Chapitre 0

Prépa begins

I Rudiments de théorie des ensembles.

Définition.

- Un ensemble E est une collection d'objets appelés éléments de E.
- Si x est un élément de E, on note $x \in E$ et on dit que l'objet x appartient à E. Sinon, on note $x \notin E$ et on dit que l'objet x n'appartient pas à E.
- Un ensemble ayant un unique élément est appelé singleton.
- On appelle ensemble vide, et on note $\varnothing$, l'ensemble ne contenant aucun élément.

Remarque : Le but de ce chapitre est de donner les outils et bases nécessaires pour la suite de l'année (par exemple pour prouver ou nier une implication ou effectuer un raisonnement par contraposée), pas de vous changer en spécialistes de logique mathématique ou de théorie des ensembles (et c'est bien dommage). Par conséquent, dans ce chapitre, quand les définitions ou les démonstrations rigoureuses seront trop techniques ou quand leur écriture à l'aide de connecteurs logiques (voir ci-dessous) sera trop obscure, nous nous contenterons d'une approche intuitive (et c'est d'ailleurs le cadre du programme). Rassurez-vous : cela sera largement suffisant pour tout ce qu'on aura à faire cette année.

Comme dit ci-dessous, nous nous contentons de la définition intuitive d'un ensemble comme collection d'objets. Cette définition était la norme jusqu'au XIXe siècle, date à laquelle on a commencé à se rendre compte de l'insuffisance de ces définitions, à cause (ou grâce à ?) de paradoxes comme le paradoxe de Russel (que nous verrons dans exercice 20 du chapitre 4). Pour éviter de tels paradoxes, il était nécessaire de fonder les mathématiques sur des axiomes (cf. IV.1) pour avoir une théorie plus rigoureuse. Il y a beaucoup de systèmes d'axiomes, mais le consensus s'est finalement réalisé sur l'un des plus puissants : la théorie de Zermelo - Fraenkel. À titre d'exemple, dans cette théorie, l'existence de l'ensemble vide découle du schéma d'axiomes de substitution, mais, encore une fois, dans ce chapitre, nous nous contenterons d'une approche intuitive.

II Rudiments de logique.

II.1 Assertions.

Définition. Une assertion (ou un énoncé, ou un prédicat) est une affirmation à laquelle on peut affirmer une valeur de vérité (vraie ou fausse).

Exemples :

- « $1 + 1 = 2$ » est une assertion vraie.
- « $\ln(1) = 1$ » est une assertion fausse.
- « f est dérivable » et « $x = 5$ » sont des assertions dépendant d'une variable (la deuxième peut par exemple s'écrire $A(x)$, et donc $A(x)$ est vraie si $x = 5$ et fausse sinon). Nous verrons ce cas de figure dans le II.6.
- Par contre, les énoncés « $1 + 1$ » ou « bienvenue » ne sont pas des assertions. Le premier est une expression arithmétique dont le résultat est un réel.

Remarque : Le fait qu'un énoncé est soit vrai, soit faux, est appelé « principe du tiers exclu ». Le fait qu'un énoncé ne peut pas être à la fois vrai et faux est appelé « principe de non contradiction ».

II.2 Connecteurs logiques.

Définition. Soient A et B deux assertions.

- On note A et B l'assertion qui est vraie quand A et B sont vraies, et qui est fausse sinon.
- On note A ou B l'assertion qui est vraie quand au moins l'une des deux assertions A ou B est vraie, et qui est fausse sinon (c'est-à-dire si les deux sont fausses).
- On note non(A) l'assertion qui est vraie quand A est fausse, et qui est fausse quand A est vraie.

Le ou mathématique est un « ou » non exclusif : dans le langage courant, A ou B signifie « A ou B ou les deux ». Ce n'est pas « fromage ou dessert » !

Remarques :

- A et B est parfois appelée « conjonction de A et B », et notée $A \wedge B$.
- A ou B est parfois appelée « disjonction de A et B », et notée $A \vee B$.
- non(A) est appelée « négation de A » et est parfois notée $\overline{A}$ ou $\neg A$.

Exemple : On lance un dé à 6 faces. Si A est l'assertion « obtenir un nombre pair » et B est l'assertion « obtenir un nombre strictement supérieur à 3 », alors :

- A ou B est l'assertion « obtenir 2, 4, 5 ou 6 ».
- A et B est l'assertion « obtenir 4 ou 6 ».
- non(A) est l'assertion « obtenir 1, 3 ou 5 ».
- non(B) est l'assertion « obtenir 1, 2 ou 3 ».

C'est le moment d'introduire un outil assez pratique : les tables de vérité.

Définition. Une table de vérité est un tableau qui indique si une assertion P, construite à l'aide de $A, B, C, \ldots$, est vraie ou fausse selon les valeurs de vérité de $A, B, C, \ldots$

Remarque : Plus précisément, une table de vérité est un tableau comportant plusieurs colonnes : dans les colonnes de gauche, on donne les différentes valeurs possibles des différentes assertions entrant en ligne de compte (A, B, C etc.) et dans la colonne de droite, on donne la valeur de vérité, vraie (V) ou fausse (F), correspondante de l'assertion étudiée. La valeur de vérité d'une assertion (sa signature, si l'on veut) est la dernière colonne de sa table de vérité. Le nombre de lignes (sans compter la première) de la table est le nombre de configurations possibles pour les valeurs de vérité des assertions en jeu :

- $4 = 2^2$ lignes s'il y a 2 propositions (VV,VF,FV,FF).
- $8 = 2^3$ lignes s'il y a 3 propositions (VVV,VVF,VFV,VFF,FVV,FVF,FFV,FFF).

Si $n \in \mathbb{N}^*$, il y a 2^n lignes s'il y a n assertions en jeu. Disons que l'assertion dépende de 3 assertions A, B, C : la première colonne consiste en une alternance de 4 F et de 4 V, la deuxième colonne en une alternance de 2 F et de 2 V, et la troisième colonne en une alternance de F et V (cf. II.5 pour un exemple). Dans le cas général, c'est exactement pareil : la première colonne est une alternance de 2^{n-1} F et de 2^{n-1} V, la deuxième colonne est une alternance de 2^{n-2} F et de 2^{n-2} V etc. En remplaçant V par 1 et F par 0, on obtient l'écriture en binaire des entiers de 0 à $2^n - 1$ (cf. chapitre 6).

Exemples : Donnons les tables de vérité des assertions A et B, A ou B et non(A) :

A	B	A et B
F	F	F
F	V	F
V	F	F
V	V	V

A	B	A ou B
F	F	F
F	V	V
V	F	V
V	V	V

A	non(A)
F	V
V	F

II.3 Implications.

Définition. Soient A et B deux assertions. L'assertion « A implique B » est l'assertion notée $A \Rightarrow B$ qui est vraie quand B est vraie à chaque fois que A est vraie, et fausse sinon (c'est-à-dire quand A est vraie et B fausse).

Remarque : Ci-dessous la table de vérité de $A \Rightarrow B$:

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

Remarque : À la place de « A implique B » (est vraie), on peut dire aussi :

- Si A (est vraie), alors B (est vraie).
- A est une condition suffisante pour B.

- Il suffit que A soit vraie pour que B soit vraie.
- B est une condition nécessaire pour A.
- Il faut que B soit vraie pour que A soit vraie.

Exemples :

- Si f est une fonction définie sur $\mathbb{R}$, alors l'implication « f dérivable » $\Rightarrow$ « f continue » est vraie. Par conséquent, le fait que f soit dérivable est une condition suffisante pour qu'elle soit continue, et le fait que f soit continue est une condition nécessaire pour que f soit dérivable.
- Si $x \in \mathbb{R}$, alors l'implication « $x \geqslant 0$ » $\Rightarrow$ « $x + 1 \geqslant 0$ » est vraie.

Remarque : ⚠ Les deux implications données en exemple ci-dessus sont vraies. Cependant, on voit avec ces deux exemples que dire que $A \Rightarrow B$ est vraie **ne signifie pas ou même ne sous-entend pas que A est vraie** : dans nos exemples, cela dépend de f et de x, f n'est pas forcément dérivable et x n'est pas forcément positif, mais **si** f et dérivable ou **si** x est positif **alors** f est continue ou $x + 1$ est positif.

Remarque : Dans la phrase « f est dérivable donc f est continue », on affirme que f est dérivable, ce qui n'est pas le cas avec « si f est dérivable alors f est continue ». De même, dans la phrase « $x \geqslant 0$ donc $x + 1 \geqslant 0$ », on affirme que x est positif, ce qui n'est pas le cas avec « si $x \geqslant 0$ alors $x + 1 \geqslant 0$ ».

Remarque : ⚠ De la définition découle immédiatement le résultat suivant : si A est vraie et si $A \Rightarrow B$ est vraie, alors B est vraie. Ainsi, si on veut prouver B, on peut prouver que A est vraie et que $A \Rightarrow B$ est vraie. C'est le principe du modus ponens ou du syllogisme. Attention cependant : prouver que $A \Rightarrow B$ est vraie ne suffit pas ! Si $A \Rightarrow B$ est vraie, alors B n'est pas forcément vraie ! Il faut prouver également que A est vraie ! En effet, si A est fausse, alors de toute façon $A \Rightarrow B$ est vraie donc on ne prouve rien. Plus fort : à partir d'une assertion fausse, on peut « prouver » tout et n'importe quoi !

⚠ De manière encore plus frappante : d'après la définition et la table de vérité qui en découle, si A est une assertion fausse, alors l'implication $A \Rightarrow B$ est vraie ! $A \Rightarrow B$ est donc vraie dans le cas où A est fausse ! Cela peut sembler curieux au premier abord. Cela vient de l'usage courant du *Si... alors...* qui peut porter à confusion. Une implication est le *Si... alors...* que l'on utilise pour exprimer une règle. Prenons l'exemple des assertions A : « il pleut » et B : « le sol est mouillé ». La règle « S'il pleut, alors le sol est mouillé » est l'implication $A \Rightarrow B$. La règle n'est enfreinte que dans le cas où A est vraie et B est fausse, c'est-à-dire s'il pleut et si le sol est sec. Dans les autres cas elle est respectée. En particulier, elle est respectée s'il fait beau !

Exemple : Faisons comme Gödel et prouvons que si $2 + 2 = 5$ alors je suis le pape.

- Si $2 + 2 = 5$ alors, en enlevant 2 des deux côtés, il vient $2 = 3$.
- En enlevant 1 des deux côtés, il vient $1 = 2$.
- Puisque $1 = 2$, l'ensemble à deux éléments qui contient le pape et moi ne contient en fait qu'un seul élément, donc je suis le pape.

Morale de l'histoire : Le symbole « $\Rightarrow$ » ne peut pas remplacer/n'est pas une abréviation pour le mot « donc ». Si on veut traduire une implication en français, on utilisera « si ... alors ... ».

II.4 Équivalences.

