Dans la rédaction précédente, remarquez qu'on *n'a jamais supposé que* $|x+y| = |x| + |y|$. On a toujours raisonné à la place *par équivalences*, contrairement à la technique directe d'implication où on suppose l'hypothèse vérifée, à partir de quoi on avance jusqu'à aboutir à la conclusion. En particulier, il aurait été maladroit de conclure par : "Donc x et y ont même signe". Dans la démonstration, on n'affirme jamais la véracité de $|x+y| = |x| + |y|$, on ne fait qu'étudier des propositions qui lui sont équivalentes.

En cas de doute, mieux vaut s'abstenir plutôt que de raisonner par des équivalences qui n'en sont pas. Peut-être n'a-t-on en fait besoin que d'une implication, et pas d'une équivalence. Dans ce cas-là, il est maladroit d'indiquer une équivalence, qui peut se révéler être fausse, alors que seule une implication est utilisée.

Par ailleurs, si on a vraiment besoin de l'équivalence, mais que celle-ci n'est pas claire, il est judicieux de recourir à la technique dite de *double implication* : pour prouver $A \iff B$, on prouve séparément $A \implies B$ et $B \implies A$. Ceci est cohérent avec ce qui a été dit en 4.2.6, puisque $(A \iff B) = (A \implies B) \wedge (B \implies A)$. On se rend compte alors que les preuves des deux implications peuvent être très différentes l'une de l'autre. On renvoie à la preuve du Théorème 3.3 page 24 pour un exemple de telle démonstration. Le cours d'Algèbre linéaire, entre autres, fourmille d'exemples de telles démonstrations.

4.3—Utilisation d'un énoncé au sein d'une preuve

Jusqu'à présent, on s'est intéressé aux manipulations concernant la *conclusion* de l'énoncé à prouver. Nous allons maintenant analyser les manipulations qu'on peut opérer sur les *hypothèses*. Du point de vue des tableaux introduits précédemment, après avoir étudié la colonne de droite, on va maintenant regarder plus attentivement la colonne de gauche.

On observera une dualité d'une colonne à l'autre et entre les opérateurs logiques $\vee$ et $\wedge$, et entre les quantificateurs $\forall$ et $\exists$.

4.3.1—Hypothèse de la forme $A \vee B$, raisonnement par disjonction des cas

Prouver un énoncé P sous une hypothèse de la forme $A \vee B$, c'est prouver une implication de la forme $(A \vee B) \implies P$.

Tableau de départ :

Données	But
$A \vee B$	P

Il faut donc prouver P que ce soit sous l'hypothèse A ou sous l'hypothèse B. On peut le voir en développant l'implication :

$$\begin{aligned}
\big((A \vee B) \implies P\big) &= \big(\neg(A \vee B) \vee P\big) && \text{(définition de l'implication)}\\
&= \big((\neg A \wedge \neg B) \vee P\big) && \text{(loi de de Morgan)}\\
&= (\neg A \vee P) \wedge (\neg B \vee P) && \text{(distributivité de } \vee \text{ sur } \wedge)\\
&= (A \implies P) \wedge (B \implies B) && \text{(définition de l'implication)}
\end{aligned}$$

On est donc amenés à faire deux preuves, ce qui revient à considérer deux nouveaux tableaux.

Deux tableaux modifiés :

Tableau n° 1		Tableau n° 2	
Données	But	Données	But
A	P	B	P

Cette démarche est appelée *raisonner par disjonction de cas*. Elle revient à traiter séparément les deux cas ; remarquer que les deux cas ne sont pas forcément disjoints, autrement dit $A \wedge B$ peut être vrai.

Il est parfois intéressant de faire apparaître une disjonction de cas là où il n'y en a pas *a priori*, comme dans l'exemple suivant.

Exemple. *Montrer que, pour tout entier $n \in \mathbb{N}$, n et n^2 ont même parité.*

On peut raisonner suivant la parité de n. On considère donc les énoncés suivants :

$A =$ "n est pair" $\qquad B =$ "n est impair" $\qquad P =$ "n et n^2 ont même parité"

et on veut montrer l'énoncé :

$$\forall n \in \mathbb{N} \quad (A \vee B) \implies P$$

La rédaction peut être la suivante.

Rédaction. Raisonnons par disjonction de cas suivant la parité de n. Si n est pair, il s'écrit sous la forme $n = 2k$ pour un certain entier k. Alors $n^2 = 4k^2$ donc n^2, qui est pair, est bien de la même parité que n. Et si n est impair, n s'écrit sous la forme $n = 2k + 1$ pour un certain entier k. Alors $n^2 = 4(k^2 + k) + 1$. Donc n^2 est impair, c'est-à-dire de la même parité que n. On voit donc que n et n^2 ont la même parité dans ces deux cas.

