Dauphine | PSL
UNIVERSITÉ PARIS

Département MIDO, première année

Pré-rentrée : raisonnement

Alexandre Afgoustidis

(version du 9 septembre 2020)

Alexandre Afgoustidis
CEREMADE, Université Paris-Dauphine, 75016 Paris, France.
E-mail : `afgoustidis@ceremade.dauphine.fr`

Ce polycopié a été créé avec LaTeX; pour la mise en forme, nous avons adapté des fichiers de style fournis par la Société Mathématique de France, notamment la classe `smfbook`.

PRÉ-RENTRÉE : RAISONNEMENT

Alexandre Afgoustidis

TABLE DES MATIÈRES

AVANT DE COMMENCER

À propos de ce document. — Le texte qui suit a été rédigé durant l'été 2019 pour accompagner le cours « raisonnement » de la pré-rentrée. Il n'a pas vocation à se substituer au cours dispensé dans votre groupe : il comporte des passages qui ne seront pas traités en classe, et à l'inverse certains éléments ou exemples développés en classe ne figureront pas dans le polycopié.

Pour le rédiger, je me suis appuyé sur une partie des ouvrages mentionnés dans la bibliographie, ainsi que sur le document écrit par Pierre Cardaliaguet et Denis Pasquignon les années précédentes.

Ce document doit beaucoup aux discussions que j'ai eues à son sujet avec Emeric Bouin, Guillaume Carlier, Benjamin Mélinand, Moulka Tamzali-Lafond, et beaucoup d'autres. Il comporte très certainement des fautes de frappe et des erreurs : si vous en trouvez, je vous serais très reconnaissant de me les signaler.

Un conseil pour votre travail. — Pour bien s'approprier le cours,

- D'une part, il est essentiel d'avoir compris les définitions et les résultats (propositions, théorèmes) du cours, de les *connaître* avec précision, et d'avoir *étudié les exemples du cours* sans lesquels les notions paraîtront inévitablement très abstraites,
- D'autre part, il est utile de faire *soi-même* des exercices variés, pour tester sa compréhension du cours et pour s'entraîner à développer sa réflexion autour (et à l'aide) des notions nouvellement étudiées.

Deux écueils sont à éviter. D'une part, il n'est pas nécessairement souhaitable de faire *énormément* d'exercices au détriment de l'étude approfondie du cours. Souvenez-vous que le cours n'est *pas* un prétexte pour faire des exercices et passer des examens : au contraire, ce sont les exercices qui sont faits pour tester et améliorer votre compréhension du cours. D'autre part, il est probablement nuisible de se contenter de lire les corrections d'exercices que l'on n'a pas cherché soi-même : l'impression, en lisant et en comprenant le corrigé, qu'on « aurait su faire l'exercice » est en général mauvaise conseillère.

Sur les exercices de ce polycopié. — Les listes présentes à la fin de chaque chapitre contiennent plus d'exercices que ce qui pourra être traité en classe. Les étoiles attribuées à chaque exercice sont à interpréter comme suit :

★☆☆ : exercices proches du cours, c'est-à-dire pouvant être résolus par une application rapide des résultats du cours, ou par un raisonnement directement inspiré d'un exemple développé dans le cours.

★★☆ : exercices nécessitant plus qu'une application directe des résultats du cours : ces exercices peuvent demander un peu de recul, une certaine persévérance ou de l'aisance technique.

★★★ : exercices plus difficile, à n'aborder qu'une fois que vous êtes à l'aise avec les autres.

Il peut arriver qu'un exercice marqué ★☆☆ vous donne plus de mal, ou vous prenne beaucoup plus de temps, qu'un exercice marqué ★★☆ . Pas de panique : ce n'est pas parce qu'un exercice est *proche du cours* qu'il est forcément *très facile*. Par ailleurs, certains exercices vous prendront beaucoup de temps, y compris dans certains cas où l'énoncé est très court. Là encore, il n'y a pas nécessairement lieu de s'inquiéter : le temps passé à réfléchir à un exercice, *même si vous n'avez pas abouti*, n'est en général pas perdu.

CHAPITRE 1

ÉNONCÉS MATHÉMATIQUES

Il est sans doute plus facile de *faire* des mathématiques que de savoir *ce que c'est* exactement. Les deux idées suivantes semblent cependant consensuelles :

- il existe des *objets ou concepts mathématiques* (même si cette notion est difficile à définir précisément),
- dans notre discipline, on étudie des *affirmations portant sur ces objets ou concepts* ; bien souvent, on tente d'établir si ces affirmations sont vraies ou fausses.

Le but de ce chapitre n'est pas d'expliquer ce qu'est un objet mathématique, ni d'explorer en grand détail la structure du discours mathématique : des questions de ce type forment un domaine d'étude à part entière, la *logique mathématique*. Il s'agit simplement de vous présenter certains éléments de base sur la manière dont les énoncés mathématiques sont construits : ces éléments sont ceux qui s'avèrent nécessaires pour la pratique quotidienne des mathématiques dans le supérieur.

1. Qu'est-ce qu'un énoncé mathématique ?

1.1. Énoncés, variables. — Une *assertion*, ou *énoncé*, est une affirmation portant sur des objets. Voici des exemples d'assertions mathématiques :

$$\text{La fonction exp tend vers } +\infty \text{ en } +\infty \tag{1.1}$$

$$\text{La fonction } f \text{ est croissante} \tag{1.2}$$

$$n \text{ est pair} \tag{1.3}$$

$$\text{Il existe un nombre réel } x \text{ vérifiant } x^4 - 2x^2 + 2 < 0 \tag{1.4}$$

$$2^3 \geq 10 \tag{1.5}$$

$$a^2 + b^2 > 3 \tag{1.6}$$

$$\text{Tous les nombres premiers sont impairs} \tag{1.7}$$

Certains de ces énoncés sont vrais, d'autres sont faux. Pour d'autres, il est impossible de savoir si l'assertion est vraie ou fausse, car ils portent sur des objets qui ne sont pas précisés.

Par exemple, les énoncés (1.4) et (1.5) sont sans ambiguité : il ne manque aucune information pour déterminer s'ils sont vrais ou faux (ils sont faux). Par contre, (1.2) porte sur une fonction f qui n'est pas précisée.

Lorsqu'un énoncé permet de savoir *sans aucune ambiguïté* sur quels objets il porte, on dit qu'il est *complet*. Un des principes fondamentaux en mathématiques est le fait que lorsqu'un énoncé est complet, il n'y a que deux cas possibles concernant ce qu'il affirme :

Une assertion complète est soit vraie, soit fausse.

Ainsi, si un énoncé est complet, soit il est vrai (et alors il est vrai *absolument*, sans « exception » ni « peut-être »), soit il est faux (et alors il est faux absolument, et pas « un peu faux » ou « parfois vrai »). Cela dit, on a naturellement le droit de *ne pas savoir* s'il est vrai ou faux, ou d'avoir deviné s'il est vrai ou faux sans arriver à *démontrer* son affirmation...

Les énoncés (1.1), (1.4), (1.5) et (1.7) sont complets. En revanche, les énoncés (1.2), (1.3) et (1.6) ne sont pas complets, car ils portent sur un ou des objets qui ne sont *pas précisés dans l'assertion* : dans (1.2) l'énoncé est une affirmation sur la fonction f, mais on ne dit pas qui est f, dans (1.3) l'énoncé porte sur un objet n qui n'est pas précisé, dans (1.6) l'énoncé est une affirmation sur deux objets a et b qui ne sont pas précisés. Pour des énoncés de ce type, les objets « non précisés et sur lesquels portent l'assertion » sont appelés des *variables*.

1.2. Vocabulaire : axiome, définition, théorème... — Parmi les énoncés complets, certains sont vrais, les autres faux. Mais les énoncés vrais n'ont pas tous le même *intérêt*. Pour pouvoir discuter de certains éléments du discours mathématique, voici six exemples d'énoncés complets.

$$2 - 17 = 5 \tag{1.8}$$

$$2^3 > 0,89 \tag{1.9}$$

Dans un triangle rectangle, le carré de la longueur de l'hypoténuse est la somme des carrés des longueurs des deux autres côtés (1.10)

Si n est un entier naturel, alors $n + 0 = n$. (1.11)

Si a, b et c sont trois entiers relatifs non nuls et si n est un entier vérifiant $n \geq 3$, alors il est impossible qu'on ait $a^n + b^n = c^n$. (1.12)

Si s est un nombre complexe vérifiant $s \notin \mathbb{Z}$ et $\sum_{n=1}^{+\infty} \frac{1}{n^s} = 0$, alors $\mathfrak{Re}(z) = -\frac{1}{2}$. (1.13)

On peut faire à leur sujet les remarques suivantes.

(a) L'énoncé (1.8) est complet, mais faux.
L'énoncé (1.9) est un énoncé complet, et il assurément vrai, mais il n'est pas très intéressant...

(b) En revanche, (1.10) est un énoncé vrai, et certainement plus important que le précédent : pour signaler son importance, on l'appelle *théorème* (de Pythagore). Vous avez vu dans vos études secondaires *pourquoi* il est vrai, c'est-à-dire comment le *démontrer* à partir des « règles » de la géométrie.

(c) L'énoncé (1.11) présente une difficulté. Il est vrai, et sans aucun doute plus utile au quotidien que (1.9). Mais si vous cherchez à le *démontrer*, par où commencer ? Est-ce un théorème ? Une « convention » ?

(d) L'énoncé (1.12) a été proposé par Pierre de Fermat en 1637 ; mais ce n'est que depuis 1994 (et les travaux, entre autres, d'Andrew Wiles) qu'on *sait* qu'il est vrai, autrement dit, qu'on dispose d'une *démonstration* reconnue comme valide par la communauté mathématique.

(e) Quant à l'énoncé (1.13), il est sans doute plus mystérieux ; pour qu'il prenne un sens, il faudrait *définir avec précision* ce que signifie $\sum_{n=1}^{+\infty} \frac{1}{n^s}$ lorsque s est un nombre complexe [1]. Vous conviendrez peut-être que si on donne une telle définition, alors (1.13) deviendra un énoncé complet, soit vrai, soit faux.

Voici un glossaire permettant de distinguer, en lien avec la discussion ci-dessus, différents éléments du discours mathématique.

- ***Définition.*** Une définition est un texte qui introduit un objet mathématique, ou des mots pour parler d'une situation mathématique, de façon précise et sans ambiguïté. Une définition n'est pas une assertion mathématique, mais elle introduit une terminologie qui doit être assez précise pour permettre de former des énoncés complets.

  Par exemple, le texte

  Soient d et n deux entiers relatifs.
  On dit que d est un diviseur *de n lorsqu'il existe un entier relatif k vérifiant : $n = kd$.*

  n'est pas une *assertion* mathématique. C'est une *définition* : il introduit une *terminologie* à partir de laquelle on pourra ensuite formuler des assertions mathématiques complètes, par exemple

  Le nombre 5 est un diviseur de 25, mais le nombre 7 n'est pas un diviseur de 25,

  ou d'autres définitions, comme

  Soit p un entier naturel. On dit que p est premier si $p \geq 2$ et si les seuls diviseurs de p sont 1 et p.

Parmi les énoncés complets, il y en a bien sûr qui sont vrais mais qui ne semblent pas avoir d'intérêt particulier, comme (1.9). Parmi les énoncés ayant un intérêt (ou paraissant en avoir un...), on distingue les types suivants.

- ***Axiome.*** Un énoncé complet dont on *décide* qu'il est vrai et que ce sera l'un de nos points de départ pour faire des mathématiques.

  La liste des axiomes couramment utilisés pour faire des mathématiques est extrêmement courte (et peut sembler ésotérique) ; nous ne ferons que l'évoquer au chapitre 2.

- ***Théorème.*** Un énoncé
  - complet,
  - vrai (c'est-à-dire démontré sans ambiguité à partir des axiomes),
  - jugé suffisamment intéressant pour mériter le nom de « théorème ».

- ***Proposition ou Lemme.*** La même chose qu'un théorème, mais jugé un peu moins important : digne d'être distingué des autres énoncés mathématiques vrais, digne d'être étudié, mais pas aussi important que les énoncés qui portent le nom de « théorème ».

- ***Corollaire d'un énoncé.*** Une assertion complète qui est vraie et qui peut être démontrée « facilement » à partir d'un énoncé donné au départ. Par exemple,

  Dans un carré dont le côté est de longueur 1, la longueur des diagonales est $\sqrt{2}$

  est un corollaire du théorème de Pythagore (1.10).

- ***Conjecture.*** Un énoncé complet, qui est donc soit vrai soit faux, et dont on *pense qu'il est vrai, mais sans savoir démontrer que c'est bien le cas.* La conjecture la plus célèbre en mathématiques à l'heure actuelle est probablement l'énoncé (1.13), la *conjecture de Riemann* (ou *hypothèse de Riemann*).

La distinction entre *théorème*, *proposition* et *lemme* est affaire d'appréciation sur ce qui est « important ». Elle est donc subjective : un même énoncé pourra être appelé « théorème » dans un ouvrage et « proposition » dans un autre.

---

1. En L2, vous verrez ce que signifie la « somme infinie » $\sum_{n=1}^{+\infty} \frac{1}{n^s}$ lorsque s est un nombre réel vérifiant $s > 1$; plus tard, en L3, vous verrez comment donner un sens à l'expression y compris lorsque s est un nombre complexe.

1.3. Équivalence logique. —

Définition 1.1 – Énoncés équivalents

Si P et Q sont deux énoncés, on dit que P et Q sont *équivalents* lorsqu'il est
- impossible que P soit vrai sans que Q soit vrai,
- et également impossible que Q soit vrai sans que P soit vrai.

Pour dire que P et Q sont équivalents, on dit aussi que « P est vrai *si et seulement si* Q est vrai ».

Exemple 1.2. — Si x est un nombre réel, les énoncés « $x \in [-8, 5]$ » et « $(x+8)(x-5) \leq 0$ » sont équivalents.

Remarque 1.3. — Si P et Q sont deux énoncés, l'affirmation « P et Q sont équivalents » est elle-même une assertion, qui peut être vraie ou fausse. On la note généralement $(P \iff Q)$.

Par exemple, l'affirmation « $x = 3 \iff x + 2 = 5$ » est une affirmation vraie pour *tout* réel x, tandis que l'assertion « $x = 1 \iff x^2 = 1$ » est une affirmation qui n'est pas *vraie pour tout réel* x.

Attention. — En première année, pour éviter des confusions dommageables, il est important de ne pas utiliser le symbole $\iff$ comme abréviation de « c'est-à-dire » : il vaut mieux le réserver à des usages compatibles avec sa signification logique.

Vocabulaire : table de vérité. — Lorsque P et Q sont deux énoncés complets, chacun est soit vrai, soit faux, et donc l'énoncé $(P \iff Q)$ est lui-même complet. Compte tenu de la définition de l'équivalence logique, on peut alors déterminer s'il est vrai ou faux à partir des *valeurs de vérité* de P et Q. Le tableau suivant résume les résultats :

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

Ce tableau est connu sous le nom de *table de vérité* de l'équivalence logique. On remarquera que dans le cas où P et Q sont complets, il n'y a pas besoin de savoir exactement *ce que disent* P et Q pour savoir si l'énoncé $(P \iff Q)$ est vrai ou faux.

Remarque 1.4. — L'étude des propositions logiques à l'aide de tables de vérité est sans aucun doute utile. Mais le fait d'y distinguer radicalement « vérité » et « signification » peut être source d'inconfort. Par exemple, il semble raisonnable d'imaginer que l'assertion

$$\text{Pour tout entier } n \in \mathbb{N}, \quad \big(n \text{ est divisible par } 3 \iff n^2 \text{ est divisible par } 9 \big)$$

est utile pour faire des mathématiques. Par contre, elle a pour conséquence inévitable que l'affirmation

$$11 \text{ est divisible par } 3 \iff 121 \text{ est divisible par } 9$$

doit aussi être considérée comme une proposition vraie... même si celle-là, qui relie deux énoncés faux, a l'air moins intéressante pour faire des mathématiques.

1.4. Négation d'un énoncé mathématique. —

Définition 1.5 – Négation d'un énoncé

Si P est un énoncé, la *négation* de P est l'assertion « P n'est pas vrai ».
On note $\text{NON}(P)$ cette assertion.

Exemple 1.6. —
- Si x est un nombre réel, alors la négation de « $x > 3$ » est « $x \leq 3$ ».
- Si f est une fonction de $\mathbb{R}$ dans $\mathbb{R}$, la négation de l'assertion « pour tout réel x, on a $f(x) \in]0,1[$ » est l'assertion « il existe au moins un réel x vérifiant $f(x) \notin]0,1[$ ».

Attention. — On peut commettre des erreurs embarrassantes si l'on va trop vite au moment d'écrire la négation d'un énoncé. Voici quelques exemples :
- La négation de « dans tous les pays, tous les musiciens sont mortels » est « il existe au moins un pays dans lequel on peut trouver au moins un musicien immortel » (et non « il existe un pays où tous les musiciens sont immortels »).
- La négation de « ma voiture est blanche » est simplement « ma voiture n'est pas blanche » : c'est très différent de « ma voiture est noire », n'est-ce pas ?
- De même, si f est une fonction de $\mathbb{R}$ dans $\mathbb{R}$, la négation de « f est croissante » est simplement « f n'est pas croissante ». C'est très différent de « f est décroissante » (voyez-vous pourquoi ?).

Axiome 1.7 – Double négation

Pour tout énoncé P, on a l'équivalence $P \iff \text{NON}\,[\text{NON}(P)]$.

Cet axiome exprime le fait qu'on ne reconnaît en mathématiques que deux « valeurs de vérité » : si un énoncé complet n'est pas faux, alors c'est qu'il est vrai !

2. Connecteurs logiques : conjonction, disjonction

2.1. Les connecteurs ET et OU. —

Définition 1.8 – Conjonction de deux énoncés

Si P et Q sont deux énoncés, l'énoncé (P ET Q) est l'assertion « P est vrai *et* Q est vrai ».

L'énoncé (P ET Q) est vrai lorsque P et Q sont *tous les deux* vrais, et il est faux dans tous les autres cas. Par exemple, « $(2+2=4)$ ET $(3+3=6)$ » est vrai, mais « $(2+2=4)$ ET $(3+3=7)$ » est faux.

Notation. — On note parfois $(P \wedge Q)$ ou $(P \,\&\, Q)$ l'énoncé (P ET Q).

Définition 1.9 – Disjonction de deux énoncés

Si P et Q sont deux énoncés, l'énoncé (P OU Q) est l'assertion « l'un au moins des énoncés P, Q est vrai ».

Remarque 1.10. — Si les énoncés P et Q sont tous les deux vrais, alors l'énoncé (P OU Q) est vrai. On dit que le OU est *inclusif* en mathématiques, contrairement à ce qui se produit souvent dans le langage courant (« la bourse ou la vie »).

Exemple 1.11. — Considérons l'énoncé

$$((2+2=4) \text{ OU (il existe une infinité de couples de nombres premiers jumeaux)}.$$

Avant même de regarder la deuxième partie de l'énoncé (et même sans savoir ce qu'elle veut dire...), on sait que l'affirmation est vraie.