Définition. Soient A et B deux assertions. L'assertion « A et B sont équivalentes » est l'assertion notée $A \iff B$ qui est vraie si A et B sont simultanément vraies ou bien simultanément fausses et qui est fausse sinon. En d'autres termes, A et B sont équivalentes quand elles ont même valeur de vérité.

Remarque : Ci-dessous la table de vérité de $A \iff B$:

A	B	$A \iff B$
F	F	V
F	V	F
V	F	F
V	V	V

Remarque : Dans la suite, quand on écrira $A \iff B$ ou (ce qui revient au même) quand on dira que A et B sont équivalentes, cela signifiera : « l'assertion $A \iff B$ est vraie ».

Exemple : Soit f une fonction dérivable sur un intervalle I. Alors : $f' \geqslant 0 \iff f$ est croissante sur I.

Remarque : De la même façon que dans le paragraphe précédent, écrire $A \iff B$ ne signifie pas que A et B sont toutes les deux vraies, mais que l'une est vraie si et seulement si l'autre est vraie. Si on veut relier deux propositions vraies, on dit « c'est-à-dire » ou « i.e. » (id est, locution latine qui signifie c'est-à-dire), on n'emploie pas la double flèche ! À la limite, on peut remplacer la double flèche par « si et seulement si », mais c'est tout !

En particulier, quand on a les tables de vérité de deux assertions, celles-ci sont équivalentes quand les dernières colonnes de leur tables de vérité respectives sont identiques (voir les exemples ci-dessous).

Remarque : L'équivalence joue pour les assertions le rôle que joue l'égalité pour les nombres. Par exemple les expressions $1+2$ et 3 sont différentes et pourtant $1+2=3$. De façon analogue, si x est un réel, les assertions « $x^2 = 1$ » et « $x = 1$ ou $x = -1$ » ne sont pas identiques et pourtant $(x^2 = 1) \iff (x = 1 \text{ ou } x = -1)$.

Théorème. Soient A et B deux assertions. Alors les deux assertions $A \iff B$ et $((A \Rightarrow B)$ et $(B \Rightarrow A))$ sont équivalentes.

Ce résultat fondamental justifie la validité du raisonnement par double implication (cf. IV.2 et chapitre 1).

DÉMONSTRATION. Vérifions qu'elles ont la même table de vérité. Donnons la table de vérité de $((A \Rightarrow B)$ et $(B \Rightarrow A))$.

A	B	$A \Rightarrow B$	$B \Rightarrow A$	$((A \Rightarrow B)$ et $(B \Rightarrow A))$
F	F	V	V	V
F	V	V	F	F
V	F	F	V	F
V	V	V	V	V

La dernière colonne est la même que celle de la table de vérité de $A \iff B$ ce qui permet de conclure. $\square$

Remarque : Par conséquent, à la place de « A et B sont équivalentes », on peut dire aussi :

- A (est vraie) si et seulement si B (est vraie). D'ailleurs, on a déjà utilisé cette formulation plus haut !
- A est une condition nécessaire et suffisante (CNS) pour B.
- Il faut et il suffit que A soit vraie pour que B soit vraie.

II.5 Résultats en vrac.

II.5.a Associativité de « et » et « ou ».

Théorème. Soient A, B, C trois assertions.

- (A ou B) ou C est équivalente à A ou (B ou C).
- (A et B) et C est équivalente à A et (B et C).

La démonstration est intéressante en elle-même, mais il est plus important de bien comprendre ce résultat intuitivement : si l'on se demande si l'une des assertions A, B ou C est vérifiée, cela revient au même de se demander d'abord si A ou B est réalisée, puis de s'intéresser à C, ou de se demander si B ou C est réalisé, puis de s'intéresser à A. Même chose pour « et ».

DÉMONSTRATION. Comparons les tables de vérité de ((A ou B) ou C) et de (A ou (B ou C)).

A	B	C	A ou B	(A ou B) ou C	B ou C	A ou (B ou C)
F	F	F	F	F	F	F
F	F	V	F	V	V	V
F	V	F	V	V	V	V
F	V	V	V	V	V	V
V	F	F	V	V	F	V
V	F	V	V	V	V	V
V	V	F	V	V	V	V
V	V	V	V	V	V	V

Les deux colonnes correspondantes sont les mêmes donc les deux assertions sont équivalentes. La deuxième équivalence est laissée en exercice.

On voit que ces deux assertions sont fausses seulement dans le cas où A, B et C sont toutes fausses : nous reverrons cela en détail avec les lois de Morgan dans le II.7.a.

Remarque : On dit que « ou » et « et » sont associatives (elles sont également évidemment commutatives, nous reverrons ces deux notions dans le chapitre 18). La principale conséquence est qu'on peut se passer de parenthèses puisque la façon de les mettre n'influe pas sur l'assertion qu'elles forment. Ainsi, on écrira « A ou B ou C » pour signifier « au moins l'une des assertions parmi A, B, C est vraie » et « A et B et C » pour signifier « les assertions A, B, C sont toutes vraies ». On peut évidemment généraliser à plus de trois assertions : on notera « A_1 et $\cdots$ et A_n » pour signifier que toutes les assertions $A_1, \ldots, A_n$ sont vraies, et idem avec « ou » pour signifier qu'au moins l'une de ces assertions est vraie.

Remarque : ⚠ Attention, en général, on ne peut pas se passer de parenthèses ! Par exemple, on peut prouver avec une table de vérité que les deux assertions ((A et B) ou C) et (A et (B ou C)) ne sont pas équivalentes, mais il est plus important de comprendre intuitivement pourquoi (et c'est pour cela que nous ne démontrerons pas toutes les propriétés qui vont suivre) : si A est fausse alors la seconde est fausse, peu importe la véracité de B ou celle de C, tandis que la première est vraie si C est vraie, même si A est fausse !

Autre exemple : les deux assertions $((A \Rightarrow B) \Rightarrow C)$ et $(A \Rightarrow (B \Rightarrow C))$ ne sont pas équivalentes (cf. TD), donc on ne peut pas se passer de parenthèses dans ce cas (peu fréquent).

II.5.b Contraposée.

Définition. Soient A et B deux assertions. La contraposée de l'implication $A \Rightarrow B$ est l'implication $\text{non}(B) \Rightarrow \text{non}(A)$.

Exemples :

- La contraposée de « si je vais au lycée Faidherbe alors je vais au lycée à Lille » est « si je ne vais pas au lycée à Lille alors je ne vais pas au lycée Faidherbe ».
- La contraposée de « s'il neige alors il fait froid » est « s'il ne fait pas froid alors il ne neige pas ».
- La contraposée de « si j'ai mon permis de conduire alors je suis majeur » est « si je suis mineur alors je n'ai pas mon permis de conduire ».
- La contraposée de « si f est dérivable alors f est continue » est « si f n'est pas continue alors f n'est pas dérivable ».

Théorème. Soient A et B deux assertions. L'implication $A \Rightarrow B$ est équivalente à sa contraposée.

En d'autres termes, une implication et sa contraposée sont soit toutes les deux justes, soit toutes les deux fausses. C'est le principe du raisonnement par contraposée, cf. chapitre 1.

Démonstration. On peut le prouver facilement avec une table de vérité, mais il est plus important de s'en convaincre intuitivement avec les exemples ci-dessus : $\rightsquigarrow$ Exercice.

Remarque : ⚠ La contraposée d'une implication ne doit pas être confondue avec sa réciproque ! La réciproque de $A \Rightarrow B$ est $B \Rightarrow A$, et une implication et sa réciproque sont indépendantes, elles peuvent être toutes les deux vraies (par exemple le théorème de Pythagore et sa réciproque sont tous les deux vrais), toutes les deux fausses, ou l'une peut être vraie et l'autre fausse. Par exemple, les quatre implications ci-dessus sont vraies mais les quatre réciproques sont fausses.

II.5.c Transitivité de l'implication et de l'équivalence.

Théorème. Soient A, B et C trois assertions.

- Si $A \Rightarrow B$ et $B \Rightarrow C$ sont vraies alors $A \Rightarrow C$ est vraie.
- Si A et B sont équivalentes, et si B et C sont équivalentes, alors A et C sont équivalentes.

Remarque : Là aussi, on pourrait le prouver, mais il est plus important de les comprendre et de se forger une intuition claire. On peut évidemment généraliser à un plus grand nombre d'assertions. Ces deux résultats sont utiles quand on veut prouver des équivalences successives, cf. IV.2 et chapitre 1.

II.6 Quantificateurs.

Comme on l'a dit en début de chapitre, le but de ce chapitre n'est pas de vous transformer en spécialiste de logique mathématique. Quand on fait les choses bien, parler de quantificateurs est assez technique donc, dans ce paragraphe, on zappera des démonstrations et on se contentera souvent d'une approche intuitive. Mieux encore : il sera plus important de se forger une intuition claire et de bien comprendre les résultats vrais ou faux ci-dessous, de comprendre quelles assertions sont équivalentes et lesquelles ne le sont pas, plutôt que d'apprendre par cœur tous ces résultats (profitez-en, je ne dis pas ça souvent).

Définition. Soit $A(x)$ une assertion dépendant d'une variable x appartenant à un ensemble E.

- L'assertion « $\forall x \in E, A(x)$ » est l'assertion vraie si $A(x)$ est vraie pour tout x appartenant à E, et fausse sinon. « $\forall$ » est appelé « quantificateur universel ».
- L'assertion « $\exists x \in E, A(x)$ » est l'assertion vraie s'il existe (au moins) un x appartenant à E tel que $A(x)$ soit vraie, et fausse sinon. « $\exists$ » est appelé « quantificateur existentiel ».
- L'assertion « $\exists! x \in E, A(x)$ » est l'assertion vraie s'il existe un unique x appartenant à E tel que $A(x)$ soit vraie, et fausse sinon.

« $\forall$ » se lit « pour tout » (c'est le A de « alle » à l'envers) ou « quel que soit », « $\exists$ » se lit « il existe » et « $\exists!$ » se lit « il existe un unique ». Attention, ce sont des quantificateurs, pas des abréviations, cf IV.2. Il n'aura pas échappé aux plus perspicaces d'entre vous que « quel que soit » (qu'on peut, le cas échéant, écrire au féminin et/ou au pluriel) s'écrit en trois mots ! C'est décidé, on n'écrira donc jamais d'horreur du type « quelque soit ».

Remarque : Comme dit ci-dessus, en mathématiques, quand on dit qu'il existe un objet x qui vérifie une propriété, il est sous-entendu « au moins un ». Quand on veut préciser que cet objet est unique, on le dit explicitement.

Remarque : On généralise aisément à plus d'une variable et plus d'un quantificateur. Par exemple, si A est une assertion portant sur les éléments de deux ensembles E et F, alors l'assertion « $\forall x \in E,\ \exists y \in F,\ A(x,y)$ » est l'assertion qui est vraie si, pour tout $x \in E$, il existe $y \in F$ (dépendant de x, voir ci-dessous) tel que $A(x,y)$ soit vraie, et qui est fausse sinon.

