Logique, raisonnements, ensembles

Jeremy Daniel

> Though this be madness, yet there is method in't.
>
> Shakespeare, *Hamlet*

1 Assertions

Définition 1.1 (Assertion)
Une assertion est un énoncé mathématique ayant un sens et auquel on peut associer une (et une seule) valeur de vérité : Vrai ou Faux.

Exemples 1.2
- *"1 + 1 = 2."* est une assertion vraie.
- *"Le triangle ABC de longueurs $AB = 2$, $AC = 3$ et $BC = 4$ est un triangle rectangle."* est une assertion fausse.
- *"n est un entier pair."* n'est une assertion que si l'entier n a été préalablement défini. Dans ce cas, l'assertion peut être vraie ou fausse.
- *"Il fait beau aujourd'hui."* n'est pas une assertion : ce n'est pas un énoncé mathématique.
- *"$3 = 5+$"* n'est pas une assertion : l'énoncé utilise des symboles mathématiques mais on ne peut pas lui donner de sens.

Définition 1.3 (Résultat mathématique)
On donne différents noms aux résultats mathématiques (= assertions vraies) :
- Un *axiome* est supposé vrai par construction. Les axiomes et les règles logiques de démonstration permettent de déduire tous les résultats mathématiques.
- Une *proposition* est une appelation neutre pour désigner un résultat démontré.
- Un *théorème* est une proposition de portée plus importante ; de nombreux théorèmes ont un nom.
- Un *lemme* est un résultat souvent technique, ayant peu d'importance en soi, mais nécessaire pour démontrer d'autres propositions.

- Un *corollaire* est un résultat obtenu immédiatement à partir d'un autre ; c'est parfois une simple reformulation de ce résultat.
- Les *propriétés* d'un objet mathématique sont des propositions portant sur cet objet.

DÉFINITION 1.4 (Conjecture)
Une conjecture est une assertion non démontrée, qu'une partie de la communauté mathématique pense être vraie.

REMARQUE 1.5
Certaines conjectures ont joué un rôle tellement important dans l'histoire des mathématiques qu'il arrive qu'on utilise encore le terme de conjecture pour parler d'un théorème démontré.

EXEMPLES 1.6
- La conjecture de Fermat affirme qu'il n'existe pas d'entiers strictement positifs x, y, z et $n \geq 3$ tels que $x^n + y^n = z^n$.
  Énoncée vers 1650 dans la marge d'un exemplaire des *Arithmétiques* de Diophante, elle a été démontrée en 1995 par Andrew Wiles [1]. On parle encore du théorème de (Fermat-)Wiles.
- La conjecture de Goldbach, énoncée en 1742, affirme que tout entier pair supérieur ou égal à 4 est somme de deux nombres premiers. [2]
- La conjecture des nombres premiers jumeaux, énoncée vers 1850, affirme qu'il existe une infinité de nombres premiers p tels que $p + 2$ est aussi premier. [3]
- La conjecture de Poincaré et l'hypothèse de Riemann font partie de 7 problèmes dits du *Millénaire*, dont la résolution est couronnée d'un prix d'un million de dollars. Posés en 2000, seule la conjecture de Poincaré a été résolue, par le mathématicien russe Grigori Perelman en 2003 [4].
- On définit une fonction f de $\mathbb{N}^*$ dans $\mathbb{N}^*$ définie par $f(n) = 3n + 1$ si n est impair et $f(n) = n/2$ si n est pair. La conjecture de Syracure affirme que, si $N \geq 1$ est un entier quelconque, et si $(u_n)_{n\in\mathbb{N}}$ est la suite définie par $u_0 = N$ et $u_{n+1} = f(u_n)$, pour tout $n \in \mathbb{N}$; alors la suite (u_n) prend un moment la valeur 1. [5] En 2020, on sait que la conjecture est vraie pour tout entier $N \leq 2^{68}$.

---

1. Avec l'aide de Richard Taylor.
2. Harald Helfgott a démontré en 2013 la conjecture de Goldbach faible, affirmant que tout nombre impair strictement supérieur à 5 est somme de 3 nombres premiers.
3. Zhang Yitang a démontré en 2009 qu'il existe une infinité de nombres premiers consécutifs dont l'écart est inférieur à 70 000 000. Cet écart a été réduit à 246 en 2014 par le concours de plusieurs mathématiciens, *via* le projet Polymath.
4. Perelman a refusé le prix et la médaille Fields.
5. Le meilleur résultat sur cette conjecture est dû à Terence Tao en 2019 ; il a été obtenu par des méthodes probabilistes.

2 Calcul propositionnel

Définition 2.1 (Connecteurs logiques)
Soient P et Q deux assertions. On définit des assertions composites NON(P), P ET Q, P OU Q, $P \implies Q$ et $P \iff Q$ par :

- NON(P) est une assertion qui est vraie si P est fausse, et fausse si P est vraie.
- P ET Q est une assertion qui est vraie si les deux assertions P et Q sont vraies, et fausse dans les autres cas.
- P OU Q est une assertion qui est vraie si au moins l'une des assertions P et Q est vraie, et fausse si les deux assertions P et Q sont fausses.
- $P \implies Q$ est une assertion qui est vraie si P est fausse ou si Q est vraie. Elle est fausse dans le seul cas où P est vraie mais Q est fausse.
- $P \iff Q$ est une assertion qui est vraie quand P et Q ont la même valeur de vérité (Vrai ou Faux).