2.2. Négation d'un ET et d'un OU : les lois de De Morgan. —

Proposition 1.12 – Lois de De Morgan

Si P et Q sont deux énoncés, alors

$$\text{NON}\,(P\ \text{ET}\ Q)\ \textit{équivaut à}\ [(\text{NON}(P))\ \text{OU}\ (\text{NON}(Q))].$$
$$\text{NON}\,(P\ \text{OU}\ Q)\ \textit{équivaut à}\ [(\text{NON}(P))\ \text{ET}\ (\text{NON}(Q))].$$

Exemple 1.13. — Si f est une fonction de $\mathbb{R}$ dans $\mathbb{R}$, on a l'équivalence

$$\text{NON}\,(f(0)=0 \text{ ou } f(1)=0) \iff (f(0)\neq 0 \text{ et } f(1)\neq 0)\,.$$

Formellement, on peut retenir que la négation *échange le* ET *et le* OU.

Démonstration des lois de De Morgan. — Nous nous concentrons sur la première équivalence, l'autre se prouvant de la même manière.

Observons les différents cas possibles selon les valeurs de vérité de P et Q. En analysant chaque cas, on obtient la table de vérité suivante :

P	Q	NON $(P$ ET $Q)$	NON(P) OU NON(Q)
V	V	F	F
V	F	V	V
F	V	V	V
F	F	V	V

On constate qu'il est impossible que $A = \text{NON}\,(P\ \text{ET}\ Q)$ soit vrai sans que $B = \text{NON}(P)\ \text{OU}\ \text{NON}(Q)$ soit vrai aussi, et impossible que A soit faux sans que B soit faux aussi. C'est donc que les énoncés A et B sont équivalents, comme annoncé.

□

2.3. Le calcul propositionnel. — Partant de deux énoncés P et Q, on peut fabriquer plusieurs autres énoncés grâce aux connecteurs logiques. Cela permet de « fabriquer mécaniquement » des énoncés de plus en plus complexes, par exemple

$$[\text{NON}\,(P\ \text{ET}\,(\text{NON}\ Q))]\ \text{OU}\,(\text{NON}(P)\ \text{OU}\ \text{NON}(Q))\,. \tag{2.1}$$

Remarque 1.14. — Dans des assertions du type ci-dessus, la place des parenthèses est importante. Par exemple, NON$(P$ OU $Q)$ n'a pas la même signification que $(\text{NON}\ P)\ \text{OU}\ Q$: si P et Q sont toutes les deux vraies, la première des deux assertions est fausse alors que la seconde est vraie.

Reconnaissons que des assertions comme (2.1) peuvent paraître alambiquées. Cependant, sur des exemples concrets, on peut constater qu'elles sont utiles. Par exemple, imaginons que l'énoncé suivant soit vrai :

$$\big[\text{NON}\,(\text{j'ai les cheveux blonds})\ \text{OU}\,(\text{j'ai des chaussures noires})\,\big]\quad \text{ET}\quad (\text{j'ai les cheveux blonds})\,. \tag{2.2}$$

- On peut en tirer une information : si (2.2) est vrai, alors j'ai des chaussures noires.
- Par ailleurs, la nature exacte des énoncés à partir desquels il est composé n'a aucune importance : pour analyser la *forme logique* de l'énoncé (2.2), le fait qu'il soit composé avec des affirmations sur des chapeaux et chaussures ne joue aucun rôle.

Au fond, l'information à tirer de (2.2) est assez bien capturée par l'équivalence formelle suivante :

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

Lorsqu'on analyse ainsi des expressions logiques « compliquées » afin d'en donner une forme équivalente plus simple, on dit qu'on effectue un « calcul propositionnel ». Ce type de calcul est peu utilisé au quotidien dans la plupart des domaines mathématiques, et nous n'en aurons pas vraiment besoin au-delà de ce chapitre. Mais il est d'une extrême importance en informatique (et les propositions de ce paragraphe sous-tendent le fonctionnement des processeurs de nos ordinateurs)...

Voici des exemples de propriétés formelles très utiles pour ce type de « calcul propositionnel » ;

Proposition 1.15 – Exemples de règles formelles sur le ET et le OU

Si P, Q et R sont trois énoncés, alors on a les équivalences suivantes :

- Distributivité du ET sur le OU : $P\ \text{ET}\ (Q\ \text{OU}\ R) \iff (P\ \text{ET}\ Q)\ \text{OU}\ (P\ \text{ET}\ R)$
- Distributivité du OU sur le ET : $P\ \text{OU}\ (Q\ \text{ET}\ R) \iff (P\ \text{OU}\ Q)\ \text{ET}\ (P\ \text{OU}\ R)$

On a également toujours :

- Associativité du ET : $P\ \text{ET}\ (Q\ \text{ET}\ R) \iff (P\ \text{ET}\ Q)\ \text{ET}\ R$
- Associativité du OU : $P\ \text{OU}\ (Q\ \text{OU}\ R) \iff (P\ \text{OU}\ Q)\ \text{OU}\ R$
- Commutativité du ET : $(P\ \text{ET}\ Q) \iff (Q\ \text{ET}\ P)$
- Commutativité du OU : $(P\ \text{OU}\ Q) \iff (Q\ \text{OU}\ P)$

Démonstration. — On peut utiliser des tables de vérité ; voir l'exercice 1.5. □

Ces règles seraient plus difficiles à manier si vous n'aviez pas déjà beaucoup manipulé, pour les *nombres* (entiers ou réels), la distributivité de la multiplication sur l'addition.

Exemple 1.16. — Si a, b, c, d étaient des entiers et s'il était question de simplifier

$$(a+b)\times(c+d)$$

vous n'hésiteriez pas à écrire, *grâce à la distributivité de la multiplication sur l'addition*, que c'est égal à

$$(a\times c)\ +\ (a\times d)\ +(b\times c)\ +(b\times d).$$

Si P, Q, R et S sont quatre énoncés et s'il est question de simplifier

$$A = (P\ \text{OU}\ Q)\ \text{ET}\ (R\ \text{OU}\ S)\,,$$

appliquer les règles ci-dessus mène à un résultat analogue :

$$A \iff (P\ \text{ET}\ R)\,\text{OU}\,(P\ \text{ET}\ \ S)\,\text{OU}\,(Q\ \text{ET}\ R)\,\text{OU}\,(Q\ \ \text{ET}\ S)\,.$$

3. Implication logique

3.1. Définition formelle et remarques. — Le statut de l'affirmation « si P, alors Q » est plus subtil que celui des énoncés rencontrés jusqu'ici.

Définition 1.17 – Implication logique

Si P et Q sont deux énoncés mathématiques, on définit l'énoncé $(P \implies Q)$ comme l'assertion

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

Vocabulaire. — Dans l'implication $(P \implies Q)$, on dit que P est la *prémisse*, ou *l'hypothèse*, et Q la *conclusion*.

Exemple 1.18. — Fixons un nombre réel x. Analysons le contenu de l'énoncé

$$x \geq 3 \implies x^2 \geq 9 \tag{3.1}$$

Notons P l'affirmation « $x \geq 3$ » et Q l'affirmation « $x^2 \geq 9$ ».
Il y a deux situations possibles selon que P : « $x \geq 3$ » est vraie ou non :

- si $x \geq 3$, alors savoir que (3.1) est vraie nous fournit la certitude que $x^2 \geq 9$.
  Ici $\text{NON}(P)$ est fausse, donc si $(\text{NON}(P) \text{ OU } Q)$ est vraie, c'est nécessairement que Q est vrai.
- Par contre, si $x < 3$, alors l'implication (3.1) *ne nous apprend rien sur* x^2 :
  on peut très bien avoir $x^2 \geq 9$ (par exemple quand $x = -10$) ou $x^2 < 9$ (par exemple quand $x = 2$).
  Cela se retrouve dans la structure logique : ici, puisque $\text{NON}(P)$ est vraie, l'énoncé $(\text{NON}(P) \text{ OU } Q)$ est vrai que Q soit faux ou non.

Remarque 1.19. — Il faut faire bien attention au sens logique de l'implication. En observant la définition, on peut résumer les liens entre P, Q et $P \implies Q$ par la table de vérité suivante :

P	Q	P ⇒ Q
V	V	V
V	F	F
F	V	V
F	F	V

On constate donc que *la seule manière qu'une implication soit fausse, c'est que la prémisse soit vraie mais pas la conclusion.* Cela est cohérent avec le fait que, selon les lois de De Morgan, la négation de $(P \implies Q)$ est $(P \text{ ET } \text{NON}(Q))$.

Un aspect essentiel de ce qui précède est le principe général

« Faux implique n'importe quoi »,

ou en latin : *ex falso quodlibet* (« de faux, ce que l'on veut »).

On trouve trace de ce principe dans le langage courant (« Quand les poules auront des dents... »), mais il peut être source de confusions en mathématiques.

Exemple 1.20. — Pour tout $n \in \mathbb{N}$, l'implication suivante est vraie :

$$(n \text{ divisible par } 4 \implies n \text{ pair}).$$

Cette implication est simple et potentiellement utile. Mais si on l'accepte, alors il faut inévitablement accepter que les affirmations suivantes sont vraies :

$$(1 \text{ divisible par } 4) \implies (1 \text{ pair})$$
$$(2 \text{ divisible par } 4) \implies (2 \text{ pair}).$$

Si ces affirmations vraies paraissent étranges, c'est parce que ce sont des exemples de « faux implique faux » ou de « faux implique vrai ».

3.2. Vocabulaire : condition nécessaire, condition suffisante. —

Soit x un objet mathématique ; considérons deux assertions $\mathcal{P}(x)$ et $\mathcal{Q}(x)$ portant sur l'objet x.

Condition nécessaire. — On dit que $\mathcal{P}(x)$ est une condition *nécessaire* pour $\mathcal{Q}(x)$ s'il est impossible que $\mathcal{Q}(x)$ soit vraie sans que $\mathcal{P}(x)$ soit vraie aussi. Cela revient à dire que l'assertion $(\mathcal{Q}(x) \implies \mathcal{P}(x))$ est vraie.

Les expressions « il est nécessaire que », « il faut que » signalent en général la présence de conditions nécessaires.

Exemple 1.21. —

- Pour qu'un entier naturel k soit divisible par 6, il est nécessaire que k soit divisible par 2.
- Pour qu'un entier relatif n puisse s'écrire comme le carré d'un autre entier, il faut qu'on ait $n \geq 0$.
- Pour qu'une fonction $f : \mathbb{R} \to \mathbb{R}$ soit impaire, une condition nécessaire est $f(0) = 0$.
- Pour qu'un quadrilatère soit un carré, il faut que ses quatre côtés aient la même longueur.

Condition suffisante. — Reprenant les notations ci-dessus, on dit que $\mathcal{P}(x)$ est une condition *suffisante* pour $\mathcal{Q}(x)$ si le fait que $\mathcal{P}(x)$ soit vraie garantit automatiquement que $\mathcal{Q}(x)$ soit vraie. Formellement, cela signifie qu'il est impossible que $\mathcal{P}(x)$ soit vraie sans que $\mathcal{Q}(x)$ soit vraie aussi, ce qui revient à dire que l'assertion $(\mathcal{P}(x) \implies \mathcal{Q}(x))$ est vraie.

Les expressions « il suffit que », « dès que » signalent en général la présence de conditions suffisantes.

Exemple 1.22. —

- Soient a, b et c trois réels.
  Pour qu'il existe un réel x vérifiant $ax^2 + bx + c = 0$, il suffit que a et c soient de signes contraires.
- Pour qu'une fonction $f : \mathbb{R} \to \mathbb{R}$ soit croissante, il suffit que f soit dérivable et de dérivée partout strictement supérieure à 98.
- Pour qu'une suite $(u_n)_{n\in\mathbb{N}}$ de nombres réels soit convergente, il est suffisant qu'elle soit croissante et majorée.
- Pour x réel, on a $x^2 \geq 9$ dès que $x \geq 3$.

Condition nécessaire et suffisante. — Compte tenu de ce qui précède, dire que $\mathcal{P}(x)$ est une *condition nécessaire et suffisante* pour $\mathcal{Q}(x)$, c'est dire que les énoncés $\mathcal{P}(x)$ et $\mathcal{Q}(x)$ sont logiquement équivalents.

Les expressions « il faut et il suffit », « si et seulement si », « c'est-à-dire », « autrement dit »... signalent en général la présence de conditions nécessaires et suffisantes.

Exemple 1.23. —

- Soient a, b et c trois réels. Pour qu'il existe au moins un réel x vérifiant $ax^2 + bx + c = 0$, il faut et il suffit que le nombre $b^2 - 4ac$ soit positif.
- Pour qu'un réel x puisse s'écrire sous la forme a^2 avec $a \in \mathbb{R}$, il faut et il suffit que x soit positif.

3.3. Équivalence et double implication. —

Proposition 1.24 – Équivalence et double implication

Deux énoncés P et Q sont équivalents si et seulement si on a $(P \implies Q)$ et $(Q \implies P)$.

Démonstration (peut être omise en première lecture). — Utilisons le calcul propositionnel pour simplifier l'expression $A : (P \implies Q) \text{ ET } (Q \implies P)$. On a

$$A \iff (\text{NON}(P) \text{ OU } Q) \text{ ET } (\text{NON}(Q) \text{ OU } P).).$$

Notons $U = \text{NON}(P)$, $V = Q$, $W = \text{NON}(Q)$ et $X = P$: alors A est l'énoncé $(U \text{ OU } V) \text{ ET } (W \text{ OU } X)$. Rappelons que nous avons vu à l'exemple 1.16 l'équivalence suivante :

$$(U \text{ OU } V) \text{ ET } (W \text{ OU } X) \iff (U \text{ ET } W) \text{ OU } (U \text{ ET } X) \text{ OU } (V \text{ ET } W) \text{ OU } (V \text{ ET } X).$$

Dans notre cas, $(U \text{ ET } X)$ est l'énoncé $\text{NON}(P) \text{ ET } P$; il n'est jamais vrai. De même, $(V \text{ ET } W)$ n'est jamais vrai. En observant les énoncés $U \text{ OU } W$ et $V \text{ OU } X$, on constate alors que

$$A \iff (P \text{ ET } Q) \text{ OU } (\text{NON}(P) \text{ ET NON}(Q)) .$$

Mais le dernier énoncé est équivalent à $(P \iff Q)$. En effet, il est vrai quand P et Q ont la même valeur de vérité et faux quand P et Q n'ont pas la même valeur de vérité. Cela conclut notre démonstration. □

3.4. Contraposée d'une implication. —

Définition 1.25 – Contraposée d'une implication

Si P et Q sont deux assertions, alors la *contraposée* de l'implication $(P \implies Q)$ est l'énoncé $(\text{NON}(Q) \implies \text{NON}(P))$.

Par exemple, lorsque f est une fonction de $\mathbb{R}$ dans $\mathbb{R}$, la contraposée de l'implication

$$\text{« si } f \text{ est impaire, alors } f(0) = 0 \text{ »}$$

est l'affirmation

$$\text{« si } f(0) \neq 0, \text{ alors } f \text{ n'est pas impaire »}.$$

Le fait que la seconde assertion soit tout aussi vraie que la première n'est pas un hasard. En fait, une implication et sa contraposée ont *toujours* la même signification :

Proposition 1.26 – Équivalence entre une implication et sa contraposée

Si P et Q sont deux assertions, alors

$$(P \implies Q) \quad \textit{équivaut à} \quad (\text{NON}(Q) \implies \text{NON}(P)).$$

Démonstration. — Si P et Q sont deux assertions, alors l'énoncé « $\text{NON}(Q) \implies \text{NON}(P)$ » est, par définition de l'implication logique, équivalent à « $\text{NON}(\text{NON}(Q)) \text{ OU NON}(P)$ », autrement dit, par l'axiome 1.7, à « $Q \text{ OU NON}(P)$ ». Il est donc équivalent à l'énoncé « $\text{NON}(P) \text{ OU } Q$ », qui est exactement $(P \implies Q)$. □

Exemple 1.27. — Fixons un entier naturel n. Supposons qu'on veuille démontrer l'assertion suivante :

$$\text{Si } n^2 \text{ est impair, alors } n \text{ est nécessairement impair.} \tag{3.2}$$

On peut utiliser le fait que l'assertion (3.2) est équivalente à sa contraposée, à savoir :

$$\text{Si } n \text{ est pair, alors } n^2 \text{ est pair.} \tag{3.3}$$

L'assertion (3.3) est peut-être plus facile à démontrer : si n est pair, alors on peut écrire $n = 2k$ avec $k \in \mathbb{N}$, et alors $n^2 = (2k)^2 = 2(2k^2)$, donc n^2 peut s'écrire sous la forme $2m$ où $m = 2k^2$ est entier, ainsi n^2 est pair.

Remarque 1.28. — Ne pas confondre la *contraposée* d'une implication $P \implies Q$, qui en est une reformulation équivalente, et sa *réciproque*, qui est l'implication $Q \implies P$. La réciproque peut avoir une signification très différente de l'implication initiale (et être fausse si l'implication initiale est vraie). Par exemple, si on fixe un réel x, alors

- La contraposée de « $x = 2 \implies x^2 = 4$ » est « $x^2 \neq 4 \implies x \neq 2$ », et comme l'implication de départ est vraie pour tout réel x, cette contraposée est aussi vraie pour tout réel x.
- La réciproque de « $x = 2 \implies x^2 = 4$ » est « $x^2 = 4 \implies x = 2$ », et ce n'est *pas* une implication vraie pour tout réel x.

4. Quantificateurs : « pour tout » et « il existe »

4.1. Quantificateurs $\forall$ et $\exists$. — Supposons donnés un ensemble E et, pour tout élément x de E, une assertion $P(x)$.

Définition 1.29 – Énoncé avec quantificateur universel ou existentiel

L'énoncé « $\forall x \in E,\ P(x)$ » signifie : « pour tout élément x de E, l'assertion $P(x)$ est vraie ».

L'énoncé « $\exists x \in E \ / \ P(x)$ » signifie : « il existe au moins un élément x de E tel que $P(x)$ soit vraie ».

Exemple 1.30. — L'assertion

$$\forall x \in \mathbb{R},\ \ x^2 + x + 1 \geq 0$$

est vraie (voyez-vous pourquoi ?). Par contre, l'assertion

$$\forall x \in \mathbb{R},\ \ (x-1)(x-3) \geq 0,$$

est fausse, puisque pour $x = 2$, on a $(x-1)(x-3) < 0$. Quant à l'assertion

$$\exists x \in \mathbb{R} \ / \ (x-1)(x-3) \geq 0,$$

elle est vraie, puisque pour $x = 4$, l'inégalité est vérifiée.

Remarque 1.31. — Pour lire à haute voix un énoncé du type « $\forall x \in E,\ P(x)$ », la virgule peut se lire « on a » (ou ne pas se lire). Dans un énoncé du type « $\exists x \in E \ / \ P(x)$ », la barre peut se lire « tel(le) que » ou « vérifiant : ». par exemple, l'énoncé

$$\exists a \in \mathbb{R} \ / \ \forall x \in \mathbb{R},\ x^2 + 1 > a \tag{4.1}$$

se lit

« il existe un réel a tel que pour tout réel x, on ait $x^2 + 1 > a$ », ou

« il existe un réel a vérifiant : pour tout réel x, le nombre $x^2 + 1$ est strictement supérieur à a ».