Exemples :

- Le fait que la fonction cos est majorée par 1 sur $\mathbb{R}$ s'écrit : $\forall x \in \mathbb{R}, \cos(x) \leqslant 1$.
- Le fait que 2 admet une racine carrée s'écrit : $\exists y \in \mathbb{R},\ y^2 = 2$.
- Le fait que tout réel positif admet une unique racine carrée positive s'écrit : $\forall x \in \mathbb{R}_+,\ \exists! y \in \mathbb{R}_+,\ y^2 = x$.

Remarques :

- Le x dans « $\forall x \in E,\ A(x)$ », dans « $\exists x \in E,\ A(x)$ » et dans « $\exists!\, x \in E,\ A(x)$ » est une variable dite **muette** (ou **liée**). Cela signifie que :
  - ⋆ On peut remplacer x par une autre « lettre » (qui n'est pas déjà utilisée pour définir un autre objet). Par exemple, on peut écrire « $\forall y \in E,\ A(y)$ » au lieu de « $\forall x \in E,\ A(x)$ ». Ou même « $\forall \heartsuit \in E, A(\heartsuit)$ » !
  - ⋆ Le x n'est pas utilisable dans la suite en tant qu'objet précis (il est **lié** au quantificateur, il a une portée uniquement locale : il n'existe, il n'est défini que dans l'assertion). Notamment si on sait que l'assertion « $\exists x \in E,\ A(x)$ » est vraie et que l'on veut l'utiliser pour démontrer une autre assertion, on commencera par écrire

    « Soit x un élément de E qui vérifie l'assertion A ».

    Dans ce cas le x n'est plus une variable muette mais un objet précis (qui vérifie A). On dit aussi que la variable est **libre**.

On mettra parfois des parenthèses pour indiquer la zone de validité d'une variable. En dehors de cette zone, la variable est libérée de sa signification, on peut la réutiliser, la redéfinir. Voir les exemples avec le cosinus et avec la fonction cube ci-dessous.

- « $\exists!\ x \in E,\ A(x)$ » est une notation condensée de l'assertion

$$\exists x \in E,\ \big(A(x) \text{ et } (\forall y \in E,\ A(y)\ \Rightarrow\ x = y)\big)$$

  signifiant deux choses :

  ⋆ Il existe un élément x de E vérifiant A.

  ⋆ Si un élément y de E vérifie A, alors $y = x$. Autrement dit x est le seul élément de E à vérifier A.

On voit qu'on peut exprimer ! en fonction de $\forall$ et $\exists$: on pourrait donc n'utiliser que ces deux quantificateurs, mais cela rendrait certaines assertions beaucoup plus lourdes ! Ce sera la même idée avec le connecteur de Sheffer, cf. exercice 3.

Théorème. Soit A une assertion portant sur les éléments de deux ensembles E et F.

- Les assertions « $\forall x \in E, \forall y \in F, A(x,y)$ » et « $\forall y \in F, \forall x \in E, A(x,y)$ » sont équivalentes.
- Les assertions « $\exists x \in E, \exists y \in F, A(x,y)$ » et « $\exists y \in F, \exists x \in E, A(x,y)$ » sont équivalentes.

Remarque : En d'autres termes, on peut intervertir deux quantificateurs identiques. En effet, si une propriété est vraie pour tous x et y, cela n'a aucune importance de prendre x ou y en premier. De même, s'il existe x et y tels que la propriété soit vraie pour x et y, cela importe peu qui a été choisi d'abord.

Remarque : On fera bien attention à l'ordre des quantificateurs : si A est une assertion portant sur les éléments de deux ensembles E et F, alors les propositions

$$\text{« } \forall x \in E,\ \exists y \in F,\ A(x,y) \text{ »} \qquad \text{et} \qquad \text{« } \exists y \in F,\ \forall x \in E,\ A(x,y) \text{ »}$$

n'ont pas la même signification a priori. La première signifie que, pour chaque élément x de E, il existe y dans F (dépendant éventuellement de x) tel que $A(x,y)$ est vrai. La seconde signifie qu'il existe un y dans F tel que, quel que soit x dans E, $A(x,y)$ est vrai (le y universel : c'est le même pour tous les x). De façon générale, quand un objet est défini après un autre, il peut dépendre de l'objet défini avant. Illustrons-cela avec un exemple :

- L'assertion « $\forall x \in \mathbb{N},\ \exists y \in \mathbb{N},\ x < y$ » (qui signifie que, pour tout entier naturel x, il existe un entier naturel y tel que $x < y$) est vraie (pour tout x dans $\mathbb{N}$, $y = x + 1$ convient).
- L'assertion « $\exists y \in \mathbb{N},\ \forall x \in \mathbb{N},\ x < y$ » (qui signifie qu'il existe un entier naturel qui est strictement supérieur à tous les entiers naturels) est fausse.

Donnons un exemple issu de la vie quotidienne : si on dit « il existe un film que tous les élèves préfèrent », cela signifie que tous les élèves ont le même film préféré (ce qui est sans doute faux), tandis que si on dit « pour tous les élèves, il existe un film qu'ils préfèrent », cela signifie que tous les élèves ont un film préféré, pas forcément le même (ce qui est sans doute vrai). Morale de l'histoire : on ne peut pas intervertir $\exists$ et $\forall$ (sauf cas particulier, mais cela découle alors d'un argument mathématique, cf. exercice 8 ou, par exemple, le théorème de Heine au chapitre 13).

Remarques : Donnons d'autres exemples d'assertions équivalentes ou non (encore une fois, ce n'est pas forcément la peine d'apprendre ce qui suit, mais il faut bien le comprendre et savoir donner un contre-exemple facilement pour les assertions non équivalentes). On se donne dans la suite deux assertions A et B dépendant d'une variable x appartenant à un ensemble E.

- ⚠ Les assertions « $(\forall x \in E, A(x))$ ou $(\forall x \in E, B(x))$ » et « $\forall x \in E, (A(x)$ ou $B(x))$ » ne sont pas équivalentes. En effet, la première signifie que A est toujours vraie ou que B est toujours vraie, tandis que la seconde signifie que tout élément x de E vérifie A ou B (mais pas forcément toujours la même). Par exemple la proposition « $\forall x \in \mathbb{R},\ (\cos(x) \geqslant 0$ ou $\cos(x) \leqslant 0)$ » n'est pas équivalente à la proposition « $(\forall x \in \mathbb{R}, \cos(x) \geqslant 0)$ ou $(\forall x \in \mathbb{R}, \cos(x) \leqslant 0)$ ». En effet la première proposition est vraie mais la seconde est fausse (le cosinus n'est pas de signe constant).
- Les assertions « $(\forall x \in E, A(x))$ et $(\forall x \in E, B(x))$ » et « $\forall x \in E, (A(x)$ et $B(x))$ » sont équivalentes. En effet, elles signifient toutes les deux que A et B sont vraies pour tout élément x de E.
- Les assertions « $(\exists x \in E, A(x))$ ou $(\exists x \in E, B(x))$ » et « $\exists x \in E, (A(x)$ ou $B(x))$ » sont équivalentes. En effet, elles signifient toutes les deux que l'une des deux assertions A ou B est vraie pour au moins un élément x de E.

- Les assertions « $(\exists x \in E, A(x))$ et $(\exists x \in E, B(x))$ » et « $\exists x \in E, (A(x)$ et $B(x))$ » ne sont pas équivalentes. En effet, la seconde signifie qu'il existe un (même) élément x de E qui vérifie A et B tandis que la première signifie qu'il existe un élément x de E qui vérifie A et un élément x de E qui vérifie B, mais les deux éléments ne sont pas forcément les mêmes ! Par exemple, les assertions « $(\exists x \in \mathbb{R}, x^3 > 0)$ et $(\exists x \in \mathbb{R}, x^3 < 0)$ » et « $\exists x \in \mathbb{R}, (x^3 > 0$ et $x^3 < 0)$ » ne sont pas équivalentes. En effet, la première est vraie car la fonction cube prend des valeurs strictement positives et strictement négatives, mais la seconde est fausse car un réel ne peut pas être à la fois strictement positif et strictement négatif. Par conséquent, la première assertion sera plutôt notée « $(\exists x \in \mathbb{R}, x^3 > 0)$ et $(\exists y \in \mathbb{R}, y^3 < 0)$ » pour éviter tout risque de confusion et insister sur le fait que les deux éléments ne sont pas forcément égaux.

On voit une illustration du fait évoqué ci-dessus : les quantificateurs ont une portée locale : x n'existe que dans les parenthèses à l'intérieur desquelles il est défini. En particulier, il n'y a pas de « conflit d'intérêt » entre les différentes définitions de x.

Morale de l'histoire : Faire preuve de bon sens !

II.7 Négation d'une assertion.

Rappel : Si A est une assertion, non(A) est l'assertion vraie quand A est fausse, et fausse quand A est vraie.

II.7.a Lois de Morgan.

Théorème (Lois de Morgan). Soient A et B deux assertions.

- La négation de $(A$ ou $B)$ est équivalente à (non(A) et non(B)).
- La négation de $(A$ et $B)$ est équivalente à (non(A) ou non(B)).

Remarque : Là aussi, on le prouverait très facilement à l'aide de tables de vérité, mais il est plus important de bien comprendre ce résultat et de se forger une intuition solide à l'aide des exemples qui suivent.

Exemples :

- La négation de « $\underbrace{\text{Il a 17 ans}}_{A}$ ou $\underbrace{\text{il a 18 ans}}_{B}$ » est « $\underbrace{\text{Il n'a pas 17 ans}}_{\text{non}(A)}$ et $\underbrace{\text{il n'a pas 18 ans}}_{\text{non}(B)}$ ».
- La négation de « J'ai $\underbrace{\text{plus de 10 ans}}_{A}$ et $\underbrace{\text{moins de 100 ans}}_{B}$ » est « J'ai $\underbrace{\text{moins de 10 ans}}_{\text{non}(A)}$ ou $\underbrace{\text{plus de 100 ans}}_{\text{non}(B)}$ ».

Remarque : On généralise aisément à plus de deux assertions.

Théorème (Lois de Morgan). Soient $n \geqslant 1$ et $(A_1, \dots, A_n)$ des assertions.

- La négation de $(A_1$ ou $\cdots$ ou $A_n)$ est équivalente à (non(A_1) ou $\cdots$ ou non(A_n)).
- La négation de $(A_1$ et $\cdots$ et $A_n)$ est équivalente à (non(A_1) et $\cdots$ et non(A_n)).

En clair : on échange les « ou » et les « et » et on nie les assertions. C'est intuitif (et d'ailleurs on a déjà vu le cas $(A$ ou B ou $C)$) : une disjonction est fausse quand toutes les assertions sont fausses, et une conjonction est fausse quand au moins l'une est fausse. Ce résultat est à rapprocher des lois de Morgan, version ensembliste, que nous verrons dans le chapitre 4.