Remarques 2.2

- On peut aussi utiliser les symboles $\neg$, $\wedge$ et $\vee$ pour désigner les connecteurs NON, ET et OU.
- On peut résumer ces définitions en utilisant une table de vérité. Les valeurs de vérité des assertions composites sont données, en fonction de celles de P et Q, par :

P	Q	$\neg P$	$P \wedge Q$	$P \vee Q$	$P \implies Q$	$P \iff Q$
V	V	F	V	V	V	V
V	F	F	F	V	F	F
F	V	V	F	V	V	F
F	F	V	F	F	V	V

Remarques 2.3

- On constate aisément qu'il suffit de deux connecteurs logiques pour définir tous les autres. Par exemple, NON et OU.
- Le connecteur OU est inclusif : si P et Q sont vraies, alors P OU Q aussi.
- La valeur de vérité de $P \implies Q$ est définie comme étant vraie quand P est fausse ; pour comprendre ce choix, il faut se demander ce que signifie qu'une implication est fausse.

Attention !
On prendra garde à ne pas confondre la véracité de l'implication $P \implies Q$ avec la véracité de Q. Par exemple, l'implication $(1 + 1 = 3) \implies (1 = 2)$ est vraie !

Définition 2.4 (Condition nécessaire, condition suffisante)
Soient P et Q deux assertions telles que $P \implies Q$ est vrai. On peut aussi dire que :

- Q se déduit de P ;
- Q est une condition nécessaire de P ;
- P est une condition suffisante de Q ;

- Pour avoir P, il faut avoir/il est nécessaire d'avoir Q
- Pour avoir Q, il suffit/il est suffisant d'avoir P.

DÉFINITION 2.5 (Assertions équivalentes)
Deux assertions P et Q sont équivalentes si elles ont même valeur de vérité, c'est-à-dire si $P \iff Q$ est vraie.

PROPOSITION 2.6
On a les règles de calcul suivantes sur les connecteurs logiques (le symbole = signifiant que les deux membres ont la même valeur de vérité, quelles que soient les valeurs de vérité de P, Q et R) :

- *Distributivité de* ET *sur* OU *:*

$$P \text{ ET } (Q \text{ OU } R) = (P \text{ ET } Q) \text{ OU } (P \text{ ET } R).$$

- *Distributivité de* OU *sur* ET *:*

$$P \text{ OU } (Q \text{ ET } R) = (P \text{ OU } Q) \text{ ET } (P \text{ OU } R).$$

- *Négation de* ET *:*

$$\text{NON}(P \text{ ET } Q) = \big(\text{NON}(P)\big) \text{ OU } \big(\text{NON}(Q)\big).$$

- *Négation de* OU *:*

$$\text{NON}(P \text{ OU } Q) = \big(\text{NON}(P)\big) \text{ ET } \big(\text{NON}(Q)\big).$$

- *Contraposition :*

$$(P \implies Q) = \big(\text{NON}(Q) \implies \text{NON}(P)\big).$$

- *Négation de l'implication :*

$$\text{NON}(P \implies Q) = P \text{ ET } \big(\text{NON}(Q)\big).$$

DÉFINITION 2.7 (Réciproque, contraposée)
Soient P et Q deux assertions. on considère l'assertion $P \implies Q$: sa réciproque est $Q \implies P$; sa contraposée $\text{NON}(Q) \implies \text{NON}(P)$.

ATTENTION !
Une implication et sa contraposée ont même valeur de vérité. Mais en général, il n'y a pas de relation entre les valeurs de vérité d'une implication et de sa réciproque.

EXERCICE 2.8
S'il pleut, alors le sol dehors est mouillé.
Écrire la réciproque et la contraposée de cette assertion ; commenter.

3 Variables, prédicats et quantificateurs

Définition 3.1 (Variable)
Une variable est un symbole (le plus souvent une lettre) désignant un élément d'un ensemble fixé.

Remarque 3.2
Le nom d'une variable a en général peu d'importance mais il est bon de se conformer à un certain standard, par souci de clarté : n, m, p sont souvent utilisés pour désigner des entiers ; x, y des réels ; z, w des complexes.

Définition 3.3 (Prédicat)
Un prédicat est un énoncé mathématique dépendant d'une variable tel que, si on remplace cette variable par une valeur qu'elle peut prendre, on obtient une assertion.
On peut aussi considérer des prédicats dépendant de plusieurs variables.

Exemples 3.4
- n variable entière. *"n est pair"* est un prédicat en la variable entière n.
- x variable réelle. "$x \geq 1$" est un prédicat en la variable réelle x.
- x, y variables réelles. "$x^2 = y$" est un prédicat en les variables réelles x et y
- z variable complexe, n variable entière. "$z^n = 1$" est un prédicat en la variable complexe z et en la variable entière n.

Définition 3.5 (Quantificateurs)
Soit x une variable désignant un élément d'un ensemble E et soit $P(x)$ un prédicat dépendant de la variable x. Alors :
- L'assertion $\exists x \in E : P(x)$ est vraie s'il existe au moins une valeur prise par x telle que l'assertion $P(x)$ (pour cette valeur) est vraie.
- L'assertion $\forall x \in E, P(x)$ est vraie si, pour toutes les valeurs prises par x, l'assertion $P(x)$ (pour ces valeurs) est vraie.