La barre après $\exists$ n'est pas indispensable et si elle ne facilite pas la lecture, on peut la remplacer par une virgule ou par deux points : dans (4.1), les écritures

$$\exists a \in \mathbb{R} \ / \ \forall x \in \mathbb{R},\ x^2 + 1 > a$$
$$\exists a \in \mathbb{R},\ \ \forall x \in \mathbb{R},\ x^2 + 1 > a$$
$$\exists a \in \mathbb{R}\ : \forall x \in \mathbb{R},\ x^2 + 1 > a$$

ont exactement la même signification.

Notion de variable muette. — Considérons les deux énoncés suivants :

$$\ln(x^2 + 1) \geq 1 \tag{4.2}$$

$$\forall x \in \mathbb{R},\ \exp(x) > 0. \tag{4.3}$$

Les deux font intervenir le symbole x, mais de façon très différente.

- L'énoncé (4.2) n'est pas complet : c'est une affirmation portant sur un objet x qui n'est pas précisé. On peut décider de « voir si cet énoncé est vrai quand $x = e^2 - 1$ » (il l'est), ou de « voir si cet énoncé est vrai quand $x = 0$ » (il ne l'est pas).
- L'énoncé (4.3) est très différent : il est *complet*, et il est vrai.

Il est important de voir que contrairement à (4.2), l'énoncé (4.3) n'est pas une « affirmation portant sur un objet x ». Le rôle du symbole x dans l'énoncé (4.3) est très différent, et mérite discussion. En effet, la phrase

La fonction exp *est strictement positive sur* $\mathbb{R}$

porte exactement la même information... et ne fait pas intervenir la variable x ! C'est donc que le symbole x n'est qu'une sorte « d'intermédiaire » pour écrire (4.3). On pouvait s'en passer, et utiliser le symbole x n'est qu'un choix pour écrire ce que l'on a à dire. On aurait d'ailleurs pu choisir un autre symbole : l'énoncé

$$\forall u \in \mathbb{R},\ \exp(u) > 0 \tag{4.4}$$

a exactement la même signification que (4.3) Dans les situations où un énoncé

- fait intervenir une variable x dans sa formulation
- mais peut être reformulé de façon équivalente sans utiliser le symbole x,

on dit que la variable x est *muette* dans l'énoncé.

Dans une assertion du type « $\forall x \in E,\ P(x)$ » ou « $\exists x \in E\ /\ P(x)$ », la variable x est muette.

Vous connaissez d'autres exemples de situation où l'on trouve des variables muettes.

Par exemple, l'écriture $\sum_{k=1}^{100} k^2$ désigne « la somme des carrés des entiers de 1 à 100 » : dans l'écriture avec le symbole $\sum$, la variable k est muette. Il n'y a pas de différence entre $\left(\sum_{k=1}^{100} k^2\right)$ et $\left(\sum_{a=1}^{100} a^2\right)$.

Devant un texte mathématique, repérer les variables qui sont muettes et celles qui ne le sont pas doit devenir un réflexe.

Vocabulaire : le pseudo-quantificateur $\exists!$ ***(il existe un unique).*** — Lorsqu'une assertion du type « $\exists x \in E\ /\ \mathcal{P}(x)$ » est vraie, il existe au moins un élément x de E pour lequel $\mathcal{P}(x)$ est vrai. Dans ce cas, deux situations peuvent se présenter :

- il est possible qu'il y ait *plusieurs* (au moins deux) éléments x tels que $\mathcal{P}(x)$ soit vrai : il existe alors des éléments x et x' de E vérifiant $x \neq x'$ et tels que $\mathcal{P}(x)$ et $\mathcal{P}(x')$ soient vrais.
- mais il est aussi possible qu'il y ait *un seul* élément x de E tel que $\mathcal{P}(x)$ soit vrai : si x et x' sont deux éléments de E tels que $\mathcal{P}(x)$ et $\mathcal{P}(x')$ soient vrais, on aura alors nécessairement $x = x'$.

Pour signifier qu'on est dans le second cas, on ajoute parfois un point d'exclamation au symbole $\exists$, et on écrit « $\exists! x \in E\ /\ \mathcal{P}(x)$ ». Par exemple, l'assertion

$$\forall y \in \mathbb{R}_\star^+,\ \exists! x \in \mathbb{R}\ :\ e^x = y$$

est vraie, puisque si y est un réel strictement positif, alors $x = \ln(y)$ est un réel qui vérifie $e^x = y$, et c'est le seul. En revanche, l'assertion

$$\forall y \in \mathbb{R}_\star^+,\ \exists! x \in \mathbb{R}\ :\ x^2 = y$$

est fausse : par exemple, si $y = 4$, alors les nombres 2 et -2 ont pour carré y, mais sont distincts.

4.2. Quantificateurs imbriqués. — Les quantificateurs $\forall$ et $\exists$ permettent de former de nombreuses assertions mathématiques. Dans certaines des plus importantes, il y a *beaucoup* de quantificateurs. Par exemple, si $(u_n)_{n\in\mathbb{N}}$ est une suite de nombres réels, vous étudierez en détail (dès le premier semestre de L1) des assertions comme

$$\exists \ell \in \mathbb{R},\quad \forall \varepsilon > 0,\quad \exists N \in \mathbb{N}\quad ,\quad \forall n \in \mathbb{N},\qquad (n \geq N \implies |u_n - \ell| < \varepsilon)$$

(il s'agit de la définition rigoureuse de « la suite $(u_n)_{n\in\mathbb{N}}$ est convergente »).

Il est donc important d'être à l'aise avec les assertions comportant plusieurs quantificateurs.

Exemple 1.32. — Considérons les deux assertions suivantes :

$$\forall x \in \mathbb{R}, \quad \exists y \in \mathbb{R} \ : \ y+1 > x^2, \tag{4.5}$$

$$\exists y \in \mathbb{R} \ / \ \forall x \in \mathbb{R}, \quad y+1 > x^2. \tag{4.6}$$

Ces deux assertions n'ont *pas du tout* la même signification.

- La première est vraie : si x est un nombre réel, alors en choisissant $y = x^2$, on constate que $y+1 > x^2$.
- La seconde est fausse : en effet, s'il existait un réel y vérifiant : $\forall x \in \mathbb{R}, \quad y+1 > x^2$, alors on pourrait appliquer cette affirmation avec $x = \sqrt{|y|+1}$, et on obtiendrait $y+1 > |y|+1$, ce qui est impossible.

Exemple 1.33. — Un autre exemple, plus caricatural, est

Pour toute cerise $\mathcal{C}$, il existe un noyau N tel que le noyau N se trouve dans $\mathcal{C}$

Il existe un noyau N vérifiant : pour toute cerise $\mathcal{C}$, le noyau N se trouve dans $\mathcal{C}$.

Cet exemple non strictement mathématique, mais où la non-équivalence des deux assertions saute aux yeux, fait bien ressortir la différence essentielle entre les affirmations « $\forall \mathcal{C}$, $\exists N$, $(\dots)$ » et « $\exists N$, $\forall \mathcal{C}$, $(\dots)$ ».

- En affirmant que pour toute cerise $\mathcal{C}$, il existe un N situé dans $\mathcal{C}$, il semble aller de soi que N *dépend* a priori *de* $\mathcal{C}$.
- Au contraire, en affirmant $\exists N$, $\forall \mathcal{C}$, $(\dots)$, alors on affirme qu'il existe un N qui ne *dépend pas des variables introduites après*, et qui est commun à toutes les $\mathcal{C}$ possible.

Dans une assertion comportant plusieurs quantificateurs, l'ordre est très important.
Il permet notamment de déterminer quelles variables « peuvent dépendre des autres ».

Exemple 1.34. — Considérons les trois affirmations

$$\forall x \in \mathbb{R}^\star, \quad \exists M \in \mathbb{R}^\star \ : \quad (x+M)^2 = x^2. \tag{4.7}$$

$$\exists M \in \mathbb{R}^\star \ : \quad \forall x \in \mathbb{R}^\star, \quad (x+M)^2 = x^2. \tag{4.8}$$

$$\exists M \in \mathbb{R}^\star \ : \quad \forall x \in \mathbb{R}, \quad \exists y \in \mathbb{R} \ : \ (x+M)^2 = My + x + \frac{1}{4}. \tag{4.9}$$

- La première est vraie : si on fixe un réel non nul x et si on cherche un réel $M \neq 0$ vérifiant $(x+M)^2 = x^2$, en se rappelant que M peut dépendre de x, on constate que $M = -2x$ convient.
- La seconde est fausse. S'il existe un $M \neq 0$ qui vérifie :

$$\forall x \in \mathbb{R}^\star, \quad (x+M)^2 = M^2, \tag{4.10}$$

  on doit pouvoir appliquer (4.10) à $x = -M$; on obtient alors $0 = M^2$, et cela est impossible si M est non-nul.
- La troisième est vraie. Pour le démontrer, on doit chercher un $M \neq 0$ (indépendant des autres variables à venir) vérifiant

$$\forall x \in \mathbb{R}, \quad \exists y \in \mathbb{R} \quad : \quad x^2 + 2Mx + M^2 = My + x + \frac{1}{4} \tag{4.11}$$

  (on notera que dans l'affirmation, le y peut éventuellement dépendre de x, mais aussi de M).

  Si on choisit $M = \frac{1}{2}$, si l'on fixe un nombre $x \in \mathbb{R}$, et si l'on cherche un y vérifiant (4.11), on constate qu'en choisissant $y = \frac{x^2}{M}$ on a bien $x^2 + 2Mx + M^2 = y + x + \frac{1}{4}$.

4.3. Négation d'un énoncé écrit avec des quantificateurs. —

Proposition 1.35 – Négation d'un $\forall$ ou d'un $\exists$

On a les équivalences logiques

$$\text{non}\,[\ \forall x \in E,\ \ P(x)\ ] \iff [\ \exists x \in E\ /\ \text{non}\,(P(x))\ ]\,.$$
$$\text{non}\,[\ \exists x \in E\ /\ P(x)\ ] \iff [\ \forall x \in E,\ \text{non}\,(P(x))\ ]\,.$$

En français :

- Dire que « $\forall x \in E,\ P(x)$ » est fausse, c'est dire qu'il existe *au moins* un x de E pour lequel $P(x)$ n'est pas vérifiée.
- Dire que l'assertion « $\exists x \in E\ /\ P(x)$ » est fausse, c'est dire que l'assertion $P(x)$ est fausse pour *tout* x de E,

Exemple 1.36. — La négation de

$$\forall x \in \mathbb{R},\ \ x^2 + x + 1 \geq 0$$

est

$$\exists x \in \mathbb{R},\ \ x^2 + x + 1 < 0.$$

***Exemple 1.37* (Cas de deux quantificateurs imbriqués).** — Considérons l'énoncé suivant :

$$\forall x \in \mathbb{R},\ \exists n \in \mathbb{N},\ \ x \leq n. \tag{$\star$}$$

Cet énoncé est du type « $\forall x \in \mathbb{R}, (\dots)$ », même si ce qu'il y a dans les $(\dots)$ est un énoncé lui-même formulé avec des quantificateurs. On peut donc appliquer la proposition ci-dessus pour écrire sa négation ; c'est :

$$\exists x \in \mathbb{R}\ /\ \text{non}\,(\exists n \in \mathbb{N},\ \ x \leq n)\,. \qquad \text{(négation de } (\star)\text{, première version)}$$

On peut aller plus loin et écrire la négation du second énoncé avec « il existe ». On obtient :

$$\exists x \in \mathbb{R}\ /\ \forall n \in \mathbb{N},\ \ x > n. \qquad \text{(négation de } (\star)\text{, seconde version)}$$

On constate que dans la négation de $(\star)$, tous les quantificateurs ont été « inversés » (échange des $\forall$ et $\exists$).

L'exemple précédent fournit une méthode générale pour écrire la négation d'un énoncé, même compliqué, comportant plusieurs quantificateurs imbriqués.

Méthode 1.38 – Négation d'un énoncé avec quantificateurs imbriqués

Pour nier un énoncé comportant plusieurs quantificateurs,

- *on change tous les $\forall$ en $\exists$ et tous les $\exists$ en $\forall$, en conservant soigneusement l'ordre,*
- *on écrit la négation de la partie non quantifiée.*

Exemple 1.39. — La négation de l'énoncé

$$\forall a \in \mathbb{N},\quad \forall b \in \mathbb{N}^\star,\quad \exists q \in \mathbb{N},\quad \exists r \in \mathbb{N},\quad (a = bq + r \text{ et } r < b) \tag{4.12}$$

est

$$\exists a \in \mathbb{N},\quad \exists b \in \mathbb{N}^\star,\quad \forall q \in \mathbb{N},\quad \forall r \in \mathbb{N},\quad (a \neq bq + r \text{ ou } r \geq b)\,.$$

On remarquera qu'on n'a *pas eu besoin de se poser la question de la signification* de l'énoncé (4.12) avant d'écrire sa négation. Il n'est pas important que cet énoncé complexe soit ou non « intéressant », ni de l'avoir compris, pour pouvoir écrire sa négation. (L'énoncé (4.12) *est*, malgré tout, intéressant : il affirme l'existence de la division euclidienne, sur laquelle nous reviendrons au chapitre 4).

Exercices du chapitre 1

Énoncés, définitions, théorèmes. —

***Exercice 1.1* (Énoncés complets). — ★☆☆**
Parmi les textes suivants, lesquels sont des énoncés mathématiques ? Lesquels sont complets ?

(a) Pour tout réel x, on a $x^2 > x + 1$.

(b) Pour tout réel x, on a $x^2 > a$.

(c) Il existe un réel a vérifiant : pour tout $x \in \mathbb{R}$, $x^2 > a$.

(d) L'ensemble des entiers n tels que $n^2 + 1$ soit multiple de 3.

(e) Soit n un entier naturel. On dit que n est *fantastique* si n^2 est multiple de 3.

(f) Si n est un entier naturel, alors $n^2 + 1$ est multiple de 3.

(g) Pour toute fonction $f : \mathbb{R} \to \mathbb{R}$ telle que f est croissante et positive,

(h) Pour toute fonction $f : \mathbb{R} \to \mathbb{R}$ impaire, on a $f(0) = 0$.

***Exercice 1.2* (Différence entre énoncé, définition et charabia). — ★☆☆**
Parmi les textes suivants, lesquels sont des définitions complètes ? des énoncés complets ?

(a) Soit a un nombre réel. On dit que a est *rationnel* s'il existe p et q vérifiant $a = \frac{p}{q}$.

(b) Si a est un réel positif, alors il existe $x \in \mathbb{R}$ vérifiant $a = x^2$.

(c) Si $n \neq 0$, alors $n \geq 1$.

(d) Soit n un entier relatif. On dit que n est *pair* s'il existe $k \in \mathbb{Z}$ vérifiant $n = 2k$.

(e) Soit $f : \mathbb{R} \to \mathbb{R}$ une fonction. On dit que f est *croissante* lorsque pour tous réels x, y, on a $f(x) \leq f(y)$.

Conjonction, disjonction, négation. —

***Exercice 1.3* (Manipulation des connecteurs ET, OU, NON). — ★☆☆**
On considère les assertions suivantes portant sur un réel x :

$$P : \text{« } x < 50. \text{ »} \quad \text{et} \quad Q : \text{« } x > 40. \text{ »}$$

Écrire simplement les énoncés

(a) $\text{NON}(P)$,

(b) $\text{NON}(Q)$,

(c) $P \text{ OU } Q$,

(d) $\text{NON}(P) \text{ OU } Q$,

(e) $\text{NON}(P \text{ OU } Q)$,

(f) $\text{NON}(P) \text{ ET NON}(Q)$.

(g) $\text{NON}(\text{NON}(P))$,

(h) $P \text{ ET } Q$,

***Exercice 1.4* (Langage courant et expression logique). — ★★☆**
Trois amis, A., B. et C. passent un test.
On note $\mathcal{A}$ l'énoncé « A. a réussi le test », $\mathcal{B}$ l'énoncé « B. a réussi le test », $\mathcal{C}$ l'énoncé « C. a réussi le test ».
Écrire à l'aide des connecteurs ET, OU et NON les énoncés suivants :

(i) C. est le seul à avoir réussi le test

(ii) A. est le seul à ne pas l'avoir réussi

(iii) Un seul des trois amis a réussi le test

(iv) Au moins l'un des trois amis a réussi le test

(v) Au moins deux des trois amis ont réussi le test

(vi) Deux des trois amis, et deux seulement, ont réussi le test.

***Exercice 1.5* (Fondements du calcul propositionnel).** — ★☆☆
En utilisant des tables de vérité, démontrer les deux distributivités de la proposition 1.15.

***Exercice 1.6* (Calcul propositionnel, I).** — Soient P, Q et R trois énoncés.

1. ★☆☆ Simplifier autant que possible les énoncés suivants :
   (a) $\text{NON}\,(\text{NON}(P)\,\text{ET}\,\text{NON}(Q))$
   (b) $(P\,\text{ET}\,Q)\,\text{OU}\,(P\,\text{ET}\,\text{NON}[Q])\,\text{OU}\,(\text{NON}(P)\,\text{ET}\,Q)$
   (c) $(Q\,\text{ET}\,\text{NON}(P))\,\text{OU}\,P$
2. ★★☆ Démontrer l'équivalence suivante :

$$\text{NON}\,[(P\,\text{OU}\,\text{NON}[Q])\,\text{OU}\,(R\,\text{ET}\,(P\,\text{OU}\,\text{NON}[Q]))] \iff (\text{NON}(P)\,\text{ET}\,Q)\,.$$

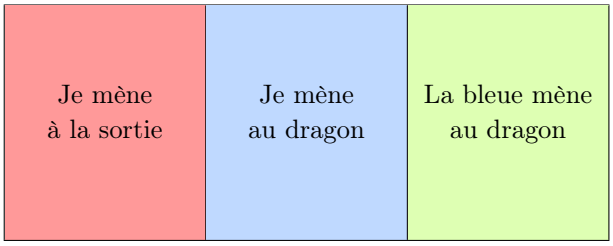
***Exercice 1.7* (Ou exclusif et barre de Sheffer).** — ★★☆
Si P et Q sont deux énoncés,

- on note $P \oplus Q$ l'énoncé « $(P\,\text{OU}\,Q)\,\text{ET}\,[\text{NON}(P\,\text{ET}\,Q)]$ »
- on note $P \uparrow Q$ l'énoncé « $\text{NON}\,(P\,\text{ET}\,Q)$ »

Montrer que les équivalences suivantes sont vraies pour tous énoncés P, Q, R :

1. (a) $(P \oplus Q) \iff [(P\,\text{OU}\,Q)\,\text{ET}\,(\text{NON}(P)\,\text{OU}\,\text{NON}(Q))]$
   (b) $[(P \oplus Q)\,\text{ET}\,R] \iff [(P\,\text{ET}\,R) \oplus (Q\,\text{ET}\,R)]$
2. (a) $(P \uparrow P) \iff \text{NON}(P)$
   (b) $(P \uparrow Q) \uparrow (P \uparrow Q) \iff (P\,\text{ET}\,Q)$
   (c) $(P \uparrow P) \uparrow (Q \uparrow Q) \iff (P\,\text{OU}\,Q)$

***Exercice 1.8* (Démêler un problème logique.)** — ★★★
Trois logicien·ne·s se trouvent dans un sombre donjon (l'histoire ne dit pas ce qui s'est passé jusque là...). Après une recherche rapide, les voilà qui découvrent trois portes : une rouge, une bleue, une verte. Elles portent les inscriptions suivantes :



Ils trouvent aussi un vieux parchemin avec les indications suivantes :

- Une seule des trois portes mène à la sortie ; les deux autres mènent à l'antre du dragon.
- Sur au moins l'une des portes, il est écrit la vérité.
- Sur au moins l'une des portes, il est écrit un mensonge.