Remarque : Nous ne mettons pas de parenthèses entre les différentes assertions ci-dessus car nous avons vu plus haut que « ou » et « et » sont associatives. Attention cependant : si on mélange les deux, les parenthèses sont obligatoires ! Par exemple, nous avons déjà vu que les deux assertions $((A$ et $B)$ ou $C)$ et $(A$ et $(B$ ou $C))$ ne sont pas équivalentes, et donc leurs négations ne sont pas non plus équivalentes.

II.7.b Négation d'une implication et d'une équivalence.

Théorème. Soient A et B deux assertions. La négation de $(A \Rightarrow B)$ est équivalente à A et non(B).

Remarque : Là aussi, remarquons que ce résultat est totalement intuitif. L'assertion $A \Rightarrow B$ peut être traduite par « si A alors B » ou encore « si A est réalisé alors B l'est ». La négation est « A est réalisé sans que B le soit » ou encore « A est réalisé et B ne l'est pas », c'est-à-dire « A et non(B) ».

Attention, la négation de « $A \Rightarrow B$ » n'est pas « non$(A) \Rightarrow B$ » ou autre joyeuseté du même genre. C'est intuitif ! Si je vous dis « s'il pleut alors le sol est mouillé » et que vous voulez me prouver que j'ai tort, me dire « ben non Monsieur, il fait beau » ne suffit pas ! Il faut me dire « ben non Monsieur, il pleut et le sol est sec ».

Exemple : La négation de « f dérivable $\Rightarrow f$ continue » est « f dérivable et f n'est pas continue ».

Remarque : Si l'on veut donner la négation d'une équivalence $A \iff B$, il suffit de l'écrire sous la forme « $((A \Rightarrow B)$ et $(B \Rightarrow A))$ » et on se ramène à ce qui précède.

II.7.c Et avec des quantificateurs ?

Proposition. Soit A une assertion portant sur les éléments d'un ensemble E.

- La négation de l'assertion « $\forall x \in E,\ A(x)$ » est « $\exists x \in E,\ \text{non}(A(x))$ ».
- La négation de l'assertion « $\exists x \in E,\ A(x)$ » est « $\forall x \in E,\ \text{non}(A(x))$ ».

Par conséquent, pour prouver qu'une assertion est fausse, il suffit d'exhiber UN contre-exemple (EXPLICITE). Attention, pour prouver qu'une assertion est vraie, exhiber un exemple ne suffit pas !

Exemples :

- La négation de « Tous les chats sont gris » est « Il existe un chat qui n'est pas gris ».
- La négation de « Tous les élèves de la classe sont des garçons » est « il y a au moins une fille dans la classe ».
- La négation de « Il y a un élève qui a son permis de conduire » est « Aucun élève n'a son permis de conduire ».

Rappel : La négation d'une assertion A est non(A), l'assertion vraie quand A est fausse, et fausse quand A est vraie. Elle ne doit pas être confondue avec « sa parfaite opposée » (qui serait d'ailleurs difficile à définir rigoureusement). Par exemple, la négation de l'assertion ci-contre n'est **pas** : « aucun chat n'est gris » ! De même, la négation de « tous les élèves de la classe sont des garçons » n'est pas « tous les élèves de la classes sont des filles » !

Remarque : On peut nier une assertion contenant plus d'un quantificateur et plus d'une variable exactement de la même façon. Plus précisément, on cherche à nier une assertion du type :

$$\left\{\begin{array}{l}\forall\\ \exists\end{array}\right. x_1 \in E_1, \left\{\begin{array}{l}\forall\\ \exists\end{array}\right. x_2 \in E_2, \dots, \left\{\begin{array}{l}\forall\\ \exists\end{array}\right. x_n \in E_n, \qquad A(x_1, \dots, x_n)$$

(c'est-à-dire que devant chaque variable x_i se trouve soit un $\forall$ soit un $\exists$) où $A(x_1, \dots, x_n)$ est une assertion dépendant des variables $x_1, \dots, x_n$. **La négation est obtenue en interchangeant $\forall$ et $\exists$ et en niant $A(x_1, \dots, x_n)$:**

$$\left\{\begin{array}{l}\exists\\ \forall\end{array}\right. x_1 \in E_1, \left\{\begin{array}{l}\exists\\ \forall\end{array}\right. x_2 \in E_2, \dots, \left\{\begin{array}{l}\exists\\ \forall\end{array}\right. x_n \in E_n, \qquad \text{non}(A(x_1, \dots, x_n))$$

Exemple : La négation de « $\exists y \in \mathbb{N}, \forall x \in \mathbb{N}, x < y$ » est « $\forall y \in \mathbb{N}, \exists x \in \mathbb{N}, x \geqslant y$ ».

Attention, il ne faut nier que A et pas les appartenances préalables : la négation de « $\forall x \in E, \dots$ » n'est pas « $\exists x \notin E, \dots$ ». Il faut également faire attention car, parfois, on écrit ces appartenances sous une forme condensée, et on peut confondre les appartenances et l'assertion A.

- Par exemple, on écrit parfois par abus de notation « $\forall x \leqslant y,\ A(x,y)$ » pour « $\forall x \in \mathbb{R}, \forall y \in \mathbb{R}, x \leqslant y \Rightarrow A(x,y)$ ». La négation de cette phrase (version longue) est « $\exists x \in \mathbb{R}, \exists y \in \mathbb{R}, x \leqslant y$ et non$(A(x,y))$ », c'est-à-dire (version courte) « $\exists x \leqslant y,\ \text{non}(A(x,y))$ », et surtout pas « $\exists x > y,\ \text{non}(A(x,y))$ » !
- De même, « $\forall \varepsilon > 0, A(\varepsilon)$ » signifie « $\forall \varepsilon \in \mathbb{R}_+^*, A(\varepsilon)$ » et donc sa négation est « $\exists \varepsilon \in \mathbb{R}_+^*, \text{non}(A(\varepsilon))$ », c'est-à-dire « $\exists \varepsilon > 0, \text{non}(A(\varepsilon))$ », et surtout pas « $\exists \varepsilon \leqslant 0, \text{non}(A(\varepsilon))$ » !

En pratique, il n'est pas nécessaire de détailler autant, on peut donner la négation « version courte » directement, mais attention à ne pas aller trop vite et à ne pas nier ce qui ne relève pas de l'assertion A !

Exemple : La négation de « $\forall \varepsilon > 0, \exists n_0 \in \mathbb{N}, \forall n \geqslant n_0, |u_n - L| \leqslant \varepsilon$ » est « $\exists \varepsilon > 0, \forall n_0 \in \mathbb{N}, \exists n \geqslant n_0, |u_n - L| > \varepsilon$ ».

Remarque : On a déjà vu que « $\exists! x \in E,\ A(x)$ » s'écrit également :

$$\exists x \in E,\ \big(A(x) \text{ et } (\forall y \in E,\ A(y) \ \Rightarrow\ x = y)\big)$$

Sa négation s'écrit donc :

$$\forall x \in E,\ \big(\text{non}(A(x)) \text{ ou } (\exists y \in E,\ A(y) \text{ et } x \neq y)\big)$$

Il est inutile d'apprendre ce résultat par coeur, il est (encore une fois) totalement intuitif : la négation de « il existe un unique $x \in E$ tel que $A(x)$ » est « soit il n'existe aucun $x \in E$ tel que $A(x)$, soit il en existe au moins deux (distincts) ».

III Retour aux ensembles : introduction des notations usuelles.

Le but de cette partie est d'introduire les notations usuelles d'ensembles (intervalles, intervalles d'entiers, ensembles produits, ensemble définis par compréhension etc.) et d'applications. Nous reverrons ces notions dans le chapitre 4, mais nous allons en parler dès à présent pour pouvoir utiliser ces notations sans nous poser de question en attendant (par exemple pour définir une somme double, cf. chapitre 3, ou pour définir une fonction croissante, cf. chapitre 2).

III.1 Existence admise des ensembles de nombres

Nous admettons l'existence et les principales propriétés des ensembles de nombres suivants :

- L'ensemble $\mathbb{N}$ des nombres entiers naturels.
- L'ensemble $\mathbb{Z}$ des nombres entiers relatifs.
- L'ensemble $\mathbb{Q}$ des nombres rationnels (voir ci-dessous).
- L'ensemble $\mathbb{R}$ des nombres réels.

Nous avons les inclusions strictes suivantes : $\mathbb{N} \subsetneq \mathbb{Z} \subsetneq \mathbb{Q} \subsetneq \mathbb{R}$.

On dit que l'ensemble E est strictement inclus dans l'ensemble F, si $E \subset F$ et $E \neq F$. On note alors $E \subsetneq F$, cf. chapitre 4.

Ces ensembles contiennent 0 et on note :

- L'ensemble $\mathbb{N}^*$ des nombres entiers naturels non nuls.
- L'ensemble $\mathbb{Z}^*$ des nombres entiers relatifs non nuls.
- L'ensemble $\mathbb{Q}^*$ des nombres rationnels (voir ci-dessous) non nuls.
- L'ensemble $\mathbb{R}^*$ des nombres réels non nuls.

Remarque : Quand nous parlerons de nombres entiers dans la suite (par exemple quand nous parlerons d'intervalles d'entiers), il sera sous-entendu (sauf indication contraire, ou si le contexte fait que nous manipulons forcément des entiers positifs) que nous parlerons d'entiers relatifs.

Rappelons la définition d'un nombre rationnel :

Définition. Soit $r \in \mathbb{R}$. On dit que r est rationnel s'il existe $p \in \mathbb{Z}$ et $q \in \mathbb{Z}^*$ tels que $r = \dfrac{p}{q}$. Si r n'est pas rationnel, on dit que r est irrationnel. L'ensemble des nombres irrationnels est noté $\mathbb{R}\backslash\mathbb{Q}$.

La notation $A\backslash B$ sera également revue dans le chapitre 4.

Remarque : On trouve également la définition suivante, totalement équivalente (cf. exercice 10) : r est rationnel s'il existe $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$ tels que $r = p/q$ (en d'autres termes, on peut choisir de faire porter le signe de la fraction par son numérateur), et on peut prendre p et q premiers entre eux, c'est-à-dire n'ayant aucun diviseur positif commun à part 1. De plus, si $r \geqslant 0$, alors soit p et q sont tous les deux négatifs, soit ils sont tous les deux positifs (par exemple, $1/2 = -1/-2$). Quitte à simplifier par -1, on suppose donc qu'ils sont tous les deux positifs. En d'autres termes, si $r \geqslant 0$, on dit qu'il est rationnel s'il existe $p \in \mathbb{N}$ et $q \in \mathbb{N}^*$ tels que $r = p/q$.

De plus, si $r \neq 0$, on peut également dire que p est non nul. Rappelons en effet qu'une fraction est non nulle si et seulement si son numérateur est non nul.