Or ces deux cas couvrent toutes les valeurs possibles de l'entier n. Donc on a montré l'énoncé quel que soit n. □

Remarque. Lorsqu'on fait une disjonction de cas, il faut s'assurer que l'ensemble des cas traités couvre bien l'ensemble des cas possibles. Il est recommandé de l'indiquer lors de la rédaction. C'est ce qui est fait à la fin de la rédaction précédente.

La valeur absolue d'un nombre est définie par disjonction de cas. Il est donc naturel de raisonner par disjonction de cas pour analyser des quantités qui font intervenir des valeurs absolues. C'est le cas pour l'exercice suivant.

Exercice Raisonner par disjonction de cas pour prouver que l'équation $|x - 1| + x = 0$ d'inconnue x n'a pas de solution réelle.

4.3.2—Utilisation d'une implication et de quantificateurs

Dans l'exemple suivant tiré de l'Analyse, on va montrer comment on peut tirer parti d'une hypothèse comprenant implication et quantificateurs.

Exemple. *Soit* $(x_n)_{n\geq 0}$ *et* $(y_n)_{n\geq 0}$ *deux suites réelles, et soit* $(z_n)_{n\geq 0}$ *la suite définie par* $z_n = x_n + y_n$. *Montrer que, si* $(x_n)_{n\geq 0}$ *et* $(y_n)_{n\geq 0}$ *tendent vers* 0, *alors* $(z_n)_{n\geq 0}$ *tend vers* 0.

Rappelons la définition de la limite, par exemple pour la suite $(z_n)_{n\geq 0}$ tendant vers 0 :

$$\forall \epsilon > 0 \quad \exists N \in \mathbb{N} \quad \forall n \in \mathbb{N} \quad (n \geq N \implies |z_n| < \epsilon)$$

Nous devons montrer cet énoncé, sous l'hypothèse que le même énoncé a lieu à la fois pour $(x_n)_{n\geq 0}$ et pour $(y_n)_{n\geq 0}$.

Puisque l'énoncé commence par $\forall \epsilon > 0$, on commence par se fixer $\epsilon_0 > 0$. Nous devons maintenant prouver l'existence d'un entier N tel que :

$$\forall n \in \mathbb{N} \quad n \geq N \implies |z_n| < \epsilon_0 \tag{6}$$

Pour cela, on se réfère à la définition de la limite pour $(x_n)_{n\geq 0}$ et pour $(y_n)_{n\geq 0}$. Puisque ces deux suites vérifient, par hypothèse, un énoncé qui est valable *quel que soit* $\epsilon > 0$, nous pouvons en particulier l'appliquer avec $\epsilon_0/2$ à la place de ϵ. On en déduit donc : **utilisation de** $\forall$

$$\exists N \in \mathbb{N} \quad \forall n \in \mathbb{N} \quad (n \geq N \implies |x_n| < \epsilon_0/2)$$
$$\exists N \in \mathbb{N} \quad \forall n \in \mathbb{N} \quad (n \geq N \implies |y_n| < \epsilon_0/2)$$

Il faut bien remarquer que la variable N dans chacun des énoncés ci-dessus est muette. Puisque ces deux énoncés nous affirment l'existence d'un certain entier N, choisissons un tel entier. Chaque énoncé nous fournit un entier, ils sont donc *a priori* différents. Soit donc N_1 d'une part, et N_2 d'autre part, deux entiers tels que : **utilisation de** $\exists$

$$\forall n \in \mathbb{N} \quad n \geq N_1 \implies |x_n| < \epsilon_0/2 \tag{7}$$
$$\forall n \in \mathbb{N} \quad n \geq N_2 \implies |y_n| < \epsilon_0/2 \tag{8}$$

Maintenant, nous posons : $N_3 = \max(N_1, N_2)$. Et alors, nous allons démontrer que l'entier N_3 satisfait l'énoncé (6). Puisque l'énoncé (6) commence par $\forall n \in \mathbb{N}$, pour le démontrer nous commençons par nous fixer un entier $n \in \mathbb{N}$. Il faut alors montrer l'implication $n \geq N_3 \implies |z_n| < \epsilon_0$, et pour cela nous supposons $n \geq N_3$. Alors $n \geq N_1$ et $n \geq N_2$. D'après le choix de N_1 et de N_2, nous avons $|x_n| < \epsilon_0/2$ et $|y_n| < \epsilon_0/2$, ainsi qu'en témoignent les énoncés (7) et (8). Nous appliquons l'inégalité triangulaire pour en déduire : **utilisation de** $\implies$

$$|z_n| \leq |x_n| + |y_n| < \epsilon_0$$

Résumons : on s'est fixé $\epsilon_0 > 0$. En appliquant la définition de la convergence aux suites $(x_n)_{n\geq 0}$ et $(y_n)_{n\geq 0}$, on a trouvé un entier N_3 vérifiant l'énoncé (6). C'est donc qu'un tel entier existe. Ceci montre donc :

$$\forall \epsilon > 0 \quad \exists N \in \mathbb{N} \quad \forall n \in \mathbb{N} \quad n \geq N \implies |z_n| < \epsilon$$

C'est la définition de la convergence de $(z_n)_{n\geq 0}$ vers 0. □

4.4—Preuves particulières

Les techniques qu'on a étudiées jusqu'à maintenant se fondaient exclusivement sur l'analyse syntaxique des hypothèses et des conclusions. Nous allons à présent appliquer ces techniques dans deux types de situation particulière.