Remarques 3.6
- On parle de quantificateurs existentiel $\exists$ et universel $\forall$.
- Quand un prédicat fait intervenir plusieurs variables, on doit mettre autant de quantificateurs que de variables pour obtenir une assertion.

Remarque 3.7
On dispose aussi d'un quantificateur $\exists!$ qui affirme l'existence et l'unicité d'un élément ayant les propriétés souhaitées.
Si $P(x)$ est un prédicat en la variable x, dans un ensemble E, l'assertion

$$\exists! x \in E : P(x)$$

est équivalente à l'assertion

$$\Big(\exists x \in E : P(x)\Big) \wedge \Big(\forall x \in E, \forall y \in E, \big(P(x) \wedge P(y)\big) \implies (x = y)\Big).$$

Exemples 3.8

- $\exists z \in \mathbb{C}, z^2 = -1$. Cette assertion affirme l'existence d'un nombre complexe de carré -1 : $z = i$ convient donc c'est vrai.
- $\forall x \in \mathbb{R}$, $x^2 > 0$. L'assertion est fausse : le carré du réel 0 n'est pas strictement positif.
- $\forall y \in \mathbb{R}, \exists x \in \mathbb{R}, x > y$. Cette assertion dit que pour tout nombre réel y, il existe un nombre réel x strictement plus grand que y. C'est vrai : on peut prendre par exemple $x = y + 1$.
- $\exists x \in \mathbb{R}, \forall y \in \mathbb{R}, x > y$. Cette assertion dit qu'il existe un nombre réel x, strictement plus grand que tous les nombres réels y. C'est faux : un nombre réel x ne sera jamais plus grand que $x + 1$ par exemple.

Attention !

On ne peut pas en général inverser l'ordre de deux quantificateurs existentiel et universel.

Remarque 3.9

On peut cependant inverser deux quantificateurs existentiels consécutifs ou deux quantificateurs universels consécutifs. Ainsi, on abrègera souvent une écriture du type

$$\exists x \in \mathbb{R} : \exists y \in \mathbb{R} : P(x, y) \quad \text{en} \quad \exists x, y \in \mathbb{R} : P(x, y).$$

De même avec le quantificateur universel.

Proposition 3.10 (Négation d'un quantificateur)

Soit $P(x)$ un prédicat en la variable x, variant dans un ensemble E.

- $\mathrm{NON}\big(\exists x \in E : P(x)\big) = \Big(\forall x \in E, \mathrm{NON}\big(P(x)\big)\Big)$
- $\mathrm{NON}\big(\forall x \in E, P(x)\big) = \Big(\exists x \in E : \mathrm{NON}\big(P(x)\big)\Big)$

Remarque 3.11

Pour nier une assertion quelconque, on procède de gauche à droite, en utilisant ces règles et les négations déjà vues des connecteurs logiques ET, OU et $\implies$.

Exercice 3.12

Soit f une fonction de $\mathbb{R}$ dans $\mathbb{R}$. Formellement, dire que f est croissante signifie :

$$\forall x \in \mathbb{R}, \forall y \in \mathbb{R}, \big(x \leq y \implies f(x) \leq f(y)\big).$$

Écrire la négation de cette assertion.

4 Écrire une démonstration

Quelle que soit la difficulté du résultat qu'on souhaite démontrer, l'écriture de sa démonstration obéira toujours aux mêmes standards. On détaille ce canevas, en distinguant suivant le type d'assertion qu'on cherche à démontrer.

4.1 $P \implies Q$.

On commence la preuve en supposant que P est vraie. On doit aboutir à la conclusion que Q est vraie.

4.2 $P \iff Q$.

L'équivalence $P \iff Q$ est logiquement équivalente à la double implication

$$(P \implies Q) \text{ ET } (Q \implies P).$$

Il s'agit donc de montrer deux implications, l'ordre n'important pas a priori.

Remarque 4.1
On pourra aussi, suivant les cas, raisonner par équivalences successives, c'est-à-dire écrire une chaîne d'assertions équivalentes de proche en proche, démarrant en P et aboutissant en Q. Dans ce cas, il faudra bien faire attention à ce que les assertions successivement écrites soient bien équivalentes entre elles ; c'est-à-dire que le raisonnement doit être vrai dans les deux sens de lecture.

4.3 $\exists x \in E : P(x)$.

On demande de montrer l'existence d'un élément x dans l'ensemble E vérifiant la propriété $P(x)$. Il suffit d'en exhiber un ! La démonstration doit faire figurer une phrase du type *Posons x égal à …* et une justification que le x donné convient bien.

Exercice 4.2
Montrer que $\exists n \in \mathbb{N} : n^2 > n + 1000$.

Résolution
On pose $n_0 = 100$. Alors $n_0^2 = 10000$ et $n_0 + 1000 = 1100$. On a bien

$$n_0^2 > n_0 + 1000.$$

Donc, $\exists n \in \mathbb{N} : n^2 > n + 1000$.

Remarque 4.3
On a choisi de noter n_0 l'élément vérifiant la propriété donnée. On aurait pu l'appeler simplement n ; mais la notation n_0 souligne le fait que cet élément a été fixé et ne correspond pas à une variable muette.