Remarque : En d'autres termes, un rationnel est un quotient de deux entiers (on peut même les supposer premiers entre eux, c'est-à-dire sans diviseur communs sauf 1, cf. chapitre 6), et un irrationnel est un nombre qui ne peut pas s'écrire comme quotient de deux entiers. Nous montrerons cette année que $\sqrt{2}, e$ et π sont irrationnels.

Rappelons enfin la définition d'un nombre pair.

Définition. Soit $n \in \mathbb{Z}$. On dit que n est pair si n est divisible par 2, c'est-à-dire s'il existe $k \in \mathbb{Z}$ tel que $n = 2k$. Il est dit impair sinon.

On dit qu'un entier p divise n s'il existe $k \in \mathbb{Z}$ tel que $n = k \times p$, nous reverrons cela dans le chapitre 6.

Remarque : Si n est positif alors k l'est également. En d'autres termes, un entier positif est pair s'il existe $k \in \mathbb{N}$ tel que $n = 2k$. De même pour impair ci-dessous.

Théorème (Admis provisoirement). Soit $n \in \mathbb{Z}$. Alors n est impair si et seulement s'il existe $k \in \mathbb{Z}$ tel que $n = 2k + 1$.

Ce résultat découle du théorème de division euclidienne que nous verrons dans le chapitre 6.

Conclusion : Entraînons-nous à manipuler ces notions et à les écrire avec des quantificateurs :

- $r \in \mathbb{Q} \iff \exists p \in \mathbb{Z}, \exists q \in \mathbb{Z}^*, r = p/q \iff \exists p \in \mathbb{Z}, \exists q \in \mathbb{N}^*, r = p/q$.
- Si r est un réel positif : $r \in \mathbb{Q} \iff \exists p \in \mathbb{N}, \exists q \in \mathbb{N}^*, r = p/q$.
- Si n est un entier, alors : n est pair $\iff \exists k \in \mathbb{Z}, n = 2k$.
- Si n est un entier, alors : n est impair $\iff \exists k \in \mathbb{Z}, n = 2k + 1$.

Comme dit ci-dessus, on remplace $\mathbb{Z}$ par $\mathbb{N}$ si on sait qu'on manipule des entiers positifs (par exemple dans des sommes allant de 0 à n, cf. chapitre 3).

Remarque : Nous verrons une version condensée de ces écritures quand nous aurons vu les ensembles produits dans le III.5.

III.2 Modes de définition d'un ensemble.

Il existe plusieurs façons de définir un ensemble. Les trois principales sont les suivantes :

1. Définir un ensemble grâce à des unions, intersections, passages au complémentaire (cf. chapitre 4) d'ensembles déjà existants. Par exemple, $E = [\,0\,;1\,] \cap \overline{\mathbb{Q}}$ est l'ensemble des irrationnels appartenant à $[\,0\,;1\,]$.
2. Définir un ensemble en donnant explicitement tous ses éléments entre accolades et séparés par des points virgules.

On dit alors que l'ensemble est défini par extension.

Exemples :

- $\{0; 1\}$ est l'ensemble à deux éléments contenant uniquement 0 et 1.
- $\{1; 2; 3; 4; 5; 6\}$ est l'ensemble à six éléments contenant les entiers de 1 à 6. On le note également $[\![\,1\,;6\,]\!]$ (cf. III.3).
- $\mathbb{N} = \{0; 1; 2; 3; \dots\}$.
- $\mathbb{Z} = \{\dots; -3; -2; -1; 0; 1; 2; 3; \dots\}$.
- $\{0\}$ est l'ensemble à un élément contenant uniquement 0. On l'appelle « singleton 0 ». Plus généralement :

Définition. Un ensemble à un élément est appelé un singleton. Si on note x cet élément, cet ensemble (noté donc $\{x\}$) est appelé « singleton x ».

Définition. On dit que deux ensembles E et F sont égaux, et on note $E = F$, si ils ont les mêmes éléments.

Remarque : Avec des quantificateurs : $\forall x,\ x \in E \iff x \in F$. On peut donc prouver que deux ensembles sont égaux en raisonnant par équivalences (mais, en général, on raisonnera par double inclusion : cf. chapitre 4).

⚠ Un élément appartient ou n'appartient pas à un ensemble, il n'y a pas de notion d'ordre ou de multiplicité (il appartient ou non à l'ensemble, il ne peut pas lui appartenir plusieurs fois). Par exemple, les trois ensembles $\{0; 1\}, \{0; 0; 1\}$ et $\{1; 0\}$ sont égaux : ils contiennent 0 et 1 et aucun autre élément, ils ont les mêmes éléments donc sont égaux.

Remarque : Inconvénients de ce mode de définition :

- Il nécessite de connaître tous les éléments de l'ensemble.
- Il est difficilement maniable avec un grand nombre d'éléments : on le voit rien qu'avec 6 éléments !

3. Définir un ensemble par une propriété caractérisant ses éléments. Plus précisément, si P est une propriété, on note $\{x \in E \,|\, P(x)\}$ l'ensemble des éléments de E qui vérifient la propriété P. Détaillons cette notation :

$$\underbrace{\{}_{\text{accolade}} \quad \underbrace{\cdots}_{\substack{\text{Nature des éléments}\\ \text{de l'ensemble}\\ \text{(réels, entiers etc.)}}} \quad \underbrace{|}_{\substack{\text{barre verticale}\\ \text{de séparation :}\\ \text{lire « tels que »}}} \quad \underbrace{\cdots}_{\substack{\text{Propriété(s) vérifiée(s)}\\ \text{par les éléments}\\ \text{de l'ensemble}}} \quad \underbrace{\}}_{\text{accolade}}$$

On dit alors que l'ensemble est défini par compréhension.

$\{x \in E \,|\, P(x)\}$ est l'ensemble des éléments x appartenant à E tels que $P(x)$ soit vraie. En d'autres termes, c'est l'ensemble des éléments de l'ensemble se situant à gauche de la barre verticale vérifiant la propriété à droite de cette barre. Ou enfin : si $x \in E$, alors x appartient à cet ensemble si et seulement si $P(x)$ est vraie. Avec le dernier exemple ci-contre : « soit $x \in \mathbb{R}$. Alors : $x \in S \iff x^5 - 3x - 1 = 0$ ». Une rapide étude de fonction couplée au théorème de la bijection prouve que cet ensemble comporte trois éléments car l'équation $x^5 - 3x - 1 = 0$ a trois solutions. Cependant, on ne les connaît pas, ce qui n'empêche pas de définir S !

Remarque : Nous nous intéressons seulement à la façon d'écrire un ensemble. Les notions mathématiques présentes ci-dessous (fonctions paires etc.) seront vues dans des chapitres ultérieurs.

Exemples :

- $P = \{f : \mathbb{R} \longrightarrow \mathbb{R} \,|\, \forall x \in \mathbb{R},\, f(-x) = f(x)\}$ est l'ensemble des fonctions f de $\mathbb{R}$ dans $\mathbb{R}$ telles que, pour tout $x \in \mathbb{R}$ $f(-x) = f(x)$. En d'autres termes, c'est l'ensemble des fonctions paires.
- $\{x \in \mathbb{R} \,|\, x^2 = 1\}$ est l'ensemble des réels dont le carré vaut 1. En d'autres termes, c'est l'ensemble à deux éléments $\{-1; 1\}$.
- $\pi\mathbb{Z} = \{x \in \mathbb{R} \,|\, \sin(x) = 0\}$ est l'ensemble des réels x tels que $\sin(x) = 0$. En d'autres termes, c'est l'ensemble des réels congrus à 0 modulo π.
- $\{f : \mathbb{R} \longrightarrow \mathbb{R} \,|\, f \text{ dérivable sur } \mathbb{R},\, f'(0) = f'(1) = 0\}$ est l'ensemble des fonctions f de $\mathbb{R}$ dans $\mathbb{R}$ dérivables et vérifiant $f'(0) = f'(1) = 0$.
- $S = \{x \in \mathbb{R} \,|\, x^5 - 3x - 1 = 0\}$ est l'ensemble des réels x solutions de l'équation $x^5 - 3x - 1 = 0$.

Remarque : Avantages de ce mode de définition :

- Il permet de définir et de manipuler facilement des ensembles infinis.
- Il n'est pas nécessaire de connaître explicitement tous les éléments de l'ensemble pour le définir. C'est particulièrement frappant avec les deux derniers exemples ci-dessus : on serait particulièrement en peine de donner toutes les fonctions f dérivables sur $\mathbb{R}$ vérifiant $f'(0) = f'(1) = 0$, et on ne sait pas résoudre l'équation $x^5 - 3x - 1 = 0$. On ne sait même pas, au premier abord, combien de solutions cette équation possède !

Remarque : L'ensemble des entiers naturels pairs (parfois noté $2\mathbb{N}$) peut être écrit de la façon suivante :

$$2\mathbb{N} = \{n \in \mathbb{N} \,|\, \exists k \in \mathbb{N},\, n = 2k\}$$

mais c'est tout de même une notation assez lourde. On utilisera plutôt la notation plus concise $2\mathbb{N} = \{2k \,|\, k \in \mathbb{N}\}$. Plus généralement, si $f : E \longrightarrow F$ est une application (nous reverrons donc cette notation dans le chapitre 4) et si A est une partie de E, on note $\{f(x) \,|\, x \in A\}$ ou $f(A)$ l'ensemble des images par f des éléments de A. On peut lire : « $\{f(x) \,|\, x \in A\}$ est l'ensemble formé des $f(x)$ quand x parcourt A ». Là aussi, détaillons cette notation :

$$\underbrace{\{}_{\text{accolade}} \quad \underbrace{f(x)}_{\substack{\text{Éléments de}\\ \text{l'ensemble : images}\\ \text{d'un paramètre}\\ x \text{ par } f}} \quad \underbrace{|}_{\substack{\text{barre verticale}\\ \text{de séparation}}} \quad \underbrace{x \in A}_{\substack{\text{Le paramètre}\\ \text{et l'ensemble}\\ \text{qu'il parcourt}}} \quad \underbrace{\}}_{\text{accolade}}$$

Là aussi, précisons une chose (encore une fois, nous reverrons cette notation dans le chapitre 4) : si $f : E \longrightarrow F$, $f(A) = \{f(x) \,|\, x \in A\}$ est l'ensemble des images par f des éléments de A. En d'autres termes, un élément de F appartient à cet ensemble ssi il s'écrit sous la forme $f(x)$ avec $x \in A$. Avec des quantificateurs, cela donne : « Soit $y \in F$. Alors : $y \in f(A) \iff \exists x \in A, y = f(x)$ ». Cette équivalence est à connaître sur le bout des doigts ! Par exemple, avec l'ensemble E ci-contre : « Soit $x \in \mathbb{R}$. Alors : $x \in E \iff \exists n \in \mathbb{N},\, x = u_n$ ». Attention x n'est pas forcément un entier !