4.4.1—Égalité et inclusion d'ensembles

Il est extrèmement fréquent d'être amené à prouver l'égalité ou l'inclusion de deux ensembles. Résoudre une équation par exemple, c'est déterminer l'ensemble de ses solutions.

Il est intéressant d'établir un parallèle entre les preuves d'égalité de deux ensembles, et les raisonnements par équivalence pour montrer l'équivalence de deux énoncés. Pour montrer $A \iff B$, on a vu en 4.2.8 qu'on pouvait soit procéder par équivalences successives, soit en montrant la double implication. De la même façon, pour prouver l'égalité $A = B$ entre deux ensembles A et B, on peut soit procéder par égalités successives, soit procéder par double inclusion, c'est-à-dire montrer séparément $A \subseteq B$ et $B \subseteq A$.

Rappelons que si A et B sont deux parties d'un ensemble U, l'inclusion $A \subseteq B$ correspond à l'énoncé suivant :

$$\forall x \in U \quad x \in A \implies x \in B$$

En conséquence, la méthode directe pour montrer l'inclusion $A \subseteq B$ consiste à :

1. Fixer un élément $x \in A$.
2. Montrer qu'alors $x \in B$.

Illustrons cette méthode avec la notion d'image d'une partie par une application (*cf.* 3.2).

Exemple. *Soit $f : E \to F$ une application, et soit A et B deux parties de E. Montrer que $A \subseteq B \implies f(A) \subseteq f(B)$.*

Rédaction. Supposons $A \subseteq B$, et montrons que $f(A) \subseteq f(B)$. Pour cela, soit $y \in f(A)$. Par définition de $f(A)$, il existe un élément $x \in A$ tel que $y = f(x)$. Nous avons $A \subseteq B$ par hypothèse, donc $x \in B$. Donc y est l'image par f d'un élément de B. Par définition de $f(B)$, cela implique $y \in f(B)$. On a donc montré $f(A) \subseteq f(B)$. □

On peut raisonner par équivalences pour montrer une double inclusion, c'est-à-dire une égalité d'ensembles, comme le montre l'exemple suivant qui utilise la notion d'image réciproque d'un ensemble par une application (*cf.* 3.2).

Exemple. *Soit $f : E \to F$ une application, et soit A et B deux parties de F. Montrer que $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$.*

Rédaction. Soit $x \in E$. Nous avons :

$$\begin{aligned}
x \in f^{-1}(A \cap B) &\iff f(x) \in A \cap B && \text{par définition de } f^{-1}(A \cap B) \\
&\iff (f(x) \in A) \wedge (f(x) \in B) && \text{par définition de } A \cap B \\
&\iff (x \in f^{-1}(A)) \wedge (x \in f^{-1}(B)) && \text{par définition de } f^{-1}(A) \text{ et de } f^{-1}(B) \\
&\iff x \in f^{-1}(A) \cap f^{-1}(B)
\end{aligned}$$

Ceci montre l'égalité des deux ensembles $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$. □

L'exemple suivant illustre la technique par double inclusion.

Exemple. *Soit $f : \mathbb{R}^3 \to \mathbb{R}^3$ une application linéaire, c'est-à-dire vérifiant :*

$$\forall x \in \mathbb{R}^3 \quad \forall y \in \mathbb{R}^3 \quad \forall (\lambda, \mu) \in \mathbb{R} \times \mathbb{R} \quad f(\lambda x + \mu y) = \lambda f(x) + \mu f(y)$$

On appele noyau de f l'ensemble $\ker f = \{x \in \mathbb{R}^3 \mid f(x) = 0\}$. *Montrer que f est injective si et seulement si* $\ker f = \{0\}$.

Rédaction. Montrons d'abord le sens $\Rightarrow$. On suppose donc f injective, et on montre l'égalité $\ker f = \{0\}$. Pour cela, procédons par double inclusion.

1. Inclusion $\{0\} \subseteq \ker f$. En effet, $f(0) = 0$ puisque f est linéaire, donc $0 \in \ker f$, c'est-à-dire $\{0\} \subseteq \ker f$.
2. Inclusion $\ker f \subseteq \{0\}$. Soit $x \in \ker f$. Alors $f(x) = 0$. Or $f(0) = 0$ d'une part, et f est injective par hypothèse d'autre part. Donc $x = 0$, ce qui montre l'inclusion $\ker f \subseteq \{0\}$.