Quel chemin prendre ?

Autour de l'implication logique. —

***Exercice 1.9* (Manipulation de la définition).** — ★☆☆
Soient P, Q, R trois assertions. On suppose que P est fausse, que Q est vraie et que R est vraie.

Parmi les assertions suivantes, lesquelles sont vraies ?

(a) $(P \implies \text{NON}(Q))\,\text{OU}\,[\text{NON}\,(R\,\text{ET}\,Q)]$
(b) $[\text{NON}(P)\,\text{OU}\,\text{NON}(Q)] \implies [P\,\text{OU}\,\text{NON}(R)]$

(c) $\text{NON}\,(\text{NON}(P) \implies \text{NON}(Q))\ \text{ET}\ R$

(d) $\text{NON}\,[\text{NON}(P) \implies [Q\ \text{ET}\ \text{NON}(R)]]$

***Exercice 1.10* (Contraposée et réciproque). — ★☆☆**
Dans tout l'exercice, on fixe un réel x et un entier naturel n.

Écrire la contraposée et la réciproque de chacune des implications suivantes :

1. Si le père Noël existe, alors Noël est en juillet.
2. Si $x \geq 3$, alors $x + 2 \geq 5$.
3. Si $n > 1$, alors $n^2 > n$.

***Exercice 1.11* (Définition de l'implication). — ★☆☆**
Étant donné trois énoncés P, Q, R, on forme l'énoncé

$$((P\ \text{ET}\ (Q\ \text{OU}\ R)) \implies (Q\ \text{OU}\ (P\ \text{ET}\ R))\,. \tag{E}$$

Écrire la négation de (E), la contraposée de (E) et la réciproque de (E).

***Exercice 1.12* (Condition nécessaire et condition suffisante). — ★☆☆**

1. Compléter chacun des énoncés suivants avec l'un des symboles $\implies$, $\impliedby$, $\iff$.

   (a) Pour $n \in \mathbb{N}$, $\quad$ (n est multiple de 2) $\quad\ldots\quad$ (n est multiple de 4 ou n est multiple de 6)

   (b) Pour $x \in \mathbb{R}$, $\quad \sqrt{x^2+4x+5} = 1 \quad\ldots\quad x^2+4x+5 = 1$

   (c) Pour $x \in \mathbb{R}$, $\quad \sqrt{x^2+4x+5} = 0 \quad\ldots\quad x^2+4x+5 = 0$

   (d) Pour $x \in \mathbb{R}$, $\quad x-3 = x^2+2x \quad\ldots\quad e^{x-3} = e^{x^2}e^{2x}$

2. Compléter chacun des énoncés suivants avec « il faut », « il suffit », « condition nécessaire », « condition suffisante », ou « condition nécessaire et suffisante ».

   Dans toutes les assertions, x et y sont des nombres réels et n est un entier naturel.

   (a) $x > 2$ est une … pour que $x^2 > 4$

   (b) $x + y = 5$ est une … pour avoir $x = 2$ et $y = 3$

   (c) pour que n soit multiple de 4, il … que n soit le carré d'un entier pair

   (d) pour que $x + y$ soit égal à 5 et xy soit égal à 6, il … que $x = 2$ et $y = 3$.

***Exercice 1.13* (Calcul propositionnel, II). — ★★☆**
Dans tout l'exercice, les symboles A, B, C, désignent des énoncés.

1. Donner une forme équivalente de l'énoncé

$$(A\ \text{OU}\ B\ \text{OU}\ C)\ \text{ET}\ (\text{NON}(A) \implies B)\ \text{ET}\ (\text{NON}(C) \implies B)\,.$$

2. Montrer que les énoncés suivants sont toujours vrais :

   (a) $(A\ \text{OU}\ B) \iff ((A \implies B) \implies B)$

   (b) $(A \implies B) \implies [(A\ \text{ET}\ C) \implies (B\ \text{ET}\ C)]$

Quantificateurs. —

***Exercice 1.14* (Lecture d'énoncés).** — ★☆☆
On considère les ensembles $A = \{1, 2, 3\}$, $B = \{1, 2, 3, 4, 5\}$, $C = \{2, 4\}$ et $D = \mathbb{N}$.
Parmi les énoncés ci-dessous, déterminer ceux qui sont vrais et ceux qui sont faux.

(a) $\forall x \in A,\ x \in B.$
(b) $\exists x \in B,\ x \in A.$
(c) $\exists x \in A,\ x \notin B$
(d) $\exists x \in B,\ x \notin A$
(e) $\forall x \in C,\ \exists y \in B,\ x \leq y.$
(f) $\forall x \in A,\ \exists y \in B,\ x \leq y.$
(g) $\exists x \in C,\ \forall y \in A,\ y \leq x.$
(h) $\exists x \in B,\ \forall y \in A,\ \forall z \in C,\ \ y + z \leq 2x.$
(i) $\exists x \in B,\ \forall y \in B,\ x \leq y.$
(j) $\exists x \in D,\ \forall y \in D,\ x \leq y$
(k) $\exists x \in D,\ \forall y \in D,\ x \geq y.$
(l) $\forall x \in D,\ \exists y \in A,\ x = y.$
(m) $\exists x \in D,\ \exists y \in A,\ x = y.$
(n) $\exists x \in D,\ \forall y \in A,\ x = y.$

***Exercice 1.15* (Traduction langage courant / quantificateurs).** — ★☆☆
Dans cet exercice, on fixe une fonction $f : \mathbb{R} \to \mathbb{R}$.

1. Pour chacune des phrases ci-dessous, écrire une assertion utilisant les quantificateurs et ayant la même signification logique.
   (a) La fonction f ne s'annule pas.
   (b) La fonction f n'est pas nulle.
   (c) La fonction f est strictement croissante.
   (d) Le graphe de f coupe l'axe des abscisses exactement une fois.
   (e) Le graphe de f contient au moins deux points dont l'ordonnée est comprise entre 0 et 3.
2. Pour chaque énoncé ci-dessous, écrire une phrase en français courant (sans quantificateurs) ayant la même signification logique.
   (a) $\exists y \in \mathbb{R}, \forall x \in \mathbb{R} : f(x) = y.$
   (b) $\forall y \in \mathbb{R}, \exists x \in \mathbb{R} : f(x) = y.$
   (c) $\exists x \in \mathbb{R}, \forall x' \in \mathbb{R},\ \ f(x) \leq f(x').$

***Exercice 1.16* (Traduction d'énoncés avec des quantificateurs).** — ★☆☆
À l'université du Portique, il n'y a que deux étudiant·e·s : Camille et Claude. Il y a trois matières : Latin, Grec et Rhétorique. À la fin de l'année, leurs notes (sur 20) sont les suivantes.

	Latin	Grec	Rhétorique
Camille	12	5	16
Claude	14	15	7

Considérons les ensembles $E = \{\text{Camille, Claude}\}$ et $F = \{\text{Latin, Grec, Rhétorique}\}$. Pour tout x dans E et tout y dans F, on considère l'énoncé

$P(x, y)$: « l'étudiant·e x a obtenu une note supérieure ou égale à 10 dans la matière y ».

Pour chacun des énoncés suivants :

- donner une traduction en français courant ;
- dire si l'énoncé est vrai ou faux.

(a) : $\forall x \in E, \forall y \in F,\ P(x, y)$ (b) : $\exists x \in E, \exists y \in F,\ \text{NON}(P(x, y))$ (c) : $\exists x \in E, \forall y \in F,\ P(x, y)$
(d) : $\forall x \in E, \exists y \in F,\ P(x, y)$ (e) : $\exists y \in F, \forall x \in E,\ \text{NON}(P(x, y))$ (f) : $\exists y \in F, \forall x \in E,\ P(x, y)$

***Exercice 1.17* (Variables muettes).** — ★☆☆
Pour chacune des expressions ci-dessous,

- Dire s'il s'agit ou non d'une assertion,
- Dire quelles sont les variables et parmi elles, dire lesquelles sont muettes,

- Écrire une expression synonyme où les variables muettes ont disparu.

(a) L'équation $2x + 3 = c$, d'inconnue réelle x, admet au moins une solution positive.

(b) L'ensemble des réels x vérifiant $\sin(x) = 0$.

(c) $\int_0^1 e^{at} dt$

(d) $\lim\limits_{x \to +\infty} \frac{x^n}{x^m} \neq 0$

(e) $\lim\limits_{n \to \infty} u_n > 0$

(f) L'ensemble des solutions de l'équation $x^2 + y^2 = 0$ d'inconnues réelles x et y.

(g) $\sum\limits_{k=1}^{n} k$

(h) Pour tout $x \in \mathbb{R}$, on a $mx^2 + 4x + 4 > 0$.

***Exercice 1.18* (Quantificateurs imbriqués et négation, I). — ★☆☆**

1. Écrire la négation de chacun des énoncés suivants :
   (a) $\exists x \in \mathbb{R} \ : \ \forall n \in \mathbb{N}, \ x > 2n$
   (b) $\forall n \in \mathbb{N}, \ \exists x \in \mathbb{R} \ : \ x > 2n$
   (c) Pour tout réel x, pour tout réel y, si $x \geq y$ alors $x^2 \geq y^2$.

2. Pour chacun des énoncés précédents, dire s'il est vrai ou s'il est faux, et justifier soigneusement.
   On pourra utiliser sans justification le fait suivant : si x est un nombre réel, alors il existe un entier $n \in \mathbb{N}$ vérifiant $n > x$.

***Exercice 1.19* (Quantificateurs imbriqués et négation, II). — ★★☆**

1. Considérons l'énoncé suivant :
$$\exists x \in \mathbb{R} \ / \ \forall y \in \mathbb{R}, \ x^2 + 2xy = 1. \tag{P}$$
   (a) Écrire la négation de (P).
   (b) L'énoncé (P) est-il vrai ?

2. L'énoncé ci-dessous est-il vrai ou faux ?
$$\forall x \in \mathbb{N}, \exists y \in \mathbb{N} \ : \ \exists z \in \mathbb{N} \ : \ (x \leq y \quad \text{et} \quad y = 2z) \tag{Q}$$
   On justifiera complètement la réponse.

CHAPITRE 2

NOTIONS ENSEMBLISTES

1. Ensembles

1.1. Premières notions et remarque sur leur rôle. —
En mathématiques, on appelle *ensemble* toute collection d'objets. Les objets présents dans la collection s'appellent les *éléments de l'ensemble*.

La notion de « collection d'objets » est généralement considérée comme *primitive* dans notre discipline : on ne cherchera pas à la définir. Au contraire, on prendra comme point de départ l'idée que, si l'on dispose d'objets, on peut former avec eux une « collection » : l'ensemble dont les éléments sont les objets donnés.

Voici quelques éléments de vocabulaire sur les ensembles :

- *Appartenance.* Si E est un ensemble et si x est un objet, l'affirmation « x est un élément de E » s'écrit « $x \in E$ » (on dit aussi que x *appartient* à E). L'affirmation « x n'est pas un élément de E » s'écrit « $x \notin E$ ».
- *Ensemble vide.* L'ensemble n'ayant aucun élément est appelé *l'ensemble vide*, on le note $\emptyset$.
- *Égalité de deux ensembles.* Deux ensembles A et B sont *égaux* lorsqu'ils ont les mêmes éléments.

Remarque 2.1. — À partir d'un ensemble, on peut généralement former d'autres ensembles : par exemple, en partant de l'ensemble E et en supposant donné, pour chaque élément x de E, un énoncé $\mathcal{P}(x)$, on peut former l'ensemble A des éléments de E vérifiant l'assertion $\mathcal{P}(x)$. Ainsi, si $E = \mathbb{R}$ et si pour $x \in \mathbb{R}$, on note $\mathcal{P}(x)$ l'affirmation « il existe un réel a tel que $x = a^2$ », alors on peut former l'ensemble $A = \{x \in \mathbb{R} \ / \ \mathcal{P}(x) \text{ est vérifiée}\}$; on obtient ainsi l'ensemble $\mathbb{R}^+$ des réels positifs.

Remarque 2.2. — Si E est vide, alors toute affirmation du type « $\forall x \in E, \dots$ » est *vraie*. Par exemple, l'affirmation suivante est vraie :

$$\text{Pour tout réel } x \text{ vérifiant } x^2 + 3 < 1, \text{ on a } x^2 + 5x - 4 = 0.$$

Remarque 2.3. — En « jouant » avec les ensembles et les règles de la logique, on peut former des ensembles « de plus en plus compliqués ». Dans les discussions des fondements des mathématiques, une idée a joué un grand rôle depuis la fin du XIX$^{\text{ème}}$ Siècle : c'est l'idée selon laquelle *les objets mathématiques courants sont « tous » des ensembles et doivent pouvoir être définis à partir d'ensembles plus simples et des règles de la logique.* Par exemple, une définition rigoureuse de la notion de « fonction » peut être donnée à partir uniquement de la notion d'ensemble (voir la définition 2.45 ci-dessous).

Remarque historique. — Suite à plusieurs crises dans les fondements des mathématiques au cours du XIX$^{\text{è}}$ Siècle, la question s'est posée au début du XX$^{\text{è}}$ Siècle de savoir jusqu'à quel point on pouvait pousser la logique de la remarque ci-dessus jusqu'au bout − autrement dit, reconstruire *tous les objets mathématiques connus*, et démontrer toutes leurs propriétés, à partir des seules règles de la logique vues au chapitre précédent et d'un très petit nombre d'ensembles « primitifs » (l'ensemble vide, etc).

1.2. Les ensembles $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$. — Vous avez souvent manipulé, au lycée, des ensembles de « nombres », parmi lesquels les suivants.

- L'ensemble $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ des *entiers naturels*.

  Certaines des propriétés de $\mathbb{N}$ traduisent des idées plongeant au plus profond de notre conception de ce que veut dire « compter » ; c'est pourquoi certaines propriétés de $\mathbb{N}$ sont des *axiomes*, acceptés comme point de départ des mathématiques par toutes celles et tous ceux qui en font. La propriété (1.11) du chapitre 1 est reliée à ces axiomes. Nous en croiserons quelques autres dans ce cours.

  On note généralement $\mathbb{N}^\star = \{1, 2, 3, \ldots\}$ l'ensemble des *entiers naturels non nuls*.
- L'ensemble $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ des *entiers relatifs*.

  Cet ensemble est généralement *construit* à partir de $\mathbb{N}$, en « ajoutant », pour chaque entier strictement positif $n \in \mathbb{N}^\star$, un « opposé » $(-n)$, puis en définissant l'addition et la multiplication de $\mathbb{Z}$ par les règles que vous connaissez bien (« moins par moins donne plus », etc). Les détails de la construction se trouvent, par exemple, dans l'ouvrage [2].

  Comme pour le cas des entiers naturels, on note $\mathbb{Z}^\star = \{\ldots, -2, -1, 1, 2, \ldots\}$ l'ensemble des *entiers relatifs non nuls*.
- L'ensemble $\mathbb{Q}$ des nombres rationnels est à son tour *construit* à partir de $\mathbb{Z}$, en créant, dès que p et q sont deux entiers relatifs avec $q \neq 0$, un nouvel objet, la « fraction » $\frac{p}{q} \in \mathbb{Q}$, puis en « décidant » que $\frac{p'}{q'} = \frac{p}{q}$ si et seulement si $p' \times q = p \times q'$. On note alors $\mathbb{Q}$ l'ensemble des « fractions ».
- L'ensemble $\mathbb{R}$ des *nombres réels* est lui aussi construit à partir de $\mathbb{Q}$. Mais c'est plus difficile. Quelques éléments à ce sujet vous seront présentées dans le cours « Analyse 1 ».

Ainsi, les ensembles de nombres usuels, puis beaucoup d'autres ensembles qui leur sont reliés (ensembles de suites, de fonctions...) sont tous *construits*, d'une façon généralement assez délicate, à partir de l'ensemble $\mathbb{N}$. Ce dernier est donc le point de départ de la majorité des constructions mathématiques.

1.3. Diverses manières de définir un ensemble : en extension, en compréhension... —

Définition en extension. — Pour décrire un ensemble, on peut donner la *liste de ses éléments* :

$$A = \{1, -8, \pi\}$$

est un ensemble comportant trois éléments.

Dans une telle description, l'ordre d'écriture « ne compte pas » : on a aussi $A = \{-8, \pi, 1\}$.

Définition en compréhension. — On peut aussi décrire un ensemble en spécifiant quelles sont les *propriétés* qui distinguent les objets qui appartiennent à E des objets qui n'y appartiennent pas. Par exemple, si nous définissons

$$B = \left\{ n \in \mathbb{N} \ / \ \exists p \in \mathbb{N} \ : \ n = p^2 \right\}$$

on a $9 \in B$, mais $3 \notin B$.

Nous rencontrerons aussi l'écriture

$$B = \left\{ p^2, \ p \in \mathbb{N} \right\} :$$

elle signifie que B est l'ensemble des objets qui peuvent s'écrire sous la forme p^2 pour un certain $p \in \mathbb{N}$.

Deux écritures à ne pas confondre. —

L'écriture $E = \{x \in A \ / \ \mathcal{P}(x)\}$ signifie « l'ensemble des x de A vérifiant la propriété $\mathcal{P}(x)$ ».

L'écriture $E = \{f(x), \ x \in A\}$ signifie « l'ensemble des objets y de la forme $y = f(x)$ avec $x \in A$ ».

Ces écritures ont des significations différentes, même si on peut souvent passer de l'une à l'autre.

Équivalence de certaines définitions. — Naturellement, un ensemble donné peut admettre plusieurs descriptions différentes : si

$$C = \{n \in \mathbb{N} \ / \ n < 5\},$$

on a bien sûr

$$C = \{0, 1, 2, 3, 4\} :$$

une description est « en extension », l'autre « en compréhension », mais elles définissent le même ensemble.

1.4. Inclusion, ensemble des parties. —

Définition 2.4 – Inclusion entre ensembles, parties d'un ensemble

Soient A et E deux ensembles. On dit que A est *inclus dans* E, ou que A est une *partie de* E, si tous les éléments de A appartiennent à E. Dans ce cas, on note $A \subset E$.

***Exemple 2.5* (Parties triviales).** — Si E est un ensemble,

- On a toujours $E \subset E$: l'ensemble E lui-même est toujours une partie de E.
- De plus, l'ensemble vide $\emptyset$ est toujours une partie de E (en vertu du principe 2.2, tous les éléments de $\emptyset$ appartiennent bien à E).

Remarque 2.6. — Si A, B et C sont trois ensembles et si on a $A \subset B$ et $B \subset C$, alors l'inclusion $A \subset C$ est aussi vérifiée. Par exemple, les ensembles $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont construits à partir de $\mathbb{N}$ de façon à ce que les inclusions suivantes soient vraies : $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

***Exemple 2.7* (Singleton, paire).** — Soit E un ensemble. Si x est un élément de E, alors l'ensemble $\{x\}$ est une partie de E qui comporte un seul élément. Si x et y sont deux éléments distincts de E, l'ensemble $\{x, y\}$ est une partie de E qui comporte exactement deux éléments.