Remarque 4.4
Cas particulier. Si on demande de montrer l'existence et l'unicité d'un objet, on sépare en général les deux arguments. Pour l'unicité, on considère deux objets x et y vérifiant la propriété et on montre l'égalité $x = y$.
On aura rarement besoin de supposer que $x \neq y$: ce n'est pas une démonstration par l'absurde !

4.4 $\forall x \in E, P(x)$.

On demande de montrer que la propriété $P(x)$ est vraie quelle que soit la valeur de x dans E. La démonstration doit commencer par *Soit x dans E* suivi de la démonstration que la propriété $P(x)$ est vraie pour ce x (quelconque dans E).

Exercice 4.5
Montrer que $\forall x \in \mathbb{R}_+ : x^2 + 1 \geq x$.

Résolution
Soit $x \in \mathbb{R}_+$. On a $x^2 + 1 - x = x^2 + 1 - 2x + x = (x-1)^2 + x$. Or, le carré d'un nombre réel est positif et x est aussi positif. Donc $x^2 + 1 - x = (x-1)^2 + x$ est positif, et donc

$$x^2 + 1 \geq x.$$

Remarque 4.6
Paradoxalement, il est en général plus difficile de montrer une propriété du type $\exists x, \ldots$ qu'une propriété du type $\forall x, \ldots$. En effet, dans le premier cas, on doit *trouver* un élément vérifiant les propriétés données, ce qui demande davantage d'initiatives.

4.5 Assertion complexe

On décortique l'assertion à démontrer et on construit sa démonstration morceau par morceau, comme dans un jeu de Lego.

Exercice 4.7
Montrer que $\exists x \in \mathbb{R}, \forall y \in \mathbb{R}, (y \geq x) \implies (y^2 - 3 > 2y)$.

Résolution
Soit $y \in \mathbb{R}$. On a $y^2 - 3 - 2y = (y-1)^2 - 4 = (y+1)(y-3)$.
Posons $x_0 = 4$. Alors, si $y \geq x_0$, on a $y + 1 > 0$ et $y - 3 > 0$. Donc $y^2 - 3 - 2y > 0$, c'est-à-dire $y^2 - 3 > 2y$.

5 Modes de raisonnement

5.1 Par déductions successives

C'est le mode standard de raisonnement mathématique. On part d'une assertion qu'on sait vraie et par une série de déductions (calcul, utilisation de théorèmes du cours, mise en relation avec d'autres données du problème...), on montre qu'une autre assertion est vraie.

Exercice 5.1
On considère un réel $x \geq 4$. Montrer que $\sqrt{x}(x-2) \geq 4$.

Résolution
Par hypothèse, $x \geq 4$. On sait que, sur $\mathbb{R}_+$, la fonction racine carrée est croissante. Donc $\sqrt{x} \geq \sqrt{4} = 2$. De plus, comme $x \geq 4$, on a $x - 2 \geq 2$. Enfin, les inégalités entre nombres réels positifs sont préservées par multiplication ; donc $\sqrt{x}(x-2) \geq 2 \times 2 = 4$.

5.2 Par contraposition

Si P et Q sont deux assertions, l'implication $P \implies Q$ est logiquement équivalente à l'implication $\mathrm{NON}(Q) \implies \mathrm{NON}(P)$, sa *contraposée.* On peut donc préférer montrer la contraposée à l'implication directe.

Exercice 5.2
Soit n un entier naturel. Montrer que si n^2 est impair, alors n est impair.

Résolution
On raisonne par contraposition et on suppose que n est pair. Donc n s'écrit $2 \times m$, où m est un entier naturel. Donc $n^2 = 4m^2 = 2 \times (2m^2)$ et n^2 est pair.
On a donc montré que si n est pair, alors n^2 est pair. Ou, de façon équivalente, que si n^2 est impair, alors n est impair.

5.3 Par l'absurde

Souvent confondu avec le raisonnement par contraposée, le raisonnement par l'absurde consiste – pour montrer qu'une assertion P est vraie – à supposer qu'elle est fausse afin d'aboutir à une contradiction manifeste. Un raisonnement par contraposée ne peut être utilisé que pour montrer une implication, alors qu'un raisonnement par l'absurde peut être utilisé pour n'importe quel type d'assertions.

Exercice 5.3
Montrer que $\sqrt{2}$ est un nombre irrationnel.

Résolution
Par l'absurde, on suppose que $\sqrt{2}$ est un nombre rationnel et on l'écrit sous la forme $\dfrac{p}{q}$

avec p et q deux entiers naturels (avec q non nul). Quitte à écrire la forme irréductible de la fraction, on peut supposer que p et q sont premiers entre eux (ils n'ont pas de diviseur commun positif autre que 1).
Comme $\sqrt{2} = \frac{p}{q}$, on obtient $2q^2 = p^2$ en élevant au carré. Donc, p^2 est un nombre pair. Cela implique que p lui-même est pair (même raisonnement que précédemment). On peut donc écrire $p = 2p'$, avec p' un entier naturel. Alors $2q^2 = (2p')^2$ et donc $q^2 = 2p'^2$. Donc q^2 est pair, et donc q aussi.
On arrive donc à la conclusion que p et q sont tous les deux divisibles par 2, ce qui contredit le fait qu'ils sont premiers entre eux. Donc $\sqrt{2}$ n'est pas un nombre rationnel.