On a donc montré l'égalité $\ker f = \{0\}$, ce qui achève la preuve de l'implication $\Rightarrow$.

Réciproquement, pour le sens $\Leftarrow$, supposons $\ker f = \{0\}$, et montrons que f est injective. Pour cela, soit $x, y \in \mathbb{R}^3$ tels que $f(x) = f(y)$, montrons que $x = y$. En effet, nous avons alors $f(x) - f(y) = 0$, ce qui implique $f(x - y) = 0$ par linéarité de f, c'est-à-dire $(x - y) \in \ker f$. Or le seul élément de $\ker f$ est 0, donc $x - y = 0$ et donc $x = y$. On a montré les deux inclusions, d'où l'équivalence. □

4.4.2—Preuves par l'absurde

Une preuve par l'absurde d'un énoncé P est une démonstration indirecte, consistant à démontrer l'impossibilité de $\neg P$. Pour cela, on pose $Q = \neg P$, et on suppose temporairement que Q est vrai. On montre qu'on aboutit alors à une contradiction.

Les contradictions sont de deux types : soit internes, soit externes. Dans tous les cas, le résultat est le même : on conclue que Q est faux, et donc que P est vrai.

Une contradiction externe est la preuve d'un énoncé que l'on sait par ailleurs être faux, par exemple $1 = 0$. On a donc une preuve de $Q \implies \mathsf{Faux}$. Or, par définition de l'implication, on a :

$$(Q \implies \mathsf{Faux}) = \neg Q \vee \mathsf{Faux} = \neg Q$$

Une preuve de $Q \implies \mathsf{Faux}$ est donc une preuve de $\neg Q$, c'est-à-dire de P.

Une contradiction interne est un énoncé qui contredit l'hypothèse elle-même, c'est-à-dire Q. Ainsi, on obtient une preuve de $Q \implies \neg Q$. Or, par définition de l'implication, on a :

$$(Q \implies \neg Q) = \neg Q \vee \neg Q = \neg Q$$

Donc, obetnir une preuve de $Q \implies \neg Q$ prouve que $\neg Q$ est vrai, c'est-à-dire que P est vrai.

La preuve par l'absurde est parfois utilisée en dernier ressort, quand on n'a pas d'autre idée. Il faut veiller à ne pas en abuser, car, bien que correct, il est maladroit de faire une preuve par l'absurde lorsqu'une preuve directe se présente facilement. Faire une preuve par l'absurde au brouillon peut être un premier essai avant d'essayer ensuite de trouver une preuve directe.

Dans certains cas, la preuve par l'absurde peut faciliter la rédaction, comme c'est le cas dans l'exemple suivant.

Exemple. *Montrer que la suite $(x_n)_{n\geq 0}$ définie par $x_n = (-1)^n$ n'a pas de limite.*

Rédaction. On raisonne par l'absurde. Supposons que $(x_n)_{n\geq 0}$ est convergente, et soit ℓ sa limite. Considérons les deux sous-suites $(y_n)_{n\geq 0}$ et $(z_n)_{n\geq 0}$ définies par $y_n = x_{2n}$ et $z_n = x_{2n+1}$. Alors $(y_n)_n$ est constante égale à 1, et $(z_n)_n$ est constante égale à -1. Comme ce sont des sous-suites de $(x_n)_n$ qui est convergente de limite ℓ, elles doivent avoir même limite, donc $\ell = 1 = -1$, contradiction. Donc l'hypothèse que $(x_n)_{n\geq 0}$ est convergente est fausse. □

Dans l'exemple suivant, on exhibe une contradiction interne.

Exemple. *Soit x un réel vérifiant la propriété suivante :*

$$\forall \varepsilon > 0 \quad x \leq \varepsilon$$

Montrer que $x \leq 0$.

Rédaction. On raisonne par l'absurde, on supposant que $x > 0$. Posons $\varepsilon_0 = x/2$. Alors $\varepsilon_0 > 0$ puisque $x > 0$. Appliquons l'hypothèse avec $\varepsilon = \varepsilon_0$, on obtient $x \leq \varepsilon_0$, c'est-à-dire $x \leq x/2$ et donc $x \leq 0$. Or ceci contredit l'hypothèse $x > 0$, donc celle-ci était absurde. □

4.4.3—Preuves d'unicité

Lorsqu'on a prouvé l'existence d'une solution à un certain problème, il est naturel de s'intéresser à l'unicité de cette solution. Pour autant, les propriétés d'existence et d'unicité sont souvent traitées indépendemment, et les preuves associées peuvent être de nature bien différente. Donnons une définition formelle de ce qu'on appelle l'unicité.