Lorsqu'un ensemble A comporte un seul élément, on dit que A est un *singleton*, et lorsqu'il comporte exactement deux éléments (distincts), on dit que c'est une *paire*.

Remarque 2.8. — Pour vérifier qu'un ensemble A est inclus dans un ensemble B, on peut (on doit !) montrer que tout élément de A est aussi un élément de B. Pour cela, on se livre généralement à l'expérience de pensée suivante : on part d'un objet de A, on lui donne un nom, par exemple en écrivant

$$\textit{Soit } x \textit{ un élément de } A.$$

puis on essaie de montrer que cet objet est nécessairement un élément de B.

Exemple 2.9. — Considérons $A = \{n \in \mathbb{N} \ / \ \exists k \in \mathbb{N} \ : \ n = k(k+1)\}$ et notons B l'ensemble des entiers pairs. Montrons l'inclusion $A \subset B$.

Soit n un élément de A. On peut alors écrire $n = k(k+1)$ avec $k \in \mathbb{N}$. Montrons que n est pair en distinguant deux cas :

- Si k est pair, alors on peut écrire $k = 2q$ avec $q \in \mathbb{N}$, et alors $n = 2q(q+1)$, donc n est pair.
- Si k est impair, alors on peut écrire $k = 2q+1$ avec $q \in \mathbb{N}$, et alors $n = 2k(2q+2) = 2k(q+1)$, donc ici aussi n est pair.

Dans tous les cas on a $n \in B$. Ainsi $A \subset B$.

Axiome 2.10 – Égalité d'ensembles $\iff$ double inclusion

Si A et B sont deux ensembles, alors on a l'équivalence

$$A = B \iff (A \subset B \quad \textit{et} \quad B \subset A)$$

Exemple 2.11. — Considérons par exemple les ensembles $A = \left\{x \in \mathbb{R} \;/\; \sqrt{2x^2+1} = 2x+1\right\}$ et $B = \{0\}$. Montrons que $A = B$ en vérifiant séparément les inclusions $A \subset B$ et $B \subset A$.

- Pour vérifier l'inclusion $B \subset A$, il suffit de constater que pour $x = 0$, on a bien $\sqrt{2x^2+1} = 2x+1$.
- Vérifions à présent l'inclusion $A \subset B$. Soit x un élément de A. On a alors $\sqrt{2x^2+1} = 2x+1$. En élevant au carré, on constate que $2x^2+1 = 4x^2+4x+1$, autrement dit, $2x^2+4x = 0$, ou encore $2x(x+2) = 0$. On a alors $x = 0$ ou $x+2 = 0$, donc $x = 0$ ou $x = -2$.

  Mais pour $x = -2$, on constate que $\sqrt{2x^2+1} = 3$ alors que $2x+1 = -3$: il est donc impossible que -2 appartienne à A.

  On en déduit donc que $x = 0$, et donc $x \in B$.

Définition 2.12 – Ensemble des parties d'un ensemble

Soit E un ensemble. On appelle *ensemble des parties de* E, et on note $\mathcal{P}(E)$, l'ensemble ayant pour éléments les parties de E.
Si A est un ensemble, on a donc : $A \in \mathcal{P}(E) \iff A \subset E$.

Exemple 2.13. — Si $A = \{1,2,3\}$, les parties de A sont

- l'ensemble vide $\emptyset$
- les singletons $\{1\}$, $\{2\}$,$\{3\}$,
- les paires $\{1,2\}$, $\{2,3\}$ et $\{1,3\}$
- l'ensemble $A = \{1,2,3\}$ lui-même.

L'ensemble $\mathcal{P}(A)$ comporte donc 8 élements : on a $\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{2,3\}, \{1,3\}, \{1,2,3\}\}$.

Remarque 2.14. — Les deux exemples ci-dessus montrent que les notions d'*ensemble* et d'*élément* sont relatives : un élément d'un ensemble peut lui-même être un ensemble...

2. Union, intersection, complémentaire

2.1. Union et intersection. —

Définition 2.15 – Intersection et réunion de deux ensembles

Soient A et B deux ensembles.
L'intersection $A \cap B$ est l'ensemble des objets appartenant à la fois à A et à B :

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

La réunion $A \cup B$ est l'ensemble des objets appartenant à au moins l'un des deux ensembles A, B :

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

Exemple 2.16. — Si $A = \{2,5,7\}$ et $B = \{1,5,7,9\}$, on a $A \cup B = \{1,2,5,7,9\}$, et $A \cap B = \{5,7\}$.

Vocabulaire. — Lorsque deux parties A et B vérifient $A \cap B = \emptyset$, on dit que A et B sont *disjointes*.

2.2. Propriétés formelles de la réunion et de l'intersection. —

Nous avons vu au §2.2 que les connecteurs logiques ET et OU vérifient un certain nombre de propriétés formelles très utiles. Les opérations ensemblistes d'union et d'intersection étant définies à partir de ces connecteurs logiques, elles ont elles aussi des propriétés formelles utiles.

Certaines ne sont pas extrêmement instructives : par exemple,

- si A est un ensemble quelconque, on a toujours $A \cap \emptyset = \emptyset$ et $A \cup \emptyset = A$.

- si A et B sont deux ensembles, on a toujours $A \cup B = B \cup A$ et $A \cap B = B \cap A$.

Il en est deux, cependant, qui ont une importance théorique particulière.

La première est la traduction pour les ensembles d'une partie de de la Proposition 1.15 (troisième et quatrième points) :

Proposition 2.17 – Associativité de la réunion et de l'intersection

Soient A, B et C trois ensembles. On a les égalités

$$(A \cup B) \cup C = A \cup (B \cup C) \quad \text{et} \quad (A \cap B) \cap C = A \cap (B \cap C).$$

Une conséquence de ce résultat est que les notations $A \cup B \cup C$ et $A \cap B \cap C$ ne sont porteuses d'aucune ambiguïté (on n'a pas besoin de parenthèses) : la première désigne l'ensemble des objets appartenant à la fois à A, B et à C, tandis que la seconde désigne l'ensemble des objets appartenant à l'un (au moins) des trois ensembles A, B, C.

Exemple 2.18. — Si $A = \{2, 5, 7\}$, $B = \{1, 5, 7, 9\}$ et $C = \{2, 7, 9, 10\}$, alors $A \cup B \cup C = \{1, 2, 5, 7, 9, 10\}$ et $A \cap B \cap C = \{7\}$.

La seconde propriété traduit, elle, les distributivités vues dans les premiers points de la Proposition 1.15 :

Proposition 2.19 – Distributivités entre réunion et intersection

Soient A, B et C trois ensembles. On a les égalités

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C);$$
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

2.3. Complémentaire. —

Définition 2.20 – Différence ensembliste

Soient A et B deux ensembles. La différence ensembliste $A \setminus B$ est l'ensemble des objets appartenant à A, mais pas à B : si x est un objet, alors

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

Exemple 2.21. — Si $A = \{2, 5, 7\}$ et $B = \{1, 5, 7, 9\}$, alors $A \setminus B = \{2\}$ et $B \setminus A = \{1, 9\}$.

Exemple 2.22. — L'ensemble $\mathbb{R} \setminus \mathbb{Q}$ est l'ensemble des nombres réels x qu'il est impossible d'écrire sous la forme $x = \dfrac{p}{q}$ avec p et q entiers (et $q \neq 0$). C'est l'ensemble des nombres *irrationnels*.

Définition 2.23 – Complémentaire d'une partie

Soient E un ensemble et A une partie de E. On appelle *complémentaire de A dans E* l'ensemble $E \setminus A$, c'est-à-dire l'ensemble des éléments de E qui n'appartiennent pas à A.

Notations. — Outre $E \setminus A$, on trouve plusieurs notations pour désigner le complémentaire de A dans E : on le note parfois $C_E(A)$, et lorsqu'il n'y a pas d'ambiguité sur E, on le note parfois A^c ou $\bar{A}$.

Exemple 2.24. — Si $E = \{1, 2, 3, 4, 5\}$ et $A = \{2, 3\}$, alors $C_E(A) = \{1, 4, 5\}$.

Exemple 2.25. — Soit $E = \mathbb{R}$. Soit $A = [0, 1]$. On a

$$C_E(A) = \{x \in \mathbb{R} \ / \ x \notin [0, 1]\} =]-\infty, 0[\cup]1, +\infty[.$$

De plus, si on note $B = C_E(A)$ l'ensemble que nous venons de décrire, alors $C_E(B) = [0, 1] = A$.

2.4. Propriétés formelles du passage au complémentaire. — De même que les propriétés formelles des connecteurs logiques ET et OU se sont traduites au §2.1 par des propriétés formelles des opération de réunion et d'intersection, on peut obtenir des propriétés de l'opération « prendre le complémentaire dans un ensemble E d'une partie A de E » à partir des propriétés du NON logique. Par exemple, on a toujours $C_E(E) = \emptyset$ et $C_E(\emptyset) = E$. De plus, on dispose d'une traduction en termes d'ensembles de l'axiome 1.7 :

Proposition 2.26 – Le complémentaire du complémentaire

Si E est un ensemble et si A est une partie de E, alors $C_E\left[C_E(A)\right] = A$.

Les lois de De Morgan ont aussi une traduction en termes d'ensembles :

Proposition 2.27 – Passer au complémentaire échange réunion et intersection

Soit E un ensemble. Soient A et B deux parties de E. On a les égalités

$$C_E\left(A \cap B\right) = \left[C_E(A) \cup C_E(B)\right];$$
$$C_E\left(A \cup B\right) = \left[C_E(A) \cap C_E(B)\right].$$

Démonstration. — Prouvons la première égalité : si x est un élément de E, alors

$$\begin{aligned} x \in C_E\left(A \cap B\right) &\iff x \notin A \cap B \qquad \text{par définition} \\ &\iff x \notin A \text{ ou } x \notin B \quad \text{d'après les lois de De Morgan} \\ &\iff x \in C_E(A) \text{ ou } x \in C_E(B) \\ &\iff x \in \left[C_E(A) \cup C_E(B)\right]. \end{aligned}$$

Les ensembles $C_E\left(A \cap B\right)$ et $\left[C_E(A) \cup C_E(B)\right]$ ont donc les mêmes éléments : ils sont égaux.

La seconde égalité peut se prouver de la même manière. □

Remarque 2.28. — Les liens entre les expressions utilisées en logique (et, ou, etc.) et les opérations sur les ensembles (intersection, union, etc.) sont étroits... mais il ne faut pas tout mélanger. Les expressions "et","ou", "implique", etc, sont à placer entre des propositions, pas entre des ensembles. Les signes $\cap$, $\cup$, $\subset$, etc, sont à placer entre des ensembles, pas entre des propositions. En d'autres termes, si P et Q sont des propositions, « P et Q » a un sens, mais « $P \cap Q$ » n'en a pas. Si A et B sont des ensembles, « $A \cap B$ » a un sens, mais « A et B » n'en a pas.

3. Produit cartésien d'un nombre fini d'ensembles

3.1. Couples et n-uplets d'objets. — À partir de deux objets, on peut [1] former un nouvel objet, le *couple* (x, y). Si on donne quatre objets x, y, x' et y', alors l'égalité de couples $(x, y) = (x', y')$ signifie qu'on a à la fois $x = x'$ et $y = y'$ (égalité des composantes *position par position*).

- Attention, l'ordre compte : les couples $(3, 5)$ et $(5, 3)$ sont deux objets différents.
- On peut former un couple où figure deux fois le même objet : le couple $(3, 3)$ existe, et c'est un objet différent du nombre 3.
- La notion de couple est différente de la notion ensembliste de *paire* (non ordonnée) vue au §1.4 : les ensembles $\{3, 5\}$ et $\{5, 3\}$ sont identiques, et l'ensemble $\{3, 3\}$ est identique au singleton $\{3\}$.

De même, si n est un entier naturel non nul et si on se donne n objets a_1, a_2, …, a_n, on peut former le *n-uplet* $(a_1, \dots, a_n)$. On parle ainsi de *triplet*, de *quadruplet*, de *quintuplet*...

Là encore, l'ordre compte : on a (Allegro, Adagio, Presto) $\neq$ (Presto, Allegro, Adagio). De plus, dans un n-uplet, il peut y avoir des *répétitions* : c'est le cas dans le quadruplet $(1, 3, 3, 1)$.

3.2. Produit cartésien. —

Définition 2.29 – Produit cartésien d'une famille finie d'ensembles

Cas de deux ensembles.
Soient A et B deux ensembles. Le *produit cartésien* $A \times B$ est l'ensemble des couples dont la première composante est un élément de A et la seconde un élément de B :

$$A \times B = \{(a, b), \quad a \in A, \quad b \in B\}.$$

Cas de n ensembles.
Soit n un entier naturel non nul ; supposons donnés n ensembles A_1, A_2, …, A_n. Le *produit cartésien* $A_1 \times A_2 \times \cdots \times A_n$ est l'ensemble des n-uplets où, pour chaque $i \in \{1, \dots, n\}$, la i-ème composante est un élément de l'ensemble A_i :

$$A_1 \times A_2 \times \dots A_n = \{(a_1, a_2, \cdots, a_n), \quad a_1 \in A_1, a_2 \in A_2, \dots, a_n \in B_n\}.$$

Exemple 2.30. — Si $A = \{1, 2, 3\}$ et $B = \{1, 7\}$, alors

$$A \times B = \{(1, 1), (1, 7), (2, 1), (2, 7), (3, 1), (3, 7)$$

tandis que

$$B \times A = \{(1, 1), (1, 2), (1, 3), (7, 1), (7, 2), (7, 3)\}.$$

On remarquera que $A \times B \neq B \times A$.

Notation A^n. — Si A est un ensemble, on note souvent A^2 pour $A \times A$: par exemple, $(\pi, \sqrt{3})$ est un élément de $\mathbb{R}^2$. De même, pour tout $n \in \mathbb{N}^\star$, on note souvent A^n pour $\underbrace{A \times \cdots \times A}_{n \text{ fois}}$. Un élément de A^n est donc un n-uplet d'éléments de A : par exemple, un élément de $\mathbb{Z}^6$ est un sextuplet $(n_1, n_2, n_3, n_4, n_5, n_6)$ où $n_1, \dots, n_6$ sont six entiers relatifs (pas forcément distincts).

***Exemple 2.31* (Représentation graphique de $\mathbb{R}^2$).** — Si $E = \mathbb{R}^2$, alors les éléments de E sont des couples de nombres réels. On peut les représenter sur un plan, en utilisant les *coordonnées cartésiennes* : l'élément (x, y) de $\mathbb{R}^2$ est alors représenté comme le point d'abscisse x et d'ordonnée y. Dans $\mathbb{R}^2$, on peut utiliser les coordonnées cartésiennes pour dessiner non seulement des points, mais aussi des *parties* de $\mathbb{R}^2$.

1. Cette possibilité fait partie des axiomes universellement utilisés.

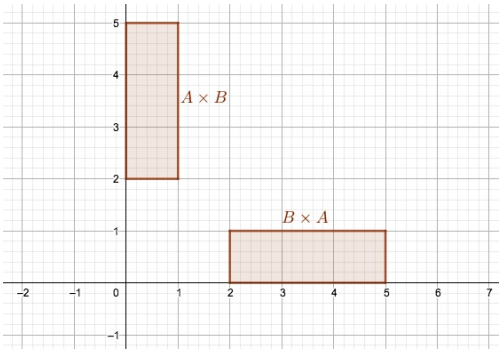


FIGURE 1. Si $A = [0, 1]$ et $B = [2, 5]$, alors $A \times B$ et $B \times A$ ne sont pas identiques. En utilisant les coordonnées cartésiennes pour représenter dans le plan $A \times B$ et $B \times A$, les deux figures obtenues sont des rectangles.

Remarque sur la terminologie. — Dans « produit cartésien » comme dans « coordonnées cartésiennes », l'adjectif « cartésien » est une référence à Descartes : c'est son travail qui montra la fécondité de l'idée de représenter un point du plan par un couple (x, y) de nombres réels.

4. Familles d'objets ou d'ensembles indexées par un ensemble quelconque

4.1. Notion de famille indexée par un ensemble I ; produit cartésien. — Soit I un ensemble non vide quelconque. Supposons donné, pour chaque $i \in I$, un objet mathématique a_i. On peut alors former un nouvel objet mathématique, la *famille* $(a_i)_{i\in I}$: il s'agit de la « liste des a_i ».

Attention. — Dans la notation $(a_i)_{i\in I}$, la variable i est muette : la notation $(a_\lambda)_{\lambda\in I}$ désigne le même objet mathématique que la notation $(a_i)_{i\in I}$.

Exemple 2.32 **(Une famille de fonctions).** — Fixons $I =]0, +\infty[$.

Pour chaque valeur de $\lambda \in I$, on peut définir une fonction

$$\begin{aligned} f_\lambda : \mathbb{R} &\to \mathbb{R} \\ x &\mapsto \sin\left(\frac{x}{\sqrt{\lambda}}\right). \end{aligned}$$

Grâce à ce qui précède on dispose, par exemple, d'une fonction f_3 (c'est la fonction $x \mapsto \sin\left(\frac{x}{\sqrt{3}}\right)$), d'une fonction $f_{\ln(2)}$, d'une fonction $f_{\frac{1}{\pi^2}}$...

La famille $(f_\lambda)_{\lambda\in\mathbb{R}}$ est alors une famille de fonctions. Il y a une infinité de fonctions dans la famille : une pour chaque valeur de λ.

Exemple 2.33 **(Lien avec les suites).** — Fixons $I = \mathbb{N}$.

Pour tout $i \in \mathbb{N}$, on peut définir un nombre u_n en posant $u_n = (n-2)(n-7)$.

On dispose donc d'un nombre $u_0 = 14$, d'un nombre $u_1 = 6$, d'un nombre $u_2 = 0$, d'un nombre $u_3 = -4$, etc : par exemple $u_{3000} = 2098 \times 2093$.

La famille $(u_n)_{n\in\mathbb{N}}$ est une « liste infinie » de nombres.

Cet exemple montre que la notion de *famille de nombres indexée par* $I = \mathbb{N}$ vous est déjà connue : une telle famille est une *suite*.

Définition 2.34 – Produit cartésien d'une famille (éventuellement infinie) d'ensembles

Soit I un ensemble non vide quelconque. On suppose donné, pour chaque i de I, un ensemble A_i.
Le *produit cartésien* $\prod_{i\in I} A_i$ est l'ensemble dont les éléments sont les familles $(a_i)_{i\in I}$
où, pour chaque $i \in I$, l'objet a_i appartient à A_i.

Exemple 2.35. — Considérons $I = \mathbb{N}$ et pour tout $i \in I$, notons $A_i = [-i, i]$.

Le produit cartésien $E = \prod_{i\in I} A_i$ est l'ensemble des familles $(u_i)_{i\in I}$ où, pour tout $i \in \mathbb{N}$, on a $u_i \in [-i, i]$.

Un élément de E est donc une suite $(u_n)_{n\in\mathbb{N}}$, mais une suite dont le premier terme u_0 est nécessairement égal à zéro, dont le terme suivant u_1 est contraint à appartenir à $[-1, 1]$, etc.