Exemples :

- $C = \left\{n^2 \,|\, n \in \mathbb{N}\right\}$ est l'ensemble des carrés parfaits.
- Plus généralement, si $(u_n)_{n \in \mathbb{N}}$ est une suite (donc une application de $\mathbb{N}$ dans $\mathbb{R}$, cf. chapitre 4 et chapitre 12), $E = \{u_n \,|\, n \in \mathbb{N}\}$ est l'ensemble des termes de la suite.
- $\{\sin(x) \,|\, x \in \mathbb{R}\} = [\,-1\,;1\,]$.

III.3 Intervalles et intervalles d'entiers.

Définition (intervalles). Pour tous réels a et b tels que $a \leqslant b$, nous notons

$[\,a\,;b\,] = \{x \in \mathbb{R} \mid a \leqslant x \leqslant b\}$ (intervalle fermé borné ou **segment**),

$]\,a\,;b\,] = \{x \in \mathbb{R} \mid a < x \leqslant b\}$ si $a < b$ (intervalle semi-ouvert borné),

$[\,a\,;b\,[= \{x \in \mathbb{R} \mid a \leqslant x < b\}$ si $a < b$ (intervalle semi-ouvert borné),

$]\,a\,;b\,[= \{x \in \mathbb{R} \mid a < x < b\}$ si $a < b$ (intervalle ouvert borné),

$]\,-\infty\,;a\,] = \{x \in \mathbb{R} \mid x \leqslant a\}$ (intervalle fermé non borné),

$]\,-\infty\,;a\,[= \{x \in \mathbb{R} \mid x < a\}$ (intervalle ouvert non borné),

$[\,a\,;+\infty\,[= \{x \in \mathbb{R} \mid x \geqslant a\}$ (intervalle fermé non borné),

$]\,a\,;+\infty\,[= \{x \in \mathbb{R} \mid x > a\}$ (intervalle ouvert non borné),

$]\,-\infty\,;+\infty\,[= \mathbb{R}$ (intervalle ouvert et fermé non borné).

Les réels a et b sont appelés les extrémités de l'intervalle.

Tout ensemble de cette forme est donc appelé un intervalle.

Remarques :

- Nous verrons dans le chapitre 12 une caractérisation des intervalles : ce sont les parties de $\mathbb{R}$ qui n'ont pas de « trous ».
- Pour tout réel a, l'intervalle $[\,a\,;a\,]$ est le singleton $\{a\}$. Les intervalles $]\,a\,;a\,]$, $[\,a\,;a\,[$ et $]\,a\,;a\,[$ sont vides.
- Par conséquent, l'ensemble vide est aussi appelé un intervalle. Cependant, quand on travaillera avec des intervalles, on prendra presque toujours le soin de préciser qu'ils sont non vides (et aussi non réduits à un point).
- Parfois, on note $[\,a\,;b\,]$ (respectivement $]\,a\,;b\,[$) l'ensemble des réels compris au sens large (respectivement au sens strict) entre a et b. Cet abus de notation peut être très utile : il permet d'éviter de distinguer plusieurs cas, selon que $a < b$ ou le contraire, par exemple pour appliquer le TVI (voir l'exemple de raisonnement par l'absurde dans le chapitre 1). Mais attention, si $a > b$, certains ouvrages prennent la convention que ces intervalles sont vides.

Définition. On note

- $\mathbb{R}_+ = [\,0\,;+\infty\,[$ l'ensemble des réels positifs.
- $\mathbb{R}_+^* =]\,0\,;+\infty\,[$ l'ensemble des réels strictement positifs.
- $\mathbb{R}_- =]\,-\infty\,;0\,]$ l'ensemble des réels négatifs.
- $\mathbb{R}_-^* =]\,-\infty\,;0\,[$ l'ensemble des réels strictement négatifs.

On trouve également les notations évidentes $\mathbb{Q}_+$ et $\mathbb{Q}_+^*$. On n'utilise pas les notations $\mathbb{Z}_+$ ou $\mathbb{Z}_+^*$ car $\mathbb{Z}_+ = \mathbb{N}$ et $\mathbb{Z}_+^* = \mathbb{N}^*$!

Définition. Si p et n sont deux entiers tels que $p \leqslant n$, alors on note $[\![p\,;n]\!] = \{p; p+1; \dots; n-1; n\}$ l'ensemble des entiers compris (au sens large) entre p et n.

Ne pas confondre les notations $[\,p\,;n\,]$ et $[\![p\,;n]\!]$. Ce dernier n'est PAS un intervalle.

Remarque : Il n'y a pas de notion « d'intervalle d'entiers ouvert ». En effet, l'ensemble des entiers strictement compris entre n et p est l'ensemble $[\![p+1\,;n-1]\!]$. C'est un résultat qui reviendra souvent, par exemple quand on manipulera la partie entière (cf. chapitre 2) : si k et si p sont deux entiers, alors $k > p$ si et seulement si $k \geqslant p+1$ (et idem dans l'autre sens : $k < p$ si et seulement si $k \leqslant p-1$).

Par exemple, un entier est supérieur strictement à 3 si et seulement s'il est supérieur ou égal à 4. C'est bien sûr faux si on ne manipule pas des entiers.

III.4 Petite pause applications.

Nous avons utilisé plus haut la notation $f : E \to F$. Nous reverrons les applications en détail dans le chapitre 4, mais donnons dès à présent la notation usuelle des fonctions :

Définition. Une fonction f de E dans F est notée de la façon suivante :

$$f : \left\{ \begin{array}{ccc} E & \longrightarrow & F \\ x & \longmapsto & f(x) \end{array} \right.$$

Cette notation signifie : f est la fonction qui va de E dans F et qui à x associe $f(x)$. On écrit aussi souvent « soit $f : E \longrightarrow F$ » pour signifier : « soit f une fonction de E dans F ».

Attention, dans l'écriture ci-contre, la variable x est muette. La fonction f ne dépend pas de x donc on peut très bien écrire

$$f : t \longmapsto f(t)$$

sans modifier en rien la fonction f. En particulier, la fonction f ne dépend pas de x, écrire (par exemple) « la fonction f est croissante pour tout x » n'a aucun sens ! Une fonction est un objet qui, à un élément de E, lui associe une image. Et c'est tout ! Et c'est déjà pas mal...

Remarques :

- On peut parfois ne pas expliciter E et F quand il n'y a aucune ambiguité. Par exemple, quand on parlera de la fonction $x \longmapsto x + \cos(x)$, il sera sous-entendu (sauf indication contraire) qu'elle va de $\mathbb{R}$ dans $\mathbb{R}$. De même, quand on parlera de la fonction $x \longmapsto \dfrac{x+1}{x-1}$, il sera sous-entendu (encore une fois sauf indication contraire) qu'elle va de $\mathbb{R}\backslash\{1\}$ (son domaine de définition) dans $\mathbb{R}$.
- Quand on écrit que f va de E dans F, cela signifie que f prend ses valeurs dans F, cela ne signifie pas du tout que tous les éléments de F sont atteints. Par exemple, on peut dire que l'exponentielle et même la fonction nulle vont de $\mathbb{R}$ dans $\mathbb{R}$! Il ne faut donc pas confondre F, l'ensemble d'arrivée, avec $f(E)$, l'ensemble image (cf. chapitre 4).
- Ne pas confondre la fonction f avec l'image $f(x)$! Ces deux objets n'ont pas la même nature et donc ne sauraient être confondus : f est une fonction et $f(x)$ est un élément de F, cela n'a rien à voir ! On ne parlera donc jamais de la fonction $f(x)$, tout simplement car ce n'est pas une fonction !
- Par exemple, on parlera de la fonction carré (sans « e » !) et pas de la fonction x^2 ! Si on a affaire à une fonction qui n'a pas de nom, on utilisera la notation avec la flèche vue ci-dessus. Par exemple, on parlera de la fonction $x \mapsto \dfrac{x+1}{x-1}$ (définie sur $\mathbb{R}\backslash\{1\}$). Cependant, cela peut vite se révéler assez lourd (surtout si on doit l'écrire plusieurs fois). On définira donc une fois pour toutes une fonction $f : x \mapsto \dfrac{x+1}{x-1}$ et on parlera ensuite de la fonction f, ce qui est tout de même plus maniable.

C'est le premier des nombreux échecs de type auxquels il faudra faire attention. Par exemple, on ne confondra pas la suite $(u_n)_{n\in\mathbb{N}}$ (c'est une suite) avec u_n, le terme d'indice n (c'est un réel). Les échecs de type sont déjà graves pour les mathématiciens, mais ils sont impardonnables pour les informaticiens : la plupart des langages refusent de traiter une commande si on l'appelle avec un objet qui n'est pas du bon type !

III.5 Produit cartésien d'un nombre fini d'ensembles.

Nous ne ferons qu'effleurer la définition dans ce paragraphe (en particulier, nous ne donnerons pas la définition de couple, de n-uplet ou de famille), nous reverrons cela plus en détails dans le chapitre 4. On se donne dans ce paragraphe deux ensembles non vides E et F.

Définition. On appelle produit cartésien de E et F, et on note $E \times F$, l'ensemble des couples (e, f) d'éléments de E et F. En d'autres termes :

$$E \times F = \{(e, f) \,|\, e \in E \text{ et } f \in F\}.$$

Si $E = F$, on le note E^2 au lieu de $E \times E$.

Remarque : Contrairement aux ensembles, ici, l'ordre compte ! Le couple (a, b) n'est pas égal au couple (b, a) quand $a \neq b$. Pour bien visualiser ceci, il suffit de voir que, dans le plan, le point de coordonnées $(1, 2)$ et le point de coordonnées $(2, 1)$ ne sont pas représentés par le même point. Nous reverrons dans le chapitre 4 que l'on peut souvent visualiser les ensembles produits avec un dessin.

Exemples :

- Si $E = \{1; 2\}$ et $F = \{1; 2; 3\}$, alors :
  - ⋆ $E \times F = \big\{(1, 1); (1, 2); (1, 3); (2, 1); (2, 2); (2, 3)\big\}$.
  - ⋆ $F \times E = \big\{(1, 1); (1, 2); (2, 1); (2, 2); (3, 1); (3, 2)\big\}$.

- Le produit cartésien $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ est l'ensemble des couples de réels. On l'identifie parfois au plan (en identifiant un point à ses cordonnées dans un repère orthonormé).
- $[\![1\,;\,6]\!]^2$ est l'univers que l'on associera à l'expérience aléatoire consistant à lancer deux dés à 6 faces (consécutivement ou en même temps). On voit une fois de plus dans cet exemple que, contrairement aux ensembles, l'ordre compte : si le premier dé donne 1 et le second donne 2, ce n'est pas la même chose que si le premier dé donne 2 et le second donne 1. De plus, on peut avoir deux fois le même élément : dans cet exemple, le couple $(2, 2)$ représente le fait que les deux dés ont donné le chiffre 2.