Définition. *Soit $P(x)$ une propriété ayant x comme unique variable libre, x étant une variable prenant ses valeurs dans un ensemble X. On dit que $P(x)$ a la* propriété d'unicité *si :*

$$\forall (x, y) \in X \times X \quad (P(x) \wedge P(y)) \implies x = y.$$

Ainsi, pour définir l'expression "$P(x)$ a une seule solution", on dit "deux solutions x et y pour $P(x)$ et $P(y)$ sont nécessairement égales". En pratique, il est souvent utile d'utiliser directement cette formulation.

Remarque. La définition ci-dessus ne suppose que $P(x)$ a au moins une solution ! Ainsi, existence et unicité sont *a priori* deux propriétés indépendantes. En fait l'unicité est automatiquement vraie si l'existence est fausse. Donc l'unicité n'a d'intérêt que si l'existence est assurée.

Remarque. Supposons qu'on connaisse un élément x_0 tel que $P(x_0)$ est vrai. Alors $P(x)$ a la propriété d'unicité si et seulement si :

$$\forall x \in X \quad P(x) \implies x = x_0 \,.$$

Exercice. Prouver l'équivalence exprimée dans la remarque ci-dessus.

Exemple. *Pour illustrer la propriété d'unicité, détaillons la preuve de l'unicité dans le théorème de la division euclidienne. Rappelons l'énoncé :* Soit a et b deux entiers naturels, avec $b \neq 0$. Alors il existe un unique couple (q, r) d'entiers tels que $a = bq + r$ et $0 \leq r < b$.

Dans cet exemple, l'unicité porte sur le couple (q, r), et elle est assurée à condition que les *deux* propriétés $a = bq + r$ *et* $0 \leq r < b$ soient vraies.

Pour la rédaction de la preuve, on utilise directement la définition de l'unicité énoncée plus haut. Les deux entiers a et b étant fixés avec $b \neq 0$, on considère donc deux couples (q, r) et (q', r') tels que :

$$a = bq + r \tag{9}$$
$$a = bq' + r' \tag{10}$$
$$0 \leq r < b \tag{11}$$
$$0 \leq r' < b \tag{12}$$

Il s'agit de prouver l'égalité des couples $(q, r) = (q', r')$, c'est-à-dire les deux égalités $q = q'$ et $r = r'$. Pour cela, de (9) et (10) on déduit :

$$b(q - q') = r - r'. \tag{13}$$

Il s'ensuite que $r - r'$ est multiple de b. Mais puisque r et r' sont tous les deux compris entre 0 et $b-1$, on a $-b < r - r' < b$. Or le seul multiple de b strictement compris entre $-b$ et b est 0, donc $r - r' = 0$ c'est-à-dire $r = r'$. En injectant $r - r' = 0$ dans (13) on trouve $b(q - q') = 0$, et comme $b \neq 0$ il s'ensuit que $q = q'$. On a bien montré l'égalité cherchée $(q, r) = (q', r)$. □

Remarque. Dans la démonstration ci-dessus, on n'a pas utilisé l'existence d'un couple (q, r) comme dans l'énoncé. Cette existence est l'objet d'une autre démonstration, qu'on ne fera pas ici.

4.5—Récurrences

Excepté pour les preuves d'égalité et d'inclusion des ensembles (4.4.1), les techniques que nous avons vues jusqu'à présent s'appliquaient quel que soit le type d'objet mathématique concerné : ce pouvait être des nombres entiers, des nombres réels, des fonctions, peu importe.

Il existe une méthode spécifique pour prouver des énoncés qui dépendent d'une variable n prenant ses valeurs dans l'ensemble $\mathbb{N}$ des entiers naturels : c'est la preuve par récurrence, aussi appelée preuve par induction.

On utilise généralement sous le même nom de récurrence, et de manière abusive, deux techniques en fait différentes : d'une part la définition d'une suite par récurrence ; et d'autre par la démonstration d'une propriété par récurrence. Nous allons les examiner l'une après l'autre.

4.5.1—Définition par récurrence

On admettra ici le résultat suivant, qui est d'ailleurs très intuitif : si y_0 est un réel, et si $f : \mathbb{R} \to \mathbb{R}$ est une application, alors il existe une unique suite $(x_n)_{n\geq 0}$ de réels vérifiant les deux propriétés suivantes :

1. $x_0 = y_0$ (*initialisation de la suite*).
2. Pour tout entier $n \geq 0$, x_{n+1} se déduit de x_n par $x_{n+1} = f(x_n)$ (*relation de récurrence*).

Exemple. *Soit x un nombre réel. Les puissances successives de x sont les termes de la suite $(u_n)_{n\geq 0}$ définie par récurrence de la façon suivante :*

$$u_0 = 1 \qquad\qquad \forall n \geq 0 \quad u_{n+1} = u_n x$$

On adopte la notation $x^n = u_n$ pour tout entier $n \geq 0$.