Remarque 2.36. — Comme pour la notation $(a_i)_{i\in I}$, dans la notation $\prod_{i\in I} A_i$, l'indice i est muet : la notation $\prod_{k\in I} A_k$ désigne aussi le produit cartésien.

Notation A^I. — Si I est un ensemble non vide quelconque et si A est un ensemble, on note souvent A^I plutôt que $\prod_{i\in I} A$. L'ensemble A^I est donc l'ensemble des familles indexées par I d'éléments de A : les éléments de A^I sont les familles $(a_i)_{i\in I}$ où, pour chaque indice $i \in I$, l'objet a_i est un élément de A.

Les exemples 2.33 et 2.35 montrent l'utilité de cette notion en pratique : l'ensemble $\mathbb{R}^{\mathbb{N}}$ est l'ensemble des familles indexées par $\mathbb{N}$ de nombres réels, autrement dit l'ensemble des *suites réelles*.

Remarque 2.37. — Si on fixe $n \in \mathbb{N}^\star$ et si I est l'ensemble fini $\{1, \dots, n\}$, alors la notation $\prod_{i\in I} A_i$ désigne simplement $A_1 \times A_2 \cdots \times A_n$. On trouve aussi les notations $\prod_{i=1}^{n} A_i$ et $\prod_{1\leq i\leq n} A_i$ pour désigner cet ensemble.

4.2. Union ou intersection indexée par un ensemble I. —

Définition 2.38 – Union et intersection indexées par un ensemble quelconque

Soit I un ensemble non vide quelconque. On suppose donné, pour chaque i de I, un ensemble A_i.
La *réunion* $\bigcup_{i\in I} A_i$ est l'ensemble des objets x vérifiant : $\exists i \in I \ / \ x \in A_i$.
L'*intersection* $\bigcap_{i\in I} A_i$ est l'ensemble des objets x vérifiant : $\forall i \in I,\ x \in A_i$.

Exemple 2.39. — Supposons $I = \mathbb{N}$ et pour tout $i \in \mathbb{N}$, notons $A_i = \{-i, i\}$. On a alors $\bigcup_{i\in I} A_i = \mathbb{N}$, tandis que $\bigcap_{i\in I} A_i = \emptyset$.

Remarque 2.40. — À nouveau, dans la notation $\bigcup_{i\in I} A_i$ et $\bigcap_{i\in I} A_i$, la variable i est muette : les notations $\bigcup_{i\in I} A_i$, $\bigcup_{k\in I} A_k$ et $\bigcup_{\Theta\in I} A_\Theta$ désignent le même ensemble.

Remarque 2.41. — Si on fixe $n \in \mathbb{N}^\star$ et si I est l'ensemble fini $\{1, \dots, n\}$, alors la notation $\bigcup_{i\in I} A_i$ désigne simplement $A_1 \cup A_2 \cup \cdots \cup A_n$, qu'on note aussi parfois $\bigcup_{i=1}^{n} A_i$ ou $\bigcup_{1\leq i\leq n} A_i$.

Lemme 2.42 – Propriétés formelles de l'union et de l'intersection

Soit I un ensemble non vide quelconque.

- Distributivité de l'union et de l'intersection.
  Si A est un ensemble et si $(B_i)_{i\in I}$ est une famille d'ensembles indexée par I, alors
$$A \cup \left(\bigcap_{i\in I} B_i\right) = \bigcap_{i\in I}(A \cup B_i) \quad \text{et} \quad A \cap \left(\bigcup_{i\in I} B_i\right) = \bigcup_{i\in I}(A \cap B_i)$$
- Propriétés du passage au complémentaire.
  Si E est un ensemble et si $(A_i)_{i\in I}$ est une famille indexée par I de parties de E, alors
$$C_E\left(\bigcup_{i\in I} A_i\right) = \bigcap_{i\in I} C_E(A_i) \quad \text{et} \quad C_E\left(\bigcap_{i\in I} A_i\right) = \bigcup_{i\in I} C_E(A_i)$$

5. Applications : premières définitions et manipulations

5.1. Notion d'application d'un ensemble vers un autre ensemble. — Vous connaissez la notion de *fonction numérique*

$$\begin{array}{rccc} f & : & \mathbb{R} & \to & \mathbb{R} \\ & & x & \mapsto & f(x) \end{array}$$

qui permet d'associer, à chaque nombre réel x, un (unique) nombre réel $f(x)$. Le cas le plus simple est celui où on donne une *formule* permettant de *calculer* $f(x)$ pour x donné, comme lorsqu'on définit

$$\begin{array}{rccc} f & : & \mathbb{R} & \to & \mathbb{R} \\ & & x & \mapsto & \ln(x^2+3) - 5x + \exp(x^4). \end{array}$$

Mais il est aussi possible de définir des fonctions de façon *beaucoup plus abstraite* : par exemple, en définissant

$$\begin{array}{rccc} f & : & \mathbb{R} & \to & \mathbb{R} \\ & & x & \mapsto & \text{le plus petit entier naturel } n \text{ vérifiant } n^3 - 8n - 97 > \dfrac{x}{2\pi}, \end{array}$$

on obtient une fonction parfaitement légitime, mais on ne peut pas vraiment *calculer* facilement $f(51)$...

On peut donc définir une notion « d'application » qui ne fait pas nécessairement intervenir de « règle de calcul ».

Définition 2.43 – Application : définition informelle

Soient E et F deux ensembles. Une *application f de E dans F* est une manière d'associer, à chaque élément x de E, un unique élément $f(x)$ de F.

Dans ce cours, on notera $\mathcal{F}(E,F)$ l'ensemble de toutes les applications de E dans F.

Attention. — Lorsqu'on s'intéresse à une application f, *l'ensemble de départ et l'ensemble d'arrivée de f font partie de la définition.* Ainsi,

$$\begin{array}{rccc} f_1 & : & \mathbb{R}^+ & \to & \mathbb{R} \\ & & x & \mapsto & x^2 \end{array}$$

$$\begin{array}{rccc} f_2 & : & \mathbb{R} & \to & \mathbb{R}^+ \\ & & x & \mapsto & x^2 \end{array}$$

sont deux applications *différentes* (par exemple, f_1 est croissante, mais f_2 ne l'est pas).

Notion de graphe. — Si f est une application de $\mathbb{R}$ (ou d'une partie de $\mathbb{R}$) dans $\mathbb{R}$, alors on peut tracer son *graphe* : c'est une partie de $\mathbb{R}^2$, et le point (x, y) de $\mathbb{R}^2$ est situé « sur » le graphe Γ si et seulement si on a $y = f(x)$.

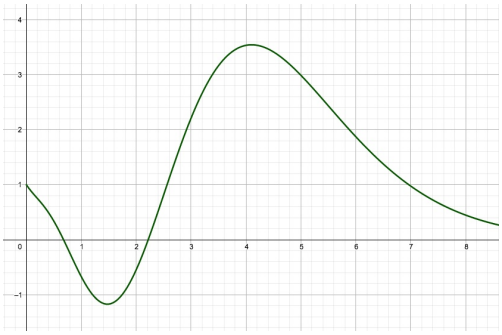


FIGURE 2. Ici $f : \mathbb{R}^+ \to \mathbb{R}$ est l'application $x \mapsto e^{-1.5x}(3x^5 - 6x^4 - 2x^3 + x^2 + 1)$.

Plus généralement, si E et F sont deux ensembles quelconques et si $f : E \to F$ est une application, l'ensemble

$$\Gamma = \{(x, y) \in E \times F \quad / \quad y = f(x)\}$$

est appelé le *graphe de* f. On remarquera que si on connaît le graphe Γ, alors on connaît « complètement » l'application f :

- si x est un élément de E, alors le point $(x, f(x))$ appartient à Γ,
- si on fixe $x \in E$ et si l'on observe tous les points de $E \times F$ de la forme (x, u) avec $u \in F$ (les « points d'abscisse x »), alors il y en a un et un seul qui appartient à Γ : c'est celui pour lequel $u = f(x)$. La donnée de Γ permet donc de déterminer $f(x)$ pour chaque x de E.

Exemple 2.44 **(Application identité).** — Si E est un ensemble quelconque, on peut définir une application id_E comme suit :

$$\begin{array}{rccc} \mathrm{id}_E & : & E & \to & E \\ & & x & \mapsto & x \end{array}$$

(pour tout x de E, on a $\mathrm{id}_E(x) = x$).

Son graphe est une partie de $E \times E$: il s'agit de l'ensemble $\Delta = \{(x, y) \in E \times E \ / \ y = x\}$.

5.2. Complément : définition formelle. — La notion d'application est d'une telle importance en mathématiques qu'il est souhaitable de ne pas se contenter d'une définition informelle. Nous donnons ici une telle définition. Nous n'en ferons pas grand usage : elle n'est là que pour signaler qu'il est possible de définir rigoureusement *tout* ce qui concerne les applications à partir des notions ensemblistes vues dans les chapitres 1 et 2.

Définition 2.45 – Application : définition formelle à l'aide du graphe

Une *application* est un triplet $f = (E, F, G)$ où

- E est un ensemble, l'*ensemble de départ de* f,
- F est un ensemble, l'*ensemble d'arrivée de* f,
- G est une partie du produit cartésien $E \times F$ ayant la propriété suivante :

$$\forall x \in E, \quad \exists! y \in F \quad : \quad (x, y) \in G.$$

On dit que G est le *graphe de* f.

Exemple 2.46. — Si E est un ensemble quelconque et Δ est la diagonale de $E \times E$ (mentionnée à l'exemple 2.44), alors l'application correspondant au triplet (E, E, Δ) est l'application id_E de l'exemple 2.44.

5.3. Composée de deux applications. —

Définition 2.47 – Composée de deux applications

Soient E, F, F', G quatre ensembles et $f : E \to F$ et $g : F' \to G$ deux applications. Supposons que l'ensemble d'arrivée F de f soit inclus dans l'ensemble de départ F' de g. La *composée de f et g*, notée $g \circ f$, est alors l'application de E dans G définie par

$$\begin{array}{rccc} g \circ f & : & E & \to & G \\ & & x & \mapsto & g(f(x)). \end{array}$$

Exemple 2.48. — Si
- $f : \mathbb{R} \to \mathbb{R}$ est l'application définie par : $\forall x \in \mathbb{R},\ f(x) = x^2$,
- $g : \mathbb{R} \to \mathbb{R}$ est l'application définie par : $\forall x \in \mathbb{R},\ g(x) = \sin(x)$,

alors $g \circ f$ et $f \circ g$ sont des applications de $\mathbb{R}$ dans $\mathbb{R}$, et pour tout $x \in \mathbb{R}$, on a

$$(f \circ g)(x) = (\sin(x))^2 \quad \text{et} \quad (g \circ f)(x) = \sin(x^2).$$

Attention. — La notation $g \circ f$ se lit « de droite à gauche » : elle désigne l'application dans laquelle on effectue *d'abord f, puis g*.

Exemple 2.49. — Considérons les applications

$$\begin{array}{rccc} f & : & \mathbb{R} & \to & \mathbb{R} \\ & & x & \mapsto & x^2 - 3x + 1 \end{array} \quad \text{et} \quad \begin{array}{rccc} g & : & \mathbb{R}_\star^+ & \to & \mathbb{R} \\ & & x & \mapsto & \ln(x). \end{array}$$

- La composée $f \circ g$ est bien définie : c'est une application de $\mathbb{R}_\star^+$ dans $\mathbb{R}$, et pour $x \in \mathbb{R}$, on a
$$(g \circ f)(x) = \ln(x)^2 - 3\ln(x) + 1.$$
- La composée $g \circ f$ n'est pas bien définie : il existe des éléments x de l'espace de départ de f pour lesquels il est impossible de définir $g(f(x))$: c'est le cas, par exemple, de $x = 1$.

Les applications $g \circ f$ et $f \circ g$ peuvent être très différentes, voire ne pas exister toutes les deux.

Voici un dernier exemple plus théorique :

Exemple 2.50. — Si $f : E \to F$ est une application, alors on a

$$\mathrm{id}_F \circ f = f \quad \text{et} \quad f \circ \mathrm{id}_E = f.$$

Évoquons enfin une propriété formelle d'usage très fréquent :

Proposition 2.51 – Associativité de la composition

Soient E, F, G, H quatre ensembles et $f : E \to F$, $g : F \to G$ et $h : G \to H$ trois applications. On a l'égalité

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

Démonstration. — Les applications $h \circ (g \circ f)$ et $(h \circ g) \circ f$ ont même ensemble de départ (à savoir E) et même ensemble d'arrivée (à savoir H) ; de plus, pour tout x de E, on constate que $[h \circ (g \circ f)](x)$ et $[(h \circ g) \circ f](x)$ sont tous les deux égaux à $h(g(f(x)))$. Cela prouve l'égalité des deux applications. □

5.4. Image directe d'une partie de l'ensemble de départ. — Dans ce paragraphe, on fixe deux ensembles E et F et une application $f : E \to F$.

Définition 2.52 – Élement atteint de l'espace d'arrivée ; antécédent d'un élément atteint

Soit y un élément de F. On dit que y est atteint par f lorsqu'il existe un élément x de E vérifiant $y = f(x)$. Un tel x est appelé un *antécédent* de y par f.

Exemple 2.53. — Considérons l'application

$$\begin{array}{rccc} f & : & \mathbb{R} & \to & \mathbb{R} \\ & & x & \mapsto & x^2. \end{array}$$

- L'élément $y = -1$ de l'ensemble d'arrivée $\mathbb{R}$ n'est pas atteint par f.
- L'élément $y = 0$ de $\mathbb{R}$ est atteint par f : le nombre $x = 0$ en est un antécédent, et c'est le seul antécédent de $y = 0$ par f.
- L'élément $y = 3$ est aussi atteint par f : il a exactement deux antécédents par f, les nombres $\sqrt{3}$ et $-\sqrt{3}$.

Remarque 2.54. — Si y est un élément atteint par f, il est tout à fait possible que y admette *plusieurs* antécédents distincts. Dans l'exemple précédent, c'est le cas pour $y = 3$.

Lecture graphique des antécédents. — Dans le cas des applications de $\mathbb{R}$ (ou d'une partie de $\mathbb{R}$) dans $\mathbb{R}$ (ou une partie de $\mathbb{R}$), tracer le graphe de f permet souvent de se faire une idée rapide des éventuels antécédents d'un réel donné :

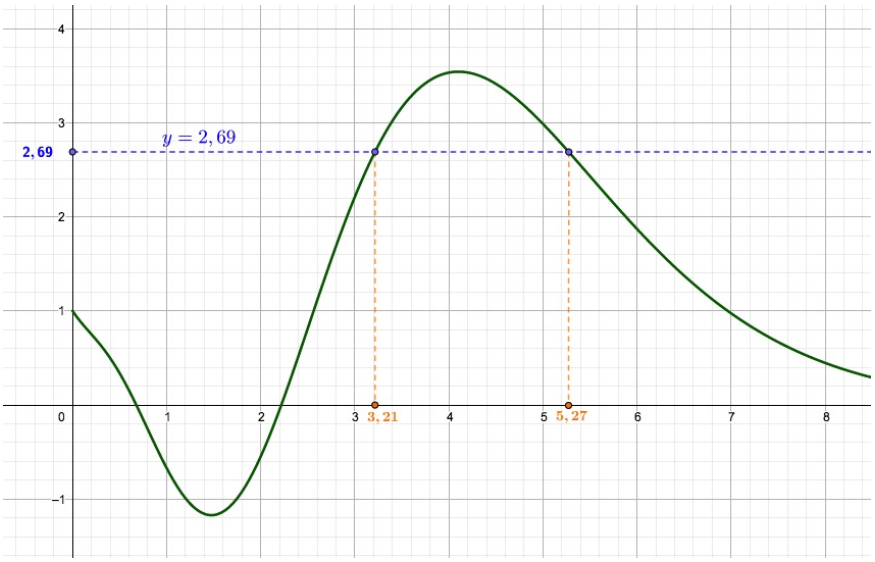


FIGURE 3. Ici f est la fonction considérée à la figure 2. Le nombre $2,69$ admet exactement deux antécédents par f : il s'agit des nombres $3,21$ et $5,27$. Le nombre 4 n'est pas atteint par f.

Définition 2.55 – Image directe d'une partie de l'ensemble de départ

Soit A une partie de E. On appelle *ensemble image de A par f*, et on note $f(A)$, la partie de F suivante :

$$f(A) = \{y \in F \ / \ \exists x \in A,\ y = f(x)\}.$$

Il s'agit de l'ensemble des éléments de F qui peuvent être obtenus comme image d'un élément de A.

Exemple 2.56. — Considérons à nouveau l'application

$$\begin{array}{rccc} f & : & \mathbb{R} & \to & \mathbb{R} \\ & & x & \mapsto & x^2. \end{array}$$

- Si $A = [2, 3]$, alors $f(A) = [4, 9]$.
- Si $A = [-4, 1]$, alors $f(A) = [0, 16]$.
- Si $A = \mathbb{R}$, alors $f(A) = \mathbb{R}^+$.

***Remarque 2.57* (Des deux usages du symbole $f(\cdots)$).** — Ne pas confondre les deux notations suivantes :

- l'image $f(x)$ d'un *élément* x de E : c'est un *élément* de l'espace d'arrivée F.
- l'image $f(A)$ d'une *partie* A de E : c'est une *partie* (un *sous-ensemble*) de l'espace d'arrivée F.

Ces deux objets n'ont pas du tout la même nature ! Il y a des liens, bien sûr : si x est un élément de E, le singleton $A = \{x\}$ est une partie de E, et l'ensemble $f(A)$ n'est autre que le singleton $\{f(x)\}$.

5.5. Image réciproque d'une partie de l'ensemble d'arrivée. — Dans ce paragraphe, on fixe à nouveau deux ensembles E et F et une application $f : E \to F$.

Définition 2.58 – Image réciproque d'une partie de l'ensemble d'arrivée

Soit B une partie de l'ensemble d'arrivée F. On appelle *image réciproque de B par f*, et on note $f^{-1}(B)$, la partie de l'ensemble de départ E suivante :

$$f(B) = \{x \in E \ / \ f(x) \in B\}.$$

Il s'agit de l'ensemble des éléments de E dont l'image par f appartient à B.

Exemple 2.59. — Considérons à nouveau l'application

$$\begin{array}{rccc} f & : & \mathbb{R} & \to & \mathbb{R} \\ & & x & \mapsto & x^2. \end{array}$$

- Si $B = [2, 3]$, alors $f^{-1}(B) = [-\sqrt{3}, -\sqrt{2}] \cup [\sqrt{2}, \sqrt{3}]$.
- Si $B = [-1, 9]$, alors $f^{-1}(B) = [-3, 3]$. Si $B' = [0, 9]$, on a en fait $f^{-1}(B') = f^{-1}(B)$.
- Si $B = [-2, -3]$, alors $f^{-1}(B)$ est vide.

Remarque 2.60. — Si y est un élément de l'ensemble d'arrivée f, alors dire que y est atteint par f revient à dire que l'ensemble $f^{-1}(\{y\})$ n'est pas vide. Dans ce cas, les antécédents de y par f sont exactement les éléments de l'ensemble $f^{-1}(\{y\})$.