Remarques 5.4

- Quand on raisonne par l'absurde, on l'indique clairement en début de preuve, avec l'hypothèse *absurde* que l'on fait. On explicite aussi clairement la conclusion absurde.
- Le recours à un raisonnement par contraposition ou par l'absurde ne doit pas être automatique. On y pensera quand les négations des assertions en présence sont plus aisées à manipuler que les assertions elles-mêmes.

5.4 Par disjonction de cas

On veut montrer une assertion portant sur un objet mathématique (nombre, fonction...) et on doit faire des preuves différentes selon certains cas. Quand ce n'est pas évident, il faut montrer que la liste ainsi produite de cas couvre toutes les possibilités (mais les cas peuvent se recouper).

Exercice 5.5
Montrer que $\forall x \in \mathbb{R}, x^2 + \cos(x) > 0$.

Résolution
Soit $x \in \mathbb{R}$.

- Cas 1 : $|x| > 1$. Dans ce cas, $x^2 > 1$. Or $\cos(x) \geq -1$. Donc $x^2 + \cos(x) > 1 + (-1) = 0$ et l'égalité est démontrée.
- Cas 2 : $x \in]-\pi/2, \pi/2[$. Dans ce cas, $\cos(x) > 0$. Donc $x^2 + \cos(x) > 0 + 0 = 0$ et l'égalité est démontrée.

Comme $[-1, 1] \subset]-\pi/2, \pi/2[$, x est concerné par l'un ou l'autre de ce cas (ou les deux). Ceci conclut la preuve.

5.5 Par analyse-synthèse

Dans le raisonnement par analyse-synthèse, on doit le plus souvent montrer qu'un objet ayant certaines propriétés existe.
La stratégie consiste à considérer un tel objet et à déterminer certaines conditions qu'il doit satisfaire. C'est *l'analyse.* Puis on considère un objet vérifiant les conditions trouvées et on vérifie s'il satisfait les propriétés qu'on souhaitait initialement. C'est la *synthèse.*

Si l'analyse n'a pas été suffisamment précise, il est tout à fait possible que les conditions trouvées ne soient pas suffisantes. Dans ce cas, la phase de synthèse éliminera certains faux candidats.

Exercice 5.6
Déterminer les x réels tels que $|x-7| = 4x-1$.

Résolution
On procède par analyse-synthèse.
- **Analyse :** Soit x un réel tel que $|x-7| = 4x-1$. On a donc en particulier $|x-7| = |4x-1|$ et donc :
  - ou bien $x-7 = 4x-1$, ce qui entraîne $x = -2$;
  - ou bien $x-7 = -(4x-1)$, ce qui entraîne $x = 8/5$.
- **Synthèse :** Pour $x = -2$, on a $|x-7| = 9 \neq -9 = 4x-1$. Pour $x = 8/5$, on a $|x-7| = 4x-1 (= 27/5)$.
- **Bilan :** Le seul réel x pour lequel $|x-7| = 4x-1$ est $x = 8/5$.

Remarque 5.7
Le raisonnement par analyse-synthèse peut être comparé à une enquête policière. Pour déterminer le(s) coupable(s) d'un crime, on commence par dresser une liste de suspects (l'analyse), puis on les interroge pour déterminer s'ils sont effectivement coupables (la synthèse).
Plus prosaïquement, on établit d'abord des conditions nécessaires sur l'objet recherché, puis on détermine si ces conditions sont suffisantes.
Ainsi, le raisonnement par analyse-synthèse est très proche d'un raisonnement par double implication, à la différence près qu'on ne sait pas *a priori* quelle équivalence on veut montrer.

Remarque 5.8
Quand le raisonnement par analyse-synthèse est utilisé pour démontrer l'existence et l'unicité d'un objet, la phase d'analyse montre en général qu'un seul candidat est possible (ce qui montre l'unicité) tandis que la phase de synthèse consiste en une simple vérification que le candidat convient.

Exercice 5.9
Déterminer les fonctions $f : \mathbb{N} \to \mathbb{N}$ telles que

$$\forall m, n \in \mathbb{N}, f(n+m) = f(n) + f(m).$$

6 Démonstrations par récurrence

Théorème 6.1 (Axiome de récurrence)
Soit $P(n)$ un prédicat dépendant d'une variable $n \in \mathbb{N}$. On suppose vraies les assertions

- $P(0)$
- $\forall n \in \mathbb{N}, P(n) \implies P(n+1)$.

Alors, l'assertion suivante est vraie : $\forall n \in \mathbb{N}, P(n)$.

Remarque 6.2
Dans une démonstration par récurrence, on devra donc successivement :
- démontrer que $P(0)$ est vraie (*l'initialisation*)
- démontrer que si $n \in \mathbb{N}$ est un entier tel que $P(n)$ est vraie, alors $P(n+1)$ est vraie (*l'hérédité*).

Exercice 6.3
Montrer que, pour tout entier naturel n : $5^n \geq n^2 + n + 1$.