La fonction $f : \mathbb{R} \to \mathbb{R}$ intervenant dans la définition par récurrence est définie par $f(y) = xy$. Les premiers termes de la suite des puissances de x sont :

$$x^0 = 1 \qquad x^1 = x \qquad x^2 = x \cdot x \qquad x^3 = x \cdot x \cdot x$$

Dans l'exemple suivant, on garde la même fonction $f(y) = xy$ et donc la même relation de récurrence, mais on initialise la suite à u_0 quelconque au lieu de 1.

Exemple. *La suite géométrique de terme initial u_0 et de raison $x \in \mathbb{R}$ est définie par la relation de récurrence $u_{n+1} = u_n x$.*

En utilisant la notation pour les puissances x^n introduite dans l'exemple précédent, les premiers termes de la suite $(u_n)_{n\geq 0}$ sont les suivantes :

$$u_0 \qquad u_1 = u_0 x \qquad u_2 = (u_0 x)x = u_0 x^2 \qquad u_3 = (u_0 xx)x = u_0 x^3$$

De nombreuses généralisation sont possibles pour la définition d'une suite par récurrence. À la place d'une suite réelle, on peut définir par récurrence une suite de complexes, ou même une suite de matrices.

On peut aussi ne pas se limiter à une dépendence uniquement au terme précédent. Voici un exemple où le prochain terme dépend des deux termes précédents.

Exemple. *La suite de Fibonacci est définie par :*

$$x_0 = 0 \qquad x_1 = 1 \qquad x_{n+2} = x_n + x_{n+1}$$

Les premiers termes de la suite de Fibonacci sont donc :

$$x_0 = 0 \qquad x_1 = 1 \qquad x_2 = 1 \qquad x_3 = 2 \qquad x_4 = 3 \qquad x_5 = 5$$
$$x_6 = 8 \qquad x_7 = 13 \qquad x_8 = 21 \qquad x_9 = 34 \qquad x_{10} = 55 \qquad x_{11} = 89$$

Le symbole $\sum$ est aussi défini par récurrence. Ici, la fonction $f : \mathbb{R} \to \mathbb{R}$ à considérer comme ci-dessus dépendrait aussi de l'entier n, mais au bout du compte, ça ne change rien au principe qui reste toujours le même : voir l'exemple ci-dessous.

Exemple. *Soit $(x_i)_{i\geq 1}$ une suite de nombre réels (ou complexes). On définit par récurrence la suite $(S_n)_{n\geq 0}$ en posant :*

$$S_0 = 0 \qquad S_{n+1} = S_n + x_{n+1}$$

On adopte la notation suivante :

$$S_n = \sum_{i=1}^{n} x_i$$

D'après la définition par récurrence, les premiers termes de la suite $(S_n)_{n\geq 0}$ sont les suivants :

$$S_0 = 0 \qquad S_1 = x_1 \qquad S_2 = x_1 + x_2 \qquad S_3 = x_1 + x_2 + x_3$$

ce qu'on symbolise souvent avec la notation suivante :

$$\sum_{i=1}^{n} x_i = x_1 + \cdots + x_n$$

Notez la convention qu'une somme sur un ensemble d'indices *vide* est nulle. Ainsi, pour $n = 0$, l'ensemble des indices est l'ensemble $\{i \in \mathbb{N} \mid i \geq 1 \wedge i \leq 0\} = \emptyset$, d'où la valeur conventionelle $S_0 = 0$.

Il faut remarquer que la définition par récurrence se prête particulièrement bien à une interprétation algorithmique, et à une implémentation sur machine. Ayant calculé les n premiers termes de la suite, la machine peut se référer à la relation de récurrence pour calculer le $(n+1)^{\text{e}}$ terme.

À retenir La définition par récurrence sert à définir des suites de nombres réels ou complexes. L'immense avantage est qu'on n'a pas besoin de donner une *formule explicite* pour le n^{e} terme de la suite. À la place, il suffit d'initialiser la suite, et d'exprimer le n^{e} terme en fonction d'un ou plusieurs termes précédents.

4.5.2—Démonstration par récurrence

Soit $P(n)$ un énoncé mathématique, ne comportant que n comme variable libre, et où n varie parmi les entiers naturels. On souhaite démontrer l'énoncé suivant, dont on remarque qu'il n'a pas de variable libre :

$$\forall n \in \mathbb{N} \quad P(n)$$

Nous avons vu que la méthode directe consiste à considérer un élément $n \in \mathbb{N}$, et à chercher une preuve de $P(n)$ (*cf.* 4.2.3). Or, il arrive fréquemment que la preuve qu'on cherche pour $P(n)$ s'appuie sur la véracité de $P(n-1)$. On est donc ramené à chercher une preuve de $P(n-1)$. Or, de la même façon, la preuve de $P(n-1)$ s'appuie sur la véracité de $P(n-2)$. On va donc reculer d'un cran à chaque itération, jusqu'à aboutir à chercher la véracité de $P(0)$.