Exercices du chapitre 2

Appartenance, égalité, inclusion. —

***Exercice 2.1* (Différence entre x et $\{x\}$, ainsi qu'entre $\in$ et $\subset$). — ★☆☆**
On considère l'ensemble

$$E = \{1, 2, \{3\}, 4, \{5, 6\}, \{7\}, 8, 9, 10\}.$$

Dans le tableau suivant, rayer les affirmations fausses.

$2 \in E$	$2 \subset E$	$\{2\} \in E$	$\{2\} \subset E$
$\{2, 4\} \in E$	$\{2, 4\} \subset E$	$\{5, 6\} \in E$	$\{5, 6\} \subset E$
$\{7, 8\} \in E$	$\{7, 8\} \subset E$	$\{9, 10\} \in E$	$\{9, 10\} \subset E$

***Exercice 2.2* (Pour manier égalité et inclusions). — ★☆☆**
Si a est un entier naturel, on note $a\mathbb{N}$ l'ensemble $\{ka,\ k \in \mathbb{N}\}$.

1. On fixe deux entiers naturels non nuls a et b. Montrer l'équivalence suivante :

$$a\mathbb{N} \subset b\mathbb{N} \iff a \in b\mathbb{N}.$$

2. On fixe deux entiers naturels non nuls a et b. Montrer l'équivalence suivante :

$$a\mathbb{N} = b\mathbb{N} \iff a = b.$$

***Exercice 2.3.* — ★☆☆**
Soit $E = \{a\}$ un singleton.
Décrire (en donnant la liste de leurs éléments) les ensembles $\mathcal{P}(E)$, $\mathcal{P}(\mathcal{P}(E))$ et $\mathcal{P}(\mathcal{P}(\mathcal{P}(E)))$.

***Exercice 2.4* (Ensembles transitifs). — ★★☆**
Soit E un ensemble non vide. On suppose que les éléments de E sont eux-mêmes des ensembles. Si $x \in E$ et si y est un objet, on peut donc avoir $y \in x$. On s'intéresse à la propriété suivante :

$$\text{Pour tout } x \in E, \text{ et pour tout } y \in x, \text{ on a } y \in E. \tag{P}$$

1. Les ensembles $E_1 = \emptyset$, $E_2 = \{\emptyset\}$, $E_3 = \{\emptyset, \{\emptyset\}\}$ et $E_4 = \{\{\emptyset\}\}$ ont-ils la propriété (P) ?
2. Montrer que si un ensemble E a la propriété (P), alors l'ensemble $\mathcal{P}(E)$ a aussi la propriété (P).
3. Montrer que si un ensemble E a la propriété (P), alors $E \cup \{E\}$ a aussi la propriété (P).

***Exercice 2.5* (Paradoxe de Russell). — ★★★**

1. Le but de cette question est de montrer que la notion d'« ensemble de tous les ensembles » est problématique.

   Supposons que cette notion ne soit pas problématique et notons E l'ensemble de tous les ensembles. On définit alors l'ensemble

$$R = \{A \in E \ / \ A \notin A\}.$$

   Montrer qu'on a à la fois $R \in R$ et $R \notin R$. Conclure.

2. (*Plus difficile*) Soit E un ensemble. Montrer qu'il est impossible qu'on ait $\mathcal{P}(E) \subset E$.

Union, intersection, complémentaire. —

***Exercice 2.6* (Union et intersection). — ★☆☆**
Soient A et B deux ensembles. Démontrer que les énoncés suivants sont équivalents :

(a) $A \subset B$

(b) $A \cup B = B$

(c) $A \cap B = A$

***Exercice 2.7* (Pour manier le complémentaire). — ★☆☆**
Soit E un ensemble ; soient A, B, C des parties de E. On note A^{c} le complémentaire de A dans E.

1. Montrer l'égalité $(A \setminus B) \setminus C = A \setminus (B \cup C)$.
2. Montrer l'égalité $A \cap (A^{\mathrm{c}} \cup B) = A \cap B$.

***Exercice 2.8* (Pour manier le complémentaire, II). — ★☆☆**

1. Soit E un ensemble. Soient A et B des parties de E. Démontrer l'équivalence suivante :
$$[A \subset B] \iff [C_E(B) \subset C_E(A)]\,.$$
2. Soit E un ensemble et U, V, W des parties de E. On note V^{c} et W^{c} les complémentaires de V et de W dans E. Montrer l'équivalence suivante :
$$U \cap (V^{\mathrm{c}}) = U \cap W^{\mathrm{c}} \iff U \cap V = U \cap W.$$

***Exercice 2.9* (Pour manier le complémentaire, III). — ★★☆** Soient E, F et G trois ensembles. Montrer les égalités suivantes :

1. $E \setminus (F \cap G) = (E \setminus F) \cup (E \setminus G)$
2. $E \cup F \cup G = (E \setminus F) \cup (F \setminus G) \cup (G \setminus E) \cup (E \cap F \cap G)$.

***Exercice 2.10* (On ne peut pas « simplifier les unions »). — ★☆☆**

1. (a) Donner un exemple d'ensembles X, Y, Z vérifiant $X \cup Y = X \cup Z$ mais $Y \neq Z$.
   (b) Donner un exemple d'ensembles X, Y, Z vérifiant $X \cap Y = X \cap Z$ mais $Y \neq Z$.
2. Soient X, Y, Z trois ensembles. Montrer que si l'on a $X \cup Y = X \cup Z$ et $X \cap Y = X \cap Z$, alors $Y = Z$.

***Exercice 2.11* (Une manipulation abstraite). — ★★☆**
Soient A, B, C, D quatre ensembles. Montrer que si les quatre propriétés suivantes sont vérifiées :

(i) $A \subset C$,

(ii) $B \subset D$,

(iii) $C \cap D = \emptyset$,

(iv) $A \cup B = C \cup D$,

alors $A = C$ et $B = D$

***Exercice 2.12* (Différence symétrique). — ★★☆**
Si A et B sont deux ensembles, on appelle *différence symétrique* de A et B, et on note $A \Delta B$, l'ensemble
$$A \Delta B = (A \cup B) \setminus (A \cap B)\,.$$

1. Soient A et B deux ensembles. Montrer l'égalité $A \Delta B = (A \setminus B) \cup (B \setminus A)$.
2. Soient A, B, C trois ensembles. Montrer l'égalité $A \cap (B \Delta C) = (A \cap B) \Delta (A \cap C)$.
3. Soient A, B, C trois ensembles. Montrer que si l'on a $A \Delta C = B \Delta C$, alors $A = B$.

Produit cartésien. —

***Exercice 2.13* (Dessins). — ★☆☆**
En utilisant les coordonées cartésiennes pour dessiner des parties de $\mathbb{R}^2$, dessiner les sous-ensembles

$$A = [-1,3] \times [-3,1], \quad B = \mathbb{Z} \times [-3,2], \quad C = A \cap ([2,3] \times [0,1])\,.$$

***Exercice 2.14* (Une manipulation abstraite). — ★★☆** Soient A, B, C, D quatre ensembles.

1. Montrer l'égalité $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$.
2. A-t-on toujours l'égalité $(A \times B) \cap C = (A \cap C) \times (B \cap C)$?
   Si votre réponse est oui, donner une démonstration ; si c'est non, donner un exemple de A, B, C pour lesquels l'égalité n'est pas vérifiée.

Familles indexées par un ensemble quelconque. —

***Exercice 2.15* (Familles et produit cartésien). — ★☆☆**
Pour tout $k \in \mathbb{N}^\star$, on note A_k l'ensemble $\left\{n \in \mathbb{N}^\star \;/\; n < \frac{5}{\sqrt{k}}\right\}$ et B_k l'ensemble $\left\{x \in \mathbb{R} \;/\; 0 < x < \frac{5}{\sqrt{k}}\right\}$.

- Donner la liste de tous les éléments du produit cartésien $\prod_{k=1}^{4} A_k$.
- Vérifier que le produit cartésien $\prod_{k\in\mathbb{N}^\star} A_k$ est vide, mais que le produit cartésien $\prod_{k\in\mathbb{N}^\star} B_k$ n'est pas vide.

***Exercice 2.16* (Union et intersection, I). — ★★☆**
Pour tout entier $k \in \mathbb{N}$, on note A_k l'intervalle $[k, k+10]$ et B_k l'intervalle $[-1, k]$.
Déterminer, en justifiant vos réponses, les ensembles suivants :

$$E_1 = \bigcap_{k=3}^{10} A_k \quad E_2 = \bigcap_{k\in\mathbb{N}} A_k, \quad E_3 = \bigcup_{k=3}^{10} A_k, \quad E_4 = \bigcup_{k\in\mathbb{N}} A_k,$$
$$F_1 = \bigcap_{k=3}^{10} B_k, \quad F_2 = \bigcap_{k\in\mathbb{N}} B_k, \quad F_3 = \bigcup_{k=3}^{10} B_k, \quad F_4 = \bigcup_{k\in\mathbb{N}} B_k.$$

On pourra utiliser librement l'« axiome » suivant : pour tout réel x, il existe un entier n vérifiant $n > x$.

***Exercice 2.17* (Compréhension des notations, II). — ★★☆**
Sans justifier votre réponse, déterminer les unions et intersections suivantes.

$$A = \bigcup_{x\in\mathbb{R}} \big[\sin(x), 1+\sin(x)\big], \quad B = \bigcup_{x\in[1,+\infty[} \left]\tfrac{1}{x}, x\right[, \quad C = \bigcap_{x\in[1,+\infty[} \left]\tfrac{1}{x}, x\right[, \quad D = \bigcap_{x\in[1,+\infty[} \left[\tfrac{1}{x}, x\right].$$

Applications. —

***Exercice 2.18* (Image directe, I). — ★☆☆**

1. Soit $f : \mathbb{R} \to \mathbb{R}$ la fonction définie par : $\forall x \in \mathbb{R}, f(x) = x^2$.
   (a) Si $A = [0,2]$ et $B = [1,4]$, que valent $f(A)$, $f(B)$, $f(A\cap B)$, $f(A\cup B)$, $f(A)\cap f(B)$ et $f(A)\cup f(B)$?
   (b) Trouver deux ensembles A et B pour lesquels on a $f(A \cap B) \neq f(A) \cap f(B)$.
2. Soit $g : \mathbb{R} \to \mathbb{R}$ une fonction quelconque.
   (a) Soient A et B deux parties de $\mathbb{R}$. Montrer que $g(A \cap B) \subset g(A) \cap g(B)$.
   (b) Que peut-on dire en général du lien entre $g(A \cup B)$ et $g(A) \cup g(B)$?

***Exercice 2.19* (Image directe, II).** —

1. ★☆☆ On considère l'application

$$\begin{array}{rccc} f & : & [0,1]\times[0,1] & \to & \mathbb{R} \\ & & (x,y) & \mapsto & x+y. \end{array}$$

Déterminer l'ensemble $f([0,1]\times[0,1])$.

2. ★★☆ On fixe un ensemble E et une partie A de E. On considère l'application

$$\begin{array}{rccc} \Phi & : & \mathcal{P}(E) & \to & \mathcal{P}(E) \\ & & B & \mapsto & A\cap B. \end{array}$$

Déterminer les ensembles $\Phi(B)$, $\Phi(\mathcal{P}(B))$ et $\Phi(\mathcal{P}(E))$.

***Exercice 2.20* (Image réciproque, I).** — ★☆☆

1. Soit $f:\mathbb{R}\to\mathbb{R}$ la fonction définie par : $\forall x\in\mathbb{R}, f(x)=x^2$.
Si $A=[0,4]$ et $B=[-1,1]$, que valent $f^{-1}(A)$, $f^{-1}(B)$, $f^{-1}(A\cap B)$ et $f^{-1}(A\cup B)$?
2. Soit $g:\mathbb{R}\to\mathbb{R}$ une fonction quelconque. Soient A et B deux parties de $\mathbb{R}$.
Montrer que $g^{-1}(A\cap B)=g^{-1}(A)\cap g^{-1}(B)$ et que $g^{-1}(A\cup B)=g^{-1}(A)\cup g^{-1}(B)$.

***Exercice 2.21* (Une manipulation abstraite, I).** — ★☆☆
Soient E et F deux ensembles, $f:E\to F$ une application. Soient A une partie de E et B une partie de F. Montrer l'égalité suivante :

$$f\left(A\cap f^{-1}(B)\right)=f(A)\cap B.$$

***Exercice 2.22* (Une manipulation abstraite, II).** — ★☆☆
Soient E et F deux ensembles et $f:E\to F$ une application. Montrer l'égalité suivante :

$$E=\bigcup_{y\in F} f^{-1}(y).$$

***Exercice 2.23* (Fonction caractéristique d'une partie).** — ★★☆ – *long*
Soit E un ensemble. Pour chaque partie A de E, on définit une application $\mathbf{1}_A : E\to\mathbb{R}$ par la formule suivante :

$$\forall x\in E,\quad \mathbf{1}_A(x)=\begin{cases}1 & \text{si } x\in A\\ 0 & \text{si } x\notin A.\end{cases}$$

1. Soit A une partie de E. Montrer l'égalité d'applications suivante : $\mathbf{1}_{C_E(A)}=1-\mathbf{1}_A$.
2. Soient A et B deux ensembles.
   (a) Montrer l'égalité d'applications suivante : $\mathbf{1}_{A\cap B}=\mathbf{1}_A\mathbf{1}_B$.
   (b) Montrer l'égalité $\mathbf{1}_{A\cup B}=\mathbf{1}_A+\mathbf{1}_B-\mathbf{1}_A\mathbf{1}_B$.
3. Soient A et B deux parties de E.
   (a) Imaginer et démontrer une formule pour $\mathbf{1}_{A\setminus B}$.
   (b) Si $A\Delta B$ est la différence symétrique de l'exercice 2.12, imaginer et démontrer une formule pour $\mathbf{1}_{A\Delta B}$.

CHAPITRE 3

RAISONNEMENT : MÉTHODES ET EXEMPLES

Ce chapitre présente les manières les plus courantes de *démontrer* une assertion mathématique. Il est crucial pour vos études, non seulement de maîtriser ces méthodes, mais aussi d'apprendre à *rédiger* vos raisonnements aussi clairement et rigoureusement que possible. L'enjeu n'est pas uniquement « scolaire » : apprendre à discerner les stratégies possibles pour un raisonnement, puis exprimer clairement ses idées, est l'un des éléments essentiels d'un début de formation scientifique.

1. Assertions avec quantificateur universel

1.1. Démontrer une assertion qui commence par un « pour tout ». —

Fixons un ensemble non vide E et supposons donnée, pour chaque x de E, une assertion $\mathcal{P}(x)$.

Sauf si E comporte un nombre fini d'éléments dont on connaîtrait une liste complète, pour vérifier l'assertion

$$\forall x \in E, \quad \mathcal{P}(x),$$

on ne peut pas procéder « élément par élément ». Une expérience de pensée est nécessaire pour travailler avec un élément x de E « quelconque » et montrer que l'assertion $\mathcal{P}(x)$ est nécessairement vraie.

> Pour commencer la démonstration d'une assertion du type « $\forall x \in E,\ \mathcal{P}(x)$ », on peut écrire
>
> « Soit x un élément de E »
>
> afin de fixer, jusqu'à nouvel ordre, un élément arbitraire x de E. On tente ensuite de montrer $\mathcal{P}(x)$.

Exemple 3.1. — Montrons l'assertion suivante :

$$\forall x \in \mathbb{R}, \quad x^2 + 1 \geq 2x.$$

Soit x un élément de $\mathbb{R}$. Partons du fait que $(x+1)^2 \geq 0$: on a alors

$$x^2 - 2x + 1 \geq 0,$$

autrement dit,

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

ce qu'il fallait démontrer.

Exemple 3.2. — Montrons l'énoncé suivant :

Pour tout entier naturel n, si n est impair, alors l'entier $n^2 - 1$ est divisible par 8.

Soit n un entier naturel. Supposons n impair : il existe donc un entier $k \in \mathbb{N}$ vérifiant $n = 2k + 1$.
On a alors

$$n^2 - 1 = (2k + 1)^2 - 1 = (2k)(2k + 2) = 4k(k + 1).$$

De plus, les entiers k et $k + 1$ sont consécutifs, donc l'un des deux est pair. On peut alors distinguer deux cas :

- Si k est pair, alors il existe un entier $q \in \mathbb{N}$ vérifiant $k = 2q$, et alors
$$n^2 - 1 = 8q(k + 1);$$
puisque le nombre $q(k + 1)$ est entier, l'entier $n^2 - 1$ est bien divisible par 8.
- Si $k + 1$ est pair, alors il existe un entier $s \in \mathbb{N}$ vérifiant $k + 1 = 2s$, et alors
$$n^2 - 1 = 8ks;$$
puisque le nombre ks est entier, l'entier $n^2 - 1$ est bien divisible par 8.

Remarque 3.3. — Dans l'exemple précédent, en écrivant « Soit $n \in \mathbb{N}$ » au début de la démonstration, on introduit un entier n quelconque mais fixé, et il *restera fixé* jusqu'à la fin de l'argument. Certains des entiers qui interviennent au cours du raisonnement (k, q...) dépendent de n et seulement de n. Ils sont donc déterminés par le n qu'on a fixé au départ : on ne peut pas les « choisir », ni les « modifier ».

1.2. Infirmer une assertion qui commence par un « pour tout ». — Considérons à nouveau un énoncé du type

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

S'il est faux, c'est qu'il existe un x de E pour lequel l'assertion $\mathcal{P}(x)$ n'est pas vérifiée. Le plus simple pour démontrer cela est de trouver un exemple concret d'élément x pour lequel $\mathcal{P}(x)$ n'est pas vérifiée :

> Pour montrer qu'une assertion du type « $\forall x \in E,\ \mathcal{P}(x)$ » est *fausse*, on peut donner un *contre-exemple*, c'est-à-dire un exemple de x pour lequel $\mathcal{P}(x)$ n'est pas vérifiée.

Exemple 3.4. — L'assertion

$$\forall n \in \mathbb{N}, \quad n^2 \geq 2n$$

est fausse, puisque pour $n = 1$, on a $n^2 < 2n$. De même, l'assertion

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

est fausse, puisque pour $x = \frac{1}{2}$, on a $x^2 < x$.

***Exemple 3.5* (Nombres de Fermat).** — Considérons l'assertion suivante :

Pour tout entier naturel n, l'entier $F_n = 2^{2^n} + 1$ est premier.

Choisissons $n = 5$; alors $F_n = F_5 = 2^{32} - 1 = 4\,294\,967\,297$, et même si cela n'a rien d'évident, ce nombre n'est pas premier : on a $F_5 = 641 \cdot 6\,700\,417$.

***Remarque 3.6* (Contre-exemple concret vs expliquer « pourquoi c'est faux »)**

Considérons l'assertion suivante :

$$\forall x \in \mathbb{R}, \quad x^2 - 3x + 2 > 0.$$

Est-elle vraie ou fausse ? Pour le savoir, on peut étudier le signe de la fonction $x \mapsto x^2 - 3x + 2$. En reconnaissant un polynôme du second degré, on s'aperçoit que cette fonction admet deux zéros en $x = 1$ et $x = 2$ et qu'elle est négative entre 1 et 2, mais positive sur $]-\infty, 1[$ et sur $]1, +\infty[$.

L'assertion est donc fausse. Que vaut-il mieux écrire pour en convaincre nos lecteurs ? Deux possibilités : on peut donner des informations assez complètes, comme

L'assertion est fausse pour tous les x compris strictement entre 1 et 2.