Résolution
On montre cette propriété par récurrence sur $n \in \mathbb{N}$.
- Initialisation : pour $n = 0$, on a $5^0 = 1$ et $0^2+0+1 = 1$. Donc on a bien $5^0 \geq 0^2+0+1$.
- Hérédité : soit $n \in \mathbb{N}$ tel que $5^n \geq n^2 + n + 1$. On doit montrer que

$$5^{n+1} \geq (n+1)^2 + (n+1) + 1,$$

c'est-à-dire que

$$5^{n+1} \geq n^2 + 3n + 3.$$

On a

$$\begin{aligned} 5^{n+1} &= 5 \times 5^n \\ &\geq 5(n^2 + n + 1) \text{ (par hypothèse de récurrence)} \\ &\geq 5n^2 + 5n + 5 \\ 5^{n+1} &\geq n^2 + 3n + 3 \text{ (car } 5n^2 \geq 3n^2,\ 5n \geq 3n \text{ et } 5 \geq 3) \end{aligned}$$

On a ainsi démontré la propriété au rang $n+1$.

Par récurrence, on a montré que : $\forall n \in \mathbb{N}, 5^n \geq n^2 + n + 1$.

Corollaire 6.4 (Récurrence double)
Soit $P(n)$ un prédicat dépendant d'une variable $n \in \mathbb{N}$. On suppose vraies les assertions
- $P(0)$
- $P(1)$
- $\forall n \in \mathbb{N}, P(n) \wedge P(n+1) \implies P(n+2)$.

Alors, on a $\forall n \in \mathbb{N}, P(n)$.

Remarque 6.5
On pourrait de même considérer des principes de récurrence triple, quadruple...

Exercice 6.6
On considère $(u_n)_{n\in\mathbb{N}}$ la suite définie par $u_0 = u_1 = 1$ et, pour tout $n \in \mathbb{N}$:

$$u_{n+2} = u_n + u_{n+1}.$$

Montrer que, pour tout $n \in \mathbb{N}$: $u_n \leq (7/4)^n$.

Résolution
On montre cette propriété par récurrence double sur $n \in \mathbb{N}$.

- Initialisation : $u_0 = 1$ et $(7/4)^0 = 1$ donc $u_0 \leq (7/4)^0$. $u_1 = 1$ et $(7/4)^1 = 7/4$ donc $u_1 \leq (7/4)^1$. La propriété est satisfaite aux rangs 0 et 1.
- Hérédité : Soit $n \in \mathbb{N}$ tel que $u_n \leq (7/4)^n$ et $u_{n+1} \leq (7/4)^{n+1}$. On veut montrer que $u_{n+2} \leq (7/4)^{n+2}$. On a

$$\begin{aligned} u_{n+2} &= u_{n+1} + u_n \\ &\leq (7/4)^{n+1} + (7/4)^n \text{ (par hypothèse de récurrence)} \\ &\leq (7/4)^n(7/4+1) \\ u_{n+2} &\leq (7/4)^n \times 11/4. \end{aligned}$$

  De plus, $(7/4)^2 = 49/16 = 44/16 + 5/16 = 11/4 + 5/16$. Donc $(7/4)^2 > 11/4$. On en déduit que

$$u_{n+2} \leq (7/4)^n \times (7/4)^2 = (7/4)^{n+2}.$$

  On a ainsi démontré la propriété au rang $n+2$.

Par récurrence double, on a montré que $\forall n \in \mathbb{N}, u_n \leq (7/4)^n$.

Corollaire 6.7 (Récurrence forte)
Soit $P(n)$ un prédicat dépendant d'une variable $n \in \mathbb{N}$. On suppose vraies les assertions

- $P(0)$
- $\forall n \in \mathbb{N}, P(0) \wedge P(1) \wedge \cdots \wedge P(n) \implies P(n+1)$.

Alors, on a : $\forall n \in \mathbb{N}, P(n)$.

Exercice 6.8
On considère $(u_n)_{n\in\mathbb{N}}$ la suite définie par $u_0 = 3$ et, pour tout entier $n \in \mathbb{N}$:

$$u_{n+1} = \frac{2}{n+1}\sum_{k=0}^{n} u_k.$$

Montrer que, $\forall n \in \mathbb{N}, u_n = 3(n+1)$.

Résolution
On le montre par récurrence forte sur $n \in \mathbb{N}$.

- Initialisation : on a $u_0 = 3$ et $3 \times 1 = 3$. Donc $u_0 = 3 \times 1$.

– Hérédité : soit $n \in \mathbb{N}$ tel que, pour tout $k \in [\![0, n]\!]$, on ait $u_k = 3k$. Montrons que $u_{n+1} = 3(n+2)$. On calcule :

$$\begin{aligned} u_{n+1} &= \frac{2}{n+1} \sum_{k=0}^{n} u_k \\ &= \frac{2}{n+1} \sum_{k=0}^{n} (3k+3) \text{ (hypothèse de récurrence)} \\ &= \frac{6}{n+1} \times \left(\frac{n(n+1)}{2} + (n+1) \right) \\ u_{n+1} &= 3(n+2). \end{aligned}$$

On a ainsi montré la propriété au rang $n+1$.

Par récurrence forte, on a montré que

$$\forall n \in \mathbb{N}, u_n = 3(n+1).$$

Remarques 6.9

Quelques variantes.

– Il arrivera fréquemment qu'on veuille montrer une assertion du type

$$\forall n \geq n_0, P(n),$$

où n_0 est un entier fixé, non nécessairement nul. Les trois types de raisonnement par récurrence discutés se généralisent à cette situation, en adaptant l'initialisation.