Admettons que $P(0)$ puisse être démontré. On fait maintenant le chemin inverse. Puisque $P(0)$ est vraie, on l'utilise pour démontrer $P(1)$, qu'on utilise à nouveau pour démontrer $P(2)$, etc. Rien ne va empêcher d'arriver ainsi jusqu'à une preuve de $P(n)$, si ce n'est que plus n est grand, plus la preuve s'allonge.

Illustrons les étapes de la méthode pour prouver $P(4)$:

	je démontre $P(0)$
or je sais que $P(0) \implies P(1)$	donc je déduis $P(1)$
or je sais que $P(1) \implies P(2)$	donc je déduis $P(2)$
or je sais que $P(2) \implies P(3)$	donc je déduis $P(3)$
or je sais que $P(3) \implies P(4)$	donc je déduis $P(4)$

Avec cette méthode, on voit que la propriété $P(n)$ peut être démontrée pour tout entier n, ce qui revient à dire que la propriété $\forall n \in \mathbb{N} \quad P(n)$ est vraie. Pour effectuer toutes les étapes, on a besoin des deux ingrédients suivants :

1. $P(0)$ (initialisation)
2. $\forall n \in \mathbb{N} \quad P(n) \implies P(n+1)$ (propriété d'hérédité)

Avant de passer à des exemples pratiques et à la phase de rédaction, voici le théorème qui assure que la méthode de démonstration par récurrence est valide.

Théorème. *Soit $P(n)$ une propriété ne contenant que n comme variable libre, avec n variant parmi les entiers naturels. On suppose que $P(n)$ vérifie les deux propriétés suivantes :*

1. $P(0)$

2. $\forall n \in \mathbb{N} \quad \big(P(n) \implies P(n+1)\big)$

Alors la propriété suivante est vraie : $\forall n \in \mathbb{N} \quad P(n)$.

Démonstration. Posons $Q = \{n \in \mathbb{N} \mid P(n)\}$. On va démontrer que $Q = \mathbb{N}$, ce qui est bien la propriété cherchée.

Pour cela, procédons par l'absurde en supposant que $Q \neq \mathbb{N}$. Alors, en posant $Q' = \mathbb{N} \setminus Q$, l'ensemble Q' est non vide. Comme c'est un ensemble d'entiers, il possède un plus petit élément, soit n_0 cet entier. En tant que son plus petit élément, n_0 appartient à Q'.

Remarquons d'abord que $n_0 > 0$. En effet, on sait que $P(0)$ est vraie, autrement dit $0 \in Q$ et donc $0 \notin Q'$, or $n_0 \in Q'$ donc $n_0 \neq 0$.

Il s'ensuit que $n_0 - 1$ est un entier naturel. Par ailleurs, $n_0 - 1 < n_0$ et n_0 est le plus petit élément de Q'. Donc $n_0 - 1 \notin Q'$, c'est-à-dire $P(n_0 - 1)$. Or, la propriété d'hérédité

est valable pour tous les entiers, donc en particulier pour $n_0 - 1$. Nous avons donc à la fois :

$$P(n_0 - 1) \qquad \text{et} \qquad P(n_0 - 1) \implies P(n_0)$$

On en déduit : $P(n_0)$, donc $n_0 \notin Q'$. C'est une contradiction puisque $n_0 \in Q'$. Donc $Q = \mathbb{N}$, ce qu'on voulait montrer. □

À retenir Une démonstration par récurrence est une technique inductive de preuve, qui s'applique aux propriétés dépendant d'une variable entière.

4.5.3—Rédaction d'une preuve par récurrence

Préliminaires. On gagne toujours en clarté à donner un nom à la propriété qu'on va démontrer par récurrence. Il est par ailleurs important de signaler qu'on fait une preuve par récurrence, et ceci bien sûr *avant* de commencer la preuve. On arrive donc à une formulation de départ telle que celle-ci :

> « Soit la propriété $P(n) : \ldots$ définie pour tout entier $n \in \mathbb{N}$.
> On va prouver par récurrence : $\forall n \in \mathbb{N} \quad P(n)$. »

Les étapes de la récurrence. La rédaction d'une preuve par récurrence se fait en trois étapes que l'on peut résumer ainsi :

1. On prouve la propriété $P(0)$, qui est l'initialisation de la récurrence.
2. On prouve la propriété d'hérédité : $\forall n \in \mathbb{N} \quad P(n) \implies P(n+1)$
3. On conclut à la preuve de : $\forall n \in \mathbb{N} \quad P(n)$

Quelques commentaires concernant l'étape 2, inspirés de confusions souvent répérées dans les copies. Puisqu'il faut montrer une propriété universellement quantifiée, on va sûrement en tenter une preuve directe (*cf.* 4.2.3), et donc considérer un entier $n \in \mathbb{N}$ pour lequel $P(n)$ est vraie. Autrement dit, on se fixe un entier n, et on suppose $P(n)$. Or *ceci n'est pas équivalent à supposer que $P(n)$ est vraie pour tout entier n !*

De plus, à cette étape, on ne *prouve ni* $P(n)$ *ni* $P(n+1)$. Ce qu'on prouve, c'est seulement *l'implication* $P(n) \implies P(n+1)$. Nous renvoyons le lecteur à la section 1.2.4 si la nuance entre la preuve de B et la preuve de $A \implies B$ lui avait échappé.