Plus généralement :

Définition. Soit n un entier naturel supérieur à 2, et soient $E_1, \dots, E_n$ n ensembles non vides. On appelle produit cartésien de $E_1, \dots, E_n$, et on note $E_1 \times \cdots \times E_n$, l'ensemble des n-uplets d'éléments de $E_1, \dots, E_n$. En d'autres termes :

$$E_1 \times \cdots \times E_n = \{(x_1, \dots, x_n) \,|\, x_1 \in E_1 \text{ et } \cdots \text{ et } x_n \in E_n\}.$$

Si $E_1 = E_2 = \cdots = E_n = E$, on le note E^n au lieu de $E_1 \times \cdots \times E_n$.

Ne pas confondre $(x_1, \dots, x_n)$ avec l'ensemble $\{x_1; \dots; x_n\}$. Par exemple le triplet $(x_1, x_2, x_3) = (2, 1, 2)$ n'est pas l'ensemble $\{x_1; x_2; x_3\} = \{1; 2\}$.

Exemple : Si $n \in \mathbb{N}^*$, on note donc $\mathbb{R}^n$ l'ensemble des n-uplets de réels. En particulier, $\mathbb{R}^3$ est l'ensemble des triplets de réels, qu'on identifiera parfois à l'espace, de la même façon qu'on a identifié $\mathbb{R}^2$ au plan.

Remarque : La notion de produit cartésien permet aussi un raccourci de notations. Par exemple on pourra écrire « $\forall (x, y, z) \in E^2 \times F$ » au lieu de « $\forall x \in E, \forall y \in E, \forall z \in F$ » . Idem avec les « $\exists$ ».

Exemple : Cela permet de réécrire les deux caractérisations possibles des rationnels de la façon suivante :

- $r \in \mathbb{Q} \iff \exists (p, q) \in \mathbb{Z} \times \mathbb{Z}^*, r = p/q \iff \exists (p, q) \in \mathbb{Z} \times \mathbb{N}^*, r = p/q.$
- Si r est un réel positif : $r \in \mathbb{Q} \iff \exists (p, q) \in \mathbb{N} \times \mathbb{N}^*, r = p/q.$

Remarque : Les éléments de $E \times F$ sont des couples, les éléments de $E_1 \times \cdots \times E_n$ sont des n-uplets. Recommençons : un élément de $E \times F$ est **un** couple, et un élément de $E_1 \times \cdots \times E_n$ est **un** n-uplet (même si ces éléments ont plusieurs coordonnées). Ainsi, on écrira (par exemple) « soit $(x, y) \in \mathbb{R}^2$ » (au singulier : on prend **un** couple de réels) ou « soient $x, y \in \mathbb{R}$ » ou « soient x, y appartenant à $\mathbb{R}$ » ou « soient x et y deux réels » (au pluriel : on prend deux réels).

Idem, soyons précis au sujet du type de l'objet que l'on manipule.

IV Premiers modes de démonstrations et premières consignes de rédaction.

IV.1 Composition d'un texte mathématique.

Définition.

- Un axiome est une assertion que l'on suppose vrai a priori (et que l'on ne cherche pas à démontrer).
- Un théorème est une assertion vraie qui désigne en général une assertion particulièrement importante.
- Une proposition est une assertion vraie, souvent de moindre envergure.
- Un lemme est une assertion vraie qui est un résultat préliminaire utile à la démonstration d'une assertion plus importante.
- Un corollaire est une assertion vraie qui est la conséquence (souvent immédiate) d'une autre assertion vraie.
- Une conjecture est une assertion dont on pense qu'elle est vraie, sans en avoir de preuve.

À part les axiomes, la véracité (ou la fausseté) d'une assertion doit résulter d'une démonstration (ou preuve) : elle s'appuie sur des hypothèses, sur des axiomes, sur des assertions démontrées précédemment et sur les règles de logique que nous vues dans ce chapitre.

Exemples :

- L'assertion « Par un point extérieur à une droite, il passe une et une seule droite parallèle à cette droite » est un axiome appelé *cinquième axiome d'Euclide*.
- Le théorème de Pythagore est l'assertion : « Dans un triangle rectangle, le carré de la longueur de l'hypoténuse est égal à la somme des carrés des longueurs des côtés adjacents à l'angle droit ». Il en existe de nombreuses démonstrations.
- La conjecture de Goldbach est l'assertion non démontrée qui s'énonce comme suit : « Tout nombre entier pair strictement supérieur à 3 peut s'écrire comme la somme de deux nombres premiers » (par exemple, $20 = 7 + 13$ et $2000 = 3 + 1997$).

En 2014, cette conjecture a été vérifiée pour tous les entiers jusqu'à 4×10^{18}... de quoi penser qu'elle doit être vraie, mais il n'y a pas de preuve à ce jour.

Remarque : Il est assez lourd de préciser à chaque fois « une assertion vraie ». Par conséquent, par convention, quand on écrit un texte mathématique, une assertion est implicitement supposée vraie, sauf mention contraire (par exemple quand on dit que c'est une conjecture, ou quand on dit explicitement qu'elle est fausse).

IV.2 Comment construire une démonstration :

Ce paragraphe sera considérablement étoffé dans le chapitre 1.

- **Si on veut prouver une conjonction** A et B **:** on prouve A puis on prouve B.
- **Si on veut prouver une disjonction** A ou B **:** on suppose que A est fausse et on prouve B. On peut bien sûr intervertir A et B, c'est-à-dire supposer B fausse et prouver A.

  Exemple : Dans l'exercice 29 du chapitre 19, il est demandé de prouver que, si z est une racine complexe du polynôme $P = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$, alors $|z| \leqslant \max\left(1, \sum_{k=0}^{n-1} |a_k|\right)$. Il faut donc prouver que $|z| \leqslant 1$ ou que $|z| \leqslant \sum_{k=0}^{n-1} |a_k|$. On suppose donc $|z| > 1$ et on prouve que $|z| \leqslant \sum_{k=0}^{n-1} |a_k|$.

Toutes les notions mathématiques présentes ci-contre (complexes, sommes, polynômes, maximum etc.) seront vues dans des chapitres ultérieurs. On se concentre pour l'instant uniquement sur le mode de raisonnement.

- **Si on veut prouver une implication** $A \Rightarrow B$ **:** on suppose A et on prouve B. On commence donc par écrire : « Supposons A vraie ». On pourra également raisonner par contraposée (cf. chapitre 1).
- **Si on veut prouver une équivalence** $A \iff B$ **:** on peut raisonner par double implication, c'est-à-dire qu'on peut prouver successivement que $A \Rightarrow B$ et $B \Rightarrow A$ sont vraies, et donc on se ramène au point ci-dessus. Il faut bien faire attention à écrire explicitement les hypothèses faites et à faire apparaître les deux étapes du raisonnement. On peut aussi travailler par équivalences successives, mais il faut être prudent, ce n'est pas toujours possible (et même quand c'est possible, un raisonnement par double implication est aussi possible). Nous en reparlerons dans le chapitre 1.
- **Si on veut prouver plusieurs équivalences, du type** $A \iff B \iff C$ **:** on prouve en général que $A \Rightarrow B, B \Rightarrow C$ et $C \Rightarrow A$ sont vraies. En effet, si ces implications sont vraies, alors on a $A \Rightarrow B$, et $B \Rightarrow C$ et $C \Rightarrow A$ donc $B \Rightarrow A$: A et B sont bien équivalentes, cf II.5.c. On montre de même que B et C sont alors équivalentes. On généralise aisément à un plus grand nombre d'équivalences (et en général l'énoncé les met dans l'ordre dans lequel la démonstration est la plus simple).

Remarque : Avant de nous intéresser aux assertions quantifiées, donnons tout de suite une consigne de rédaction très importante : les quantificateurs ne sont pas des abréviations ! On ne mélange donc pas quantificateurs et phrases en français ! Nous n'écrirons donc jamais d'horreur du type « Montrons que $\forall n \in \mathbb{N}$, H_n est vraie ». À la limite, on peut inclure une phrase entièrement écrite en langage quantifié au coeur d'une phrase en français en la séparant du reste de la phrase avec « : ». Voir des exemples ci-dessus (caractérisation des rationnels, des entiers pairs, définition d'un ensemble par compréhension etc.).

Remarque : Tant que nous parlons quantificateurs, précisons que les seuls que nous ayons sont $\forall$ et $\exists$ et qu'on peut les lire à voix haute en disant « pour tout » (ou quel que soit) et « il existe ». Ainsi, en lisant à haute voix, ce qui suit a un sens :

$$z^n = 1 \iff \exists k \in [\![0\,;\, n-1]\!], z = e^{2ik\pi/n}.$$

Le sens mathématique sera vu dans le chapitre 7.

On n'écrira donc pas :

$$z^n = 1 \iff z = e^{2ik\pi/n}, k \in [\![0\,;\, n-1]\!]$$

ce qui n'a aucun sens, ni mathématiquement, ni même en français quand on lit cela à voix haute.

Faisons d'ailleurs un test : qui reformule ce qui précède avec « $\exists$ » et « $\forall$ » ?

Ceci étant dit, reprenons.

- **Si on veut prouver une assertion du type** $\forall x \in E, A(x)$ **:** on se donne un élément x de E quelconque. On commence donc par : « Soit $x \in E$. » Attention à ne pas commencer par : « $\forall x \in E, \dots$ » D'une part, on court le risque d'utiliser les quantificateurs comme des abréviations, ce qui est exclu, et d'autre part, x est alors une variable muette, liée, qui « ne vit » que dans la phrase qui suit, tandis qu'en écrivant « Soit $x \in E$ », on se donne un élément de E qu'on peut utiliser dans toute la suite du raisonnement, cf II.6.

Encore une fois, on verra d'autres types de raisonnements dans le chapitre 1. Par exemple, on pourra raisonner par l'absurde ou, si $E = \mathbb{N}$, par récurrence.

Remarque : Tant qu'on parle de « Soit », donnons une nouvelle consigne de rédaction, très importante. Il ne faut jamais manipuler un objet sans avoir montré son existence (sauf, par exemple, dans le cadre d'un raisonnement par analyse-synthèse, cf. chapitre 1), typiquement :

- une dérivée (il faut donc justifier la dérivabilité de la fonction avant de la dériver, cf. chapitre 2).
- une limite (cf. chapitre 2).
- une somme infinie (on verra cela au chapitre 25).

Cela donne des failles logiques dans les raisonnements. Donnons un exemple particulièrement spectaculaire de ce qui peut arriver quand on manipule des objets dont on n'a pas montré l'existence. Montrons que le plus grand entier naturel est 1. Soit n le plus grand entier naturel. Alors on a évidemment $n \neq 0$. De plus, n étant le plus grand entier naturel, on a $n \geqslant n^2$. Or, $n \geqslant 1$ donc $n^2 \geqslant n$ si bien que $n^2 = n$, donc $n = 1$ puisque $n \neq 0$.

La faille vient du fait qu'on a commencé par : « Soit n le plus grand entier naturel ». Or, un tel n n'existe pas ! À part cela, tout le reste du raisonnement est correct. C'est un autre exemple du fait, cf. II.3, qu'en partant d'une assertion fausse, on peut prouver tout et n'importe quoi !