– On rencontrera aussi des récurrences finies, pour montrer une assertion du type

$$\forall n \in [\![n_0, n_1]\!], P(n),$$

où $n_0 < n_1$ sont deux entiers naturels. Dans ce cas, l'hérédité consiste à montrer (pour une récurrence simple) que

$$\forall n \in [\![n_0, n_1 - 1]\!], P(n) \implies P(n+1).$$

Remarque 6.10

Avant d'entreprendre un raisonnement par récurrence, il est pertinent de se demander pourquoi la véracité de $P(n)$, pour un entier n quelconque, permet de déduire celle de $P(n+1)$.

Attention !

Dans la très grande majorité des cas, si $(u_n)_{n \in \mathbb{N}}$ est une suite de nombres, on ne montrera pas par récurrence une *propriété de récurrence* sur la suite, c'est-à-dire une propriété liant les valeurs de u_n et u_{n+1} pour tout $n \in \mathbb{N}$.

Au contraire, ces propriétés de récurrence seront utilisées *pour démontrer* – par récurrence ! – d'autres propriétés *absolues* sur u_n.

7 Théorie naïve des ensembles

7.1 Ensembles usuels

Définition 7.1
On rappelle les notations des ensembles de nombres usuels :
- $\mathbb{N} = \{0, 1, 2, 3, \dots\}$: ensemble des entiers naturels ;
- $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$: ensemble des entiers relatifs ;
- $\mathbb{Q}$: ensemble des nombres rationnels (quotients d'entiers)
- $\mathbb{R}$: ensemble des nombres réels ;
- $\mathbb{C}$: ensemble des nombres complexes.

Remarque 7.2
Quand un ensemble a peu d'éléments ou que ses éléments obéissent à un motif, clair dans le contexte, on peut lister explicitement ses éléments.

Exemples 7.3
- $A = \{e, \pi, \ln 2\}$;
- $B = \{1, 2, 3, \dots, 35\}$;
- $C = \{0, 2, 4, 6, \dots\}$, ensemble des entiers naturels pairs ;
- $D = \{1, 2, 4, 8, 16, \dots\}$, ensemble des puissances de 2.

7.2 Principe de sélection

Définition 7.4 (Inclusion)
Soient A et B deux ensembles. On dit que A est inclus dans B (ou que A est une partie de B ; ou que B contient A) et on écrit $A \subset B$ si

$$\forall x \in A, x \in B.$$

Définition 7.5 (Égalité)
Deux ensembles A et B sont égaux si chacun est inclus dans l'autre.

Exemple 7.6
On a l'égalité $\{3, 2, 1, 1, 2\} = \{1, 2, 3\}$.

Remarque 7.7
Si $P(x)$ est un prédicat en la variable x dans un ensemble B, on peut considérer l'ensemble A des $x \in B$ tels que $P(x)$ est vrai. On note

$$A = \{x \in B \mid P(x)\}$$

et on a $A \subset B$.

Exemples 7.8

- $A = \{n \in \mathbb{N} \mid \exists k \in \mathbb{N} : n = 2k\}$ est l'ensemble des entiers naturels pairs.
- $B = \Big\{n \in \mathbb{N} \mid \Big(n \geq 2\Big) \wedge \Big(\forall a, b \in \mathbb{N}, (n = ab) \implies \big((a = 1) \vee (b = 1)\big)\Big)\Big\}$ est l'ensemble des nombres premiers.
- $C = \{x \in \mathbb{R} \mid x^3 - 7x^2 + 5x - 3 = 0\}$ est l'ensemble des racines du polynôme $X^3 - 7X^2 + 5X - 3$.
- Pour tous entiers relatifs a et b tels que $a \leq b$, on note
$$[\![a, b]\!] = \{n \in \mathbb{Z} \mid a \leq n \leq b\}.$$
- On rappelle les notations suivantes pour les parties de $\mathbb{R}$ ($a, b \in \mathbb{R}$ avec $a \leq b$) :
  - $\mathbb{R}_+ = \{x \in \mathbb{R} \mid x \geq 0\}$;
  - $\mathbb{R}_+^* = \{x \in \mathbb{R} \mid x > 0\}$;
  - $\mathbb{R}_- = \{x \in \mathbb{R} \mid x \leq 0\}$;
  - $\mathbb{R}_-^* = \{x \in \mathbb{R} \mid x < 0\}$;
  - $\mathbb{R}^* = \{x \in \mathbb{R} \mid x \neq 0\}$;
  - $[a, b] = \{x \in \mathbb{R} \mid a \leq x \leq b\}$;
  - $[a, b[= \{x \in \mathbb{R} \mid a \leq x < b\}$;
  - $]a, b] = \{x \in \mathbb{R} \mid a < x \leq b\}$;
  - $]a, b[= \{x \in \mathbb{R} \mid a < x < b\}$;
  - $]-\infty, b] = \{x \in \mathbb{R} \mid x \leq b\}$;
  - $]-\infty, b[= \{x \in \mathbb{R} \mid x < b\}$;
  - $[a, +\infty[= \{x \in \mathbb{R} \mid x \geq a\}$;
  - $]a, +\infty[= \{x \in \mathbb{R} \mid x > a\}$
  - $]-\infty, +\infty[= \mathbb{R}$.