À retenir On écrit son intention de faire une preuve par récurrence. La rédaction doit en être faite avec soin, en respectant toutes les étapes.

Un exemple de rédaction d'une preuve par récurrence. Les preuves par récurrences s'imposent comme la méthode naturelle de démonstration pour prouver des énoncés portant sur des suites qui ont été définies par récurrence.

Soit u_0 et r deux réels. On a vu plus haut (4.5.1) comment définir la suite géométrique $(u_n)_{n\geq 0}$ de terme initial u_0 et satisfaisant la relation de récurrence $u_{n+1} = ru_n$. En particulier, on a défini le symbole x^n comme le n^{e} terme de la suite géométrique de terme initial 1 et de raison r.

Commençons par démontrer la proposition suivante, en nous basant sur ces deux définitions par récurrence :

$$\forall n \geq 0 \quad u_n = u_0 r^n$$

Rédaction. Pour tout entier $n \geq 0$, posons :

$$P_n \ : \ u_n = u_0 r^n$$

On va montrer par récurrence : $\forall n \geq 0 \quad P_n$.

Initialisation. On a $r^0 = 1$ par définition, donc l'égalité P_0 est vraie.

Hérédité. Soit $n \geq 0$, et supposons P_n. D'après la définition récurrente de la suite $(u_k)_{k\geq 0}$, on a $u_{n+1} = ru_n$. Or $u_n = u_0 r^n$ d'après P_n. Donc $u_{n+1} = u_0 r r^n$. Or $r r^n = r^{n+1}$ d'après la définition récurrente de la suite $(r^k)_{k\geq 0}$, donc $u_{n+1} = u_0 r^{n+1}$, ce qui est P_{n+1}. On a donc montré $P_n \implies P_{n+1}$.

Conclusion. Donc la propriété $u_n = u_0 r^n$ est vraie pour tout entier $n \geq 0$. □

On a également défini en 4.5.1 le symbole

$$\sum_{k=0}^{n} u_k$$

par récurrence. Soit à montrer la proposition suivante, où $(u_k)_{k\geq 0}$ désigne toujours la même suite géométrique :

$$\text{Si } r \neq 1, \text{ alors } \sum_{k=0}^{n} u_k = u_0 \frac{1 - r^{n+1}}{1 - r} \text{ pour tout entier } n \geq 0.$$

Rédaction. Soit $r \neq 1$. Pour tout entier $n \geq 0$, posons :

$$Q_n \ : \ \sum_{k=0}^{n} u_k = u_0 \frac{1 - r^{n+1}}{1 - r}$$

On va montrer par récurrence la proposition $\forall n \geq 0 \quad Q_n$.

Initialisation. Pour $n = 0$, les deux membres de l'égalité dans Q_0 sont égaux à u_0, donc l'égalité a lieu.

Hérédité. Soit $n \geq 0$, et supposons Q_n, on va montrer Q_{n+1}. On a :

$$\begin{aligned} \sum_{k=0}^{n+1} u_k &= \sum_{k=0}^{n} u_k + u_{n+1} && \text{par définition du symbole } \textstyle\sum \\ &= u_0 \frac{1 - r^{n+1}}{1 - r} + u_{n+1} && \text{d'après } Q_n \end{aligned}$$

On a vu plus haut que $u_{n+1} = u_0 r^{n+1}$. Le calcul continue donc ainsi :

$$\begin{aligned} \sum_{k=0}^{n+1} u_k &= u_0 \Big(\frac{1 - r^{n+1}}{1 - r} + r^{n+1} \Big) \\ &= u_0 \frac{1 - r^{n+1} + r^{n+1} - r^{n+2}}{1 - r} && \text{car } r r^{n+1} = r^{n+2} \text{ par déf. de la suite } (r^k)_{k\geq 0} \\ &= u_0 \frac{1 - r^{n+2}}{1 - r} \end{aligned}$$

Ceci montre Q_{n+1} sous l'hypothèse Q_n, donc on a prouvé $Q_n \implies Q_{n+1}$.

Conclusion. On a prouvé par récurrence la propriété $\forall n \geq 0 \quad Q_n$. □