Remarque : Énonçons ici un principe général (qu'on peut appeler principe de substitution, mais nous nous en servirons constamment sans utiliser ce nom) : si un résultat est vrai **pour tout** $x \in E$, alors on peut l'utiliser en remplaçant x (qui est une variable muette la plupart du temps, et même si x est fixé, s'il est quelconque, alors ce qui est vrai pour lui est vrai pour tout autre élément de E) par n'importe quel élément de E (c'est-à-dire par n'importe quel élément vérifiant les mêmes conditions que x). Par exemple, un résultat vrai pour tout réel x est aussi vrai pour $x/2$ ou pour $x+1$! Cela peut paraître absurde (et ça l'est si on écrit les âneries ci-contre), mais il faut bien comprendre (encore !) que si on prouve un résultat du type « $\forall x \in \mathbb{R}, A(x)$ », la variable x est muette ! Il faut bien comprendre qu'en fait, on dit que le résultat A est vrai pour tout élément de $\mathbb{R}$, et qu'on note en général, par habitude, x un élément quelconque, mais on peut l'écrire autrement. On peut (et on le fera souvent cette année) réécrire ce résultat : « $\forall$ truc $\in \mathbb{R}, A(\text{truc})$ », et là, bizarrement, on a moins de scrupule à remplacer truc par $x/2$ ou $x+1\dots$ Quelques exemples valent mieux qu'un long discours.

Attention, si un résultat est vrai pour tout x et qu'on veut l'appliquer à $x+1$, il ne faut pas dire : « posons $x = x+1$ » ou autre joyeuseté du même genre (sinon on n'est pas loin de prouver que $0 = 1$) ! Voir une rédaction correcte ci-contre.

Exemples :

- Soit $f : \mathbb{R} \to \mathbb{R}$ vérifiant : $\forall x \in \mathbb{R}, f(2x) = f(x)$. L'égalité $f(2x) = f(x)$ pour tout x est à comprendre au sens suivant : un réel quelconque et son double ont la même image. Si x est un réel quelconque, on peut donc appliquer ce résultat à $x/2$, ce qui donne $f(x) = f(x/2)$. De même, si $x \in \mathbb{R}$, $f(x/2) = f(x/4)$. Si on fixe $x \in \mathbb{R}$, on peut montrer par une récurrence immédiate que, pour tout $n \in \mathbb{N}$, $f(x) = f(x/2^n)$: cf. exercice 17 du chapitre 13.

Si on a du mal à remplacer x par $x/2$, on réécrit l'hypothèse de la façon suivante : $\forall$truc $\in \mathbb{R}, f(\text{truc}) = f(2 \times \text{truc})$. On a moins de scrupule à remplacer truc par $x/2$...

- Nous verrons dans le chapitre 5 la formule : $\forall a \in \mathbb{R}, \cos(2a) = 1 - 2\sin^2(a)$. Si $a \in \mathbb{R}$, en appliquant cette formule à $a/2$, il vient : $\cos(a) = 1 - 2\sin^2\left(\dfrac{a}{2}\right)$.
- Nous verrons aussi dans le chapitre 5 que, pour tout $a \in \mathbb{R}, \sin(2a) = 2\sin(a)\cos(a)$. En particulier, pour tout $x \not\equiv 0[\pi]$ et tout $k \geqslant 1$, ce résultat est vrai en remplaçant a par $x/2^k$, si bien que

$$\cos\left(\frac{x}{2^k}\right) = \frac{\sin\left(\dfrac{x}{2^{k-1}}\right)}{2\sin\left(\dfrac{x}{2^k}\right)}$$

  cf. exercice 15 du chapitre 5.
- etc.

Morale de l'histoire : si on a un doute, remplacer « x » (ou « a » ou...) par « truc » (au brouillon, pas dans votre copie...). Mais attention, cela ne marche que si on a prouvé le résultat **pour tout x** ! Si on a simplement prouvé qu'il existait un x pour lequel le résultat est vrai, on ne peut pas utiliser le résultat obtenu pour une autre valeur de x !

Dans le même ordre d'idée, si on a plusieurs objets et que les hypothèses sur ces objets sont les mêmes (on dit qu'ils jouent le même rôle), alors ce qui est vrai pour l'un est vrai pour l'autre. On peut également les intervertir si on a prouvé un résultat mêlant ces deux objets : on dit qu'on raisonne alors « par symétrie des rôles ». Cela évite de faire deux fois le même raisonnement !

Exemple : Soient B_1 et B_2 deux bases d'un espace vectoriel de dimension finie E. Puisque B_1 est une base, c'est une famille génératrice, et puisque B_2 est une base, alors c'est une famille libre. Par conséquent, $\text{card}(B_1) \geqslant \text{card}(B_2)$. Par symétrie des rôles (B_1 et B_2 jouent le même rôle), $\text{card}(B_2) \geqslant \text{card}(B_1)$ donc $\text{card}(B_2) = \text{card}(B_1)$: toutes les bases de E ont le même cardinal.

Il est bien évident que les notions mathématiques sous-jacentes seront vues plus tard (au chapitre 30 pour être plus précis). L'exemple ci-contre est donné uniquement pour comprendre la notion de raisonnement par symétrie des rôles donnée juste au-dessus.

Ceci étant dit, reprenons.

- **Si on veut prouver une assertion du type $\exists x \in E, A(x)$:** C'est ce qui est le plus délicat en général. Un moyen simple est d'exhiber un élément x qui convient (mais donc il faut le deviner ou le construire, ce qui n'est parfois pas facile). Un gros travail au brouillon est parfois nécessaire. Là aussi, on verra plus tard (dans le chapitre 1 et dans d'autres chapitres ultérieurs) d'autres façons de faire (raisonnement par l'absurde ou, si on est sur un intervalle I avec une fonction continue, on pourra appliquer le TVI etc.).
- **Si on veut prouver une assertion du type $\exists! x \in E, A(x)$:** On peut prouver l'existence, et donc on se ramène au point précédent, puis on prouve l'unicité (en général en prenant deux éléments qui conviennent et en montrant qu'ils sont égaux). On peut également raisonner par analyse-synthèse ou, par exemple, si on est sur un intervalle I avec une fonction continue strictement monotone, appliquer le théorème de la bijection. Nous reverrons tout cela dans la suite, avec de nombreux exemples.

Remarque : Nous avons déjà dit que $\Rightarrow$ ne signifie pas « donc » et que $\iff$ ne signifie pas « c'est-à-dire ». Cette année, nous n'utiliserons des équivalences (presque) que pour des résolutions d'(in)équations ou des raisonnements par équivalences. Nous verrons des exemples de raisonnements par équivalences dans le chapitre 1, voyons à présent un exemple de résolution d'équation.

Exemple : Résoudre l'équation (d'inconnue $x \in \mathbb{R}$) : $(x-1)^2 - 7 = 0$.

Réponse : Soit $x \in \mathbb{R}$.

$$\begin{aligned} & (x-1)^2 - 7 = 0 \\ \iff \quad & (x-1)^2 = 7 \\ \iff \quad & (x-1) = \pm\sqrt{7} \\ \iff \quad & x = 1 \pm \sqrt{7} \end{aligned}$$

Nouvelle consigne de rédaction : toujours déclarer un objet avant de l'utiliser. Par exemple :

- Soit $x \in \mathbb{R}$.
- Soit $n \in \mathbb{N}$.
- Soit f continue sur $\mathbb{R}$.
- etc.

C'est comme dans un roman : si vous lisez « Il arriva », vous allez vous demander : qui est « Il » ?

Les équivalences sont ici indispensables :

- Les implications $\Rightarrow$ prouvent que, si x est solution, alors $x = 1 \pm \sqrt{7}$, c'est-à-dire qu'elles prouvent qu'aucun autre réel n'est solution, mais elles ne prouvent pas que ces deux réels sont effectivement solutions. En d'autres termes, elles prouvent que le fait que $x = 1 \pm \sqrt{7}$ est une condition **nécessaire** pour que x soit solution.
- Les implications $\Leftarrow$ prouvent que, si $x = 1 \pm \sqrt{7}$, alors x est solution, mais ne prouvent pas qu'il n'y en a pas d'autre. En d'autres termes, elles prouvent que le fait que $x = 1 \pm \sqrt{7}$ est une condition **suffisante** pour que x soit solution.

Remarque : Il ne faut pas utiliser des équivalences dans une suite de calculs ! Cela n'aurait aucun sens car une équivalences relie des assertions, pas des calculs ! Soit on ne met rien, soit on écrit donc, ainsi, dès lors, il en découle, par conséquent, en d'autres termes etc.

Exemple : Soit $(a, b) \in \mathbb{R}^2$. Soit f définie sur $\mathbb{R}_+^*$ par $f(x) = \dfrac{a + b\ln(x)}{x}$. Justifier rapidement que f est dérivable et prouver que, pour tout $x > 0$,

$$f'(x) = \frac{(b-a) - b\ln(x)}{x^2}$$

Réponse : f est dérivable car quotient de fonctions qui le sont, celle au dénominateur ne s'annulant pas. Soit $x > 0$.

Rappelons que pour prouver qu'un résultat est vrai pour tout $x > 0$, on commence par « Soit $x > 0$ ».

$$\begin{aligned} f'(x) &= \frac{b}{x} \times \frac{1}{x} + (a + b\ln(x)) \times \frac{-1}{x^2} \\ &= \frac{(b-a) - b\ln(x)}{x^2} \end{aligned}$$

Pas d'équivalences ici !

Remarque : Une dernière pour la route : on rappelle que les quantificateurs et les variables qu'ils introduisent ont une portée purement locale ! Par conséquent, quand on écrira des équivalences, si on a besoin de quantificateurs, il faut les écrire à chaque ligne (tant qu'on en a besoin), ils ne « survivent pas d'une équivalence à une autre » ! À titre d'exemple, nous résolvons ci-dessous l'équation (d'inconnue $z \in \mathbb{C}$) $(z+1)^n = 1$.

Cette équation et sa résolution ne sont données qu'à titre d'exemple, le contenu mathématique sera (re)vu dans le chapitre 7.

Réponse : Soit $z \in \mathbb{C}$. Soit $n \geqslant 1$.

$$\begin{aligned} & (z+1)^n = 1 \\ \iff\ & z + 1 \text{ est une racine } n\text{-ième de l'unité} \\ \iff\ & \exists k \in [\![0\,;\, n-1]\!], z + 1 = e^{2ik\pi/n} \\ \iff\ & \exists k \in [\![0\,;\, n-1]\!], z = e^{2ik\pi/n} - 1 \\ \iff\ & \exists k \in [\![0\,;\, n-1]\!], z = e^{ik\pi/n} \times \left(e^{ik\pi/n} - e^{-ik\pi/n}\right) \\ \iff\ & \exists k \in [\![0\,;\, n-1]\!], z = e^{ik\pi/n} \times 2\cos\left(\frac{k\pi}{n}\right) \end{aligned}$$