Définition 7.9 (Ensemble vide)
On note $\emptyset$ l'ensemble ne contenant aucun élément.

Remarque 7.10
Cet ensemble est unique et est inclus dans tout autre ensemble. Si $P(x)$ est un prédicat toujours faux en la variable $x \in A$, on a $\emptyset = \{x \in A \mid P(x)\}$.

Exemple 7.11
$\emptyset = \{x \in \mathbb{R} \mid x^2 + 1 = 0\}$

7.3 Opérations sur les ensembles

Définition 7.12 (Union, intersection, complémentaire, différence)
Soient Ω un ensemble, A et B deux parties de Ω. On note

- $A \cup B = \{x \in \Omega \mid (x \in A) \text{ OU } (x \in B)\}$ l'union de A et B ;
- $A \cap B = \{x \in \Omega \mid (x \in A) \text{ ET } (x \in B)\}$ l'intersection de A et B ;
- $\overline{A}$ (ou $\overline{A}^{\Omega}$; ou A^c) $= \{x \in \Omega \mid x \notin A\}$ le complémentaire de A dans Ω.
- $A \setminus B = A - B = \{x \in \Omega \mid (x \in A) \text{ ET } (x \notin B)\}$ la différence de A et B.

Proposition 7.13 (Lois de De Morgan)
Soient Ω un ensemble, A, B et C trois parties de Ω.

- *Commutativité :* $A \cup B = B \cup A$; $A \cap B = B \cap A$
- *Associativité :* $A \cup (B \cup C) = (A \cup B) \cup C$; $A \cap (B \cap C) = (A \cap B) \cap C$

- *Distributivité :* $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$; $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
- *Passage au complémentaire :* $\overline{A \cup B} = \overline{A} \cap \overline{B}$; $\overline{A \cap B} = \overline{A} \cup \overline{B}$
- $\overline{(\overline{A})} = A$; $A \cap \overline{A} = \emptyset$; $A \cup \overline{A} = \Omega$; $A \setminus B = A \cap \overline{B}$.

Définition 7.14 (Produit cartésien)
Soient A et B deux ensembles. Le produit cartésien de A et B, noté $A \times B$, est l'ensemble des couples (a, b), où $a \in A$ et $B \in B$.
Deux couples (a, b) et (a', b') sont égaux ssi $a = a'$ et $b = b'$.

Remarque 7.15
On peut généraliser à un nombre fini d'ensembles $E_1, \ldots, E_n$ et considérer le produit cartésien $E_1 \times \cdots \times E_n$.

Définition 7.16 (Puissance d'un ensemble)
Si E est un ensemble et $n \geq 1$ un entier, on note E^n le produit cartésien

$$E^n = E \times \cdots \times E,$$

avec n facteurs E. Un élément de E^n est une n-liste ou un n-uplet d'éléments de E.

Exemples 7.17
- $\mathbb{R}^2$ est l'ensemble des couples de nombres réels. Géométriquement, on peut y penser comme l'ensemble des points (ou des vecteurs) du plan usuel à deux dimensions.
- Si on note E l'ensemble des symboles d'un digicode (par exemple les 10 chiffres et les lettres A et B), alors un code à 4 chiffres est une 4-liste d'éléments de E, c'est-à-dire un élément de E^4.

Attention !
Ne pas confondre le couple (a, b) et la paire $\{a, b\}$ (ensemble contenant uniquement a et b). Par exemple, les couples $(1, 2)$ et $(2, 1)$ sont deux éléments distincts de $\mathbb{R}^2$, tandis que la paire $\{1, 2\} = \{2, 1\}$ est une partie à deux éléments de $\mathbb{R}$.

Définition 7.18 (Ensemble des parties)
Soit E un ensemble. On note $\mathcal{P}(E)$ l'ensemble des parties de E, dont les éléments sont les parties de E.

Remarque 7.19
On a donc $A \subset E \iff A \in \mathcal{P}(E)$.

Exemples 7.20
- Si $E = \{1, 2, 3\}$, on a

$$\mathcal{P}(E) = \Big\{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\Big\}.$$

– Si $F = \emptyset$,
$$\mathcal{P}(F) = \{\emptyset\}.$$

7.4 Plus petit et plus grand éléments d'un ensemble

Définition 7.21 (Partie majorée/minorée de $\mathbb{R}$)
Une partie $X \subset \mathbb{R}$ est majorée si $\exists M \in \mathbb{R} : \forall x \in X, x \leq M$.
Une partie $X \subset \mathbb{R}$ est minorée si $\exists m \in \mathbb{R} : \forall x \in X, x \geq m$.

Proposition 7.22
On pourra librement utiliser les assertions suivantes :
- *Toute partie non vide de $\mathbb{N}$ a un plus petit élément.*
- *Toute partie non vide majorée de $\mathbb{N}$ a un plus grand élément.*
- *Toute partie non vide de $\mathbb{Z}$ minorée/majorée a un plus petit/plus grand élément.*
- *Toute partie non vide et finie de $\mathbb{R}$ a un plus petit et un plus grand élément.*

Attention !
La partie $[0, 1[$ est une partie majorée de $\mathbb{R}$ mais elle n'admet pas de plus grand élément.