Mais on peut aussi donner un contre-exemple concret, en écrivant par exemple :

Choisissons $x = \frac{3}{2}$: alors $x^2 - 3x + 2 = -\frac{1}{4}$, et donc on n'a pas $x^2 - 3x + 2 > 0$.

Paradoxalement, c'est la *seconde* solution qu'on vous recommandera le plus souvent pour rédiger vos textes dans vos études. Certes, elle ne montre pas ce qui « motive » le choix de $x = \frac{3}{2}$, elle passe sous silence le fait qu'il existe d'autres choix de x pour lesquels l'assertion échoue... Mais il est très facile de vérifier concrètement ce qui est écrit, et c'est ce qui compte pour convaincre nos lecteurs que l'assertion est fausse.

1.3. Utiliser une assertion qui commence par un « pour tout ». — La situation où l'on doit *partir* d'une assertion du type « $\forall x \in E,\ \mathcal{P}(x)$ », puis démontrer autre chose, donne souvent lieu à des difficultés.

Pour utiliser une assertion du type « $\forall x \in E,\ \mathcal{P}(x)$ », on doit choisir un x auquel l'appliquer.

Exemple 3.7. — Soit f une fonction de $\mathbb{R}$ dans $\mathbb{R}$. Supposons vérifiée la propriété suivante :

$$\forall x \in \mathbb{R},\ f(1-x) = 5f(x) \tag{1.1}$$

- À partir de (1.1), il n'est pas difficile de montrer que $f(\frac{1}{2}) = 0$: en appliquant la propriété (1.1) avec $x = \frac{1}{2}$, on obtient $f(\frac{1}{2}) = 5f(\frac{1}{2})$, donc $4f(\frac{1}{2}) = 0$, et on a bien $f(\frac{1}{2}) = 0$ comme espéré.
- Il est un peu plus délicat de montrer à partir de (1.1) que $f(0) = 0$.
  En appliquant d'abord (1.1) avec $x = 0$, on obtient $f(1) = 5f(0)$. Mais en appliquant à nouveau (1.1) avec $x = 1$, on obtient $f(0) = 5f(1)$. On a donc $f(0) = 5f(1) = 5\,[5f(0)] = 25f(0)$, d'où on déduit comme précédemment que $f(0) = 0$.

Exemple 3.8. — Soit f une fonction de $\mathbb{R}$ dans $\mathbb{R}$. Supposons que f est croissante sur $\mathbb{R}^+$ et que $f(0) = 0$. Montrons que pour tout $x \in \mathbb{R}^+$, on a $f(x) \geq 0$.

L'hypothèse « f croissante sur $\mathbb{R}^+$ » s'écrit avec des quantificateurs

$$\forall a \geq 0,\ \forall b \geq 0, \quad (a \leq b \implies f(a) \leq f(b)) \tag{1.2}$$

Soit x un élément de $\mathbb{R}^+$. Appliquons (1.2) avec $a = 0$ et $b = x$: puisque $x \geq 0$, cela fournit $f(0) \leq f(x)$; comme $f(0) = 0$ on obtient $f(x) \geq 0$, ce qu'il fallait démontrer.

Attention aux variables muettes. — Lorsqu'on veut montrer une assertion écrite avec des quantificateurs à partir d'autres assertions elles-mêmes écrites avec des quantificateurs, les *noms des variables* peuvent semer la confusion, notamment lorsqu'il y a des variables muettes en commun dans les deux assertions à montrer. L'exemple suivant est une illustration emblématique de cette difficulté.

***Exemple 3.9* (Important !)** — Soit f une fonction de $\mathbb{R}$ dans $\mathbb{R}$. Supposons vérifiée la propriété suivante :

$$\forall \varepsilon > 0, \exists x \in \mathbb{R}, \quad 0 < f(x) < \varepsilon. \tag{H}$$

Montrons l'assertion suivante :

$$\forall \varepsilon > 0,\ \exists x \in \mathbb{R}, \quad 0 < 2f(x) < \varepsilon. \tag{1.3}$$

Comment débuter notre raisonnement ? Un conseil général s'impose à ce stade :

Se laisser guider par *l'assertion à montrer.*

Ici, c'est l'assertion (1.3) que nous devons prouver. C'est une assertion qui commence par un « pour tout », on peut (et on doit) donc suivre les préceptes du §1.1. Écrivons donc :

Soit $\varepsilon > 0$.

Nous avons maintenant fixé un nombre ε, qui ne *peut plus bouger* jusqu'à la fin de notre raisonnement. Pour aller plus loin, nous ne pouvons pas appliquer l'hypothèse (H) à ce ε-là, puisque cela ne donnera pas la conclusion voulue.

Mais on peut (et on doit) remarquer que dans (H), les variables sont *muettes* : l'hypothèse (H) a *exactement la même signification* que la version suivante :

$$\forall \alpha > 0,\ \exists x \in \mathbb{R},\quad 0 < f(x) < \alpha. \qquad \text{(H, reformulée)}$$

Nous avons fixé ε au début de notre raisonnement, mais nous pouvons appliquer (H, reformulée) avec un α de notre choix. On constate alors qu'en appliquant (H, reformulée) avec $\alpha = \dfrac{\varepsilon}{2}$, on obtient l'existence d'un réel x vérifiant

$$0 < f(x) < \frac{\varepsilon}{2}$$

autrement dit, $0 < 2f(x) < \varepsilon$, comme espéré.

2. Assertions avec quantificateur existentiel

2.1. Démontrer une assertion qui commence par un « il existe ». — Considérons à nouveau un ensemble non vide E et supposons donnée, pour chaque x de E, une assertion $\mathcal{P}(x)$. Si nous voulons vérifier l'assertion

$$\exists x \in E \ / \ \mathcal{P}(x),$$

nous devons montrer qu'il existe au moins un élément de E pour lequel $\mathcal{P}(x)$ est vraie. Le plus simple est encore de trouver concrètement un tel élément, lorsque c'est possible :

> Pour démontrer une assertion du type « $\exists x \in E \ / \ \mathcal{P}(x)$ », on peut chercher un *exemple concret* d'élément x de E pour lequel $\mathcal{P}(x)$ est vérifiée.

Exemple 3.10. — On fixe trois réels a, b et c, on suppose $a > 0$ et $c < 0$ et on veut montrer l'assertion

$$\exists x \in \mathbb{R} \ / \ ax^2 + bx + c \leq 0.$$

Choisissons $x = 0$; on a alors $ax^2 + bx + c = c < 0$, ce qui montre que le x choisi convient.

2.2. Infirmer une assertion qui commence par un « il existe ». — Considérons à nouveau une assertion de la forme

$$\exists x \in E \ / \ \mathcal{P}(x).$$

Si elle est fausse, c'est que sa négation est vraie. Or sa négation est « $\forall x \in E, \text{NON}\,[\mathcal{P}(x)]$ » : cette négation est une assertion du type considéré au §1.1.

> Pour montrer qu'une assertion du type « $\exists x \in E \ / \ \mathcal{P}(x)$ » est fausse,
> on montre que pour tout x de E, la négation de $\mathcal{P}(x)$ est vraie.

Exemple 3.11. — Montrons qu'il n'existe pas de nombre réel α vérifiant

$$e^{2\alpha} + 3e^{\alpha} + 2 = 0.$$

Soit α un nombre réel. On a alors $e^{2\alpha} > 0$ et $e^{\alpha} > 0$, car la fonction exp est strictement positive sur $\mathbb{R}$. Les nombres $e^{2\alpha}$, $3e^{\alpha}$ et 2 sont donc tous les trois strictement positifs ; leur somme $e^{2\alpha} + 3e^{\alpha} + 2$ est donc strictement positive ; ainsi $e^{2\alpha} + 3e^{\alpha} + 2 \neq 0$.

2.3. Utiliser une assertion qui commence par un « il existe ». — À nouveau, cette situation peut induire des difficultés. La raison est la suivante :

> Un énoncé du type « $\exists x \in E \ / \ \mathcal{P}(x)$ » nous fournit abstraitement un élément x tel que $\mathcal{P}(x)$ soit vérifiée, mais ne permet pas de savoir concrètement qui est ce x.

Exemple 3.12. — Considérons une fonction $f : \mathbb{R} \to \mathbb{R}$ vérifiant l'hypothèse suivante :

$$\exists M \in \mathbb{R}_\star^+ \ / \quad \forall u \in \mathbb{R}, \quad f(u) > M. \tag{2.1}$$

et vérifions qu'il est impossible que f soit impaire.

Fixons un nombre $M > 0$ tel que décrit par (2.1) : on ne sait pas exactement qui est ce M, mais on sait qu'il est strictement positif et qu'on a

$$\forall u \in \mathbb{R}, \quad f(u) > M.$$

En particulier, on doit avoir $f(0) > M > 0$. Or, si f est impaire, alors on a nécessairement $f(0) = 0$: il est donc impossible que f soit impaire.

Exemple 3.13. — Soit E une partie de $\mathbb{N}$ ne contenant pas le nombre 1. Supposons vérifiée l'hypothèse suivante :

$$\forall n \in \mathbb{N}, \quad \exists m \in E \quad / \quad m \text{ divise } n. \tag{2.2}$$

- Appliquée à $n = 150$, l'assertion (2.2) fournit l'existence d'un élément m de E vérifiant $m|n$; un tel m est nécessairement un diviseur de $150 = 2 \cdot 3 \cdot 5^2$, mais notre hypothèse ne dit pas qui est ce m : le nombre 150 admet 12 diviseurs différents ($1, 2, 3, 5, 6, 10, 15, 25, 30, 50, 75$ et 150) et on ne sait rien de plus que le fait que notre m est l'un de ces 12 entiers.

- Montrons cependant que E contient tous les nombres premiers.

  Soit p un nombre premier. Appliquons (2.2) avec $n = p$: on obtient l'existence d'un entier m appartenant à E et qui divise p. Fixons un tel m. On ne peut pas avoir $m = 1$, car on a supposé que E ne contient pas le nombre 1. Comme p est premier, les seuls diviseurs positifs de p sont 1 et p ; on a donc nécessairement $m = p$, et comme par définition on a $m \in E$, le nombre p appartient à E, comme espéré.

3. Équivalences et implications

3.1. Démontrer une implication directement. — Nous avons vu dans le chapitre précédent certaines subtilités du connecteur logique $\implies$ et des assertions du type $A \implies B$. Ces subtilités sont importantes et bonnes à connaître, mais ne remettent pas en cause la stratégie la plus habituelle pour montrer que « si A est vraie, alors B est vraie ».

> Pour démontrer une implication $A \implies B$, on peut supposer A et tenter de montrer B, en se laissant guider par l'assertion B à montrer.

Exemple 3.14. — Soient A et B deux ensembles. Démontrons l'implication suivante :

$$\textit{Si } A \cap B = A, \textit{ alors } A \subset B.$$

Supposons que l'égalité $A \cap B = A$ soit vérifiée et montrons l'inclusion $A \subset B$. Ce qu'il nous faut maintenant, c'est démontrer $A \subset B$: nous devons donc démontrer l'assertion « $\forall x \in A, \ x \in B$ ».

Soit x un élément de A. Alors, d'après l'hypothèse $A \cap B = A$, on a aussi $x \in A \cap B$, et en particulier x appartient à B : c'est ce qu'il fallait montrer.

3.2. Montrer une implication en raisonnant par contraposition. — Lorsqu'on souhaite démontrer qu'une assertion de la forme $(A \implies B)$ est vraie, le plus simple est de supposer A vraie et d'essayer de montrer B, comme dans le paragraphe précédent. Mais si cela s'avère difficile, une autre stratégie est possible : on peut s'appuyer sur le fait que l'implication $A \implies B$ est logiquement équivalente à l'implication $\text{NON}(B) \implies \text{NON}(A)$.

Proposition 3.15 – Raisonnement par contraposition

Pour montrer une implication $A \implies B$, on peut supposer la négation de B et montrer la négation de A.

Exemple 3.16. — Soit n un entier naturel. Pour démontrer l'assertion

« Si n^2 est pair, alors n est nécessairement pair »,

on peut raisonner par contraposition et remarquer que cela revient à démontrer que si n est impair, alors n^2 est impair. Or, si n est un entier impair, il existe un entier k vérifiant $n = 2k+1$, et alors $n^2 = (2k+1)^2 = 4k^2+4k+1 = 2\left(2k^2+2k\right)+1$, si bien que n^2 est impair, comme espéré.

Exemple 3.17. — On fixe deux nombres réels a et b. Montrons l'implication suivante :

$$(\forall \varepsilon > 0,\ a < b+\varepsilon) \implies (a \leq b)\,.$$

Raisonnons par contraposition : supposons $a > b$ et montrons qu'il existe un nombre $\varepsilon > 0$ vérifiant $a \geq b+\varepsilon$. Ce que nous devons montrer maintenant, c'est qu'il existe un $\varepsilon > 0$ vérifiant $\varepsilon \leq a-b$.
Choisissons $\varepsilon = \frac{a-b}{2}$. On a alors $b+\varepsilon = \frac{2b+a-b}{2} = \frac{a+b}{2}$, et comme $a > b$, on a bien $a \geq \frac{a+b}{2}$. Avec ce choix de ε, on a donc bien $a \geq b+\varepsilon$.

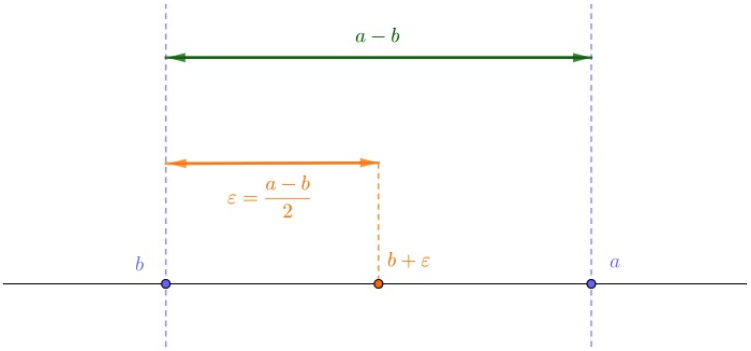


FIGURE 1. Illustration du choix de $\varepsilon = \frac{a-b}{2}$: il s'agit de la moitié de la distance entre a et b.

3.3. Démontrer une équivalence. —

Pour démontrer une équivalence $A \iff B$, deux stratégies sont possibles :
(a) Démontrer séparément les implications $A \implies B$ et $B \implies A$,
(b) Ou montrer directement que A et B ont la même signification.

Exemple 3.18. — Soient x et y deux réels. Montrons l'assertion

$$x^2+y^2 = 0 \iff x = y = 0.$$

On peut ici utiliser la stratégie (a) et établir la double implication :

- Si $x^2+y^2=0$, alors $x^2=-y^2$; le nombre x^2 est donc à la fois positif (puisque c'est le carré du réel x) et négatif (puisque c'est l'opposé du carré du réel y). Il est donc nul : on a ainsi $x^2=0$, donc $x=0$, et aussi $y^2=-x^2=0$, donc $y=0$.
- Réciproquement, si $x=y=0$, alors on a bien sûr $x^2+y^2=0+0=0$.

Exemple 3.19. — On donne ici une illustration de la stratégie (b). Soient x et y deux réels ; on suppose $0<x<1$. Montrons l'équivalence suivante :

$$x=\frac{e^y}{1+e^y} \iff y=\ln\left(\frac{x}{1-x}\right).$$

Dire que $x=\frac{e^y}{1+e^y}$ revient à dire que $x\,(1+e^y)=e^y$, autrement dit : $e^y\,(1-x)=x$.

Comme $x<1$, le nombre $1-x$ est non-nul, donc l'équation précédente équivaut à : $e^y=\frac{x}{1-x}$.

Par ailleurs, comme on a supposé $0<x<1$, les nombres x et $1-x$ sont strictement positifs, donc $\frac{x}{1-x}$ est strictement positif.

L'équation $e^y=\frac{x}{1-x}$ est donc équivalente à $y=\ln\left(\frac{x}{1-x}\right)$, comme espéré.

Méfiez-vous des chaînes d'équivalences ! — Le raisonnement de l'exemple précédent a le mérite d'éviter deux vérifications séparées. Mais, outre le fait que cette stratégie n'est pas toujours disponible (comment aurait-on fait sur l'exemple 3.18 ?), lorsqu'elle est utilisable il faut le faire avec précaution. En effet, dans une chaîne d'équivalences, *toute l'information doit être préservée d'une étape à l'autre*, il faut donc le faire soigneusement. Par exemple, si x est un réel positif et y un réel quelconque et si l'on écrit

$$x-y\geq\frac{1}{x+y} \iff (x+y)(x-y)\geq 1 \iff x^2-y^2\geq 1 \iff x^2\geq y^2+1 \iff x\geq\sqrt{y^2+1} \quad \text{(Faux !)}$$

voyez-vous où est l'erreur ?

De même, voyez-vous pourquoi la discussion aurait pu être plus délicate si on n'avait pas supposé à l'avance $x>1$ dans l'énoncé de l'exemple 3.19 ?

N'utilisez le symbole $\iff$ qu'avec précaution. — La remarque précédente rappelle que le symbole $\iff$ ne peut être utilisé que pour *affirmer* que deux « parties de discours » ont *exactement la même signification*. Il est donc souhaitable de ne jamais l'utiliser comme un simple « mot de liaison » entre deux parties de discours si l'on n'a pas réfléchi et constaté qu'elles avaient *vraiment* la même signification.

4. Disjonction de cas

Si l'on veut montrer une assertion comme

si x est égal soit à 5, soit à 13, alors x^2 peut s'écrire comme la somme des carrés de deux entiers

on hésite rarement sur la stratégie à adopter : on distingue les deux cas à traiter, $x=5$ et $x=13$, et on vérifie la conclusion dans chaque cas (dans le premier cas, $5^2=25=16+9$ peut s'écrire comme 3^2+4^2, et dans le deuxième cas, $13^2=169=144+25$ peut s'écrire comme 12^2+5^2).

Dans certaines situations, le fait qu'il soit bon de traiter séparément plusieurs cas peut être moins apparent. Voici quelques exemples.

Exemple 3.20. — Montrer que pour tout entier relatif x, l'entier x^2+x est pair.
Soit x un entier relatif. Distinguons deux cas :

- Si x est pair, alors il existe un entier $k\in\mathbb{Z}$ tel que $x=2k$, et alors
$$x^2+x=4k^2+2k=2\left(2k^2+k\right).$$
- Si x est impair, alors il existe un entier $k\in\mathbb{Z}$ tel que $x=2k+1$, et alors
$$x^2+x=\left(4k^2+4k+1\right)+(2k+1)=2\left(2k^2+3k+1\right).$$

Dans tous les cas, x^2+x est pair.

Exemple 3.21. — Montrer que pour tout réel x, on a $|x-2| \leq x^2 - 2x + 3$.
Soit x un nombre réel. Distinguons deux cas :

- Si $x \geq 2$, alors $|x-2| = x-2$ et ce que nous devons montrer est qu'on a $x - 2 \leq x^2 - 2x + 3$. Or, on constate que
$$\left(x^2 - 2x + 3\right) - (x-2) = x^2 - 3x + 5 = \left(x^2 - \frac{3}{2}\right)^2 + \frac{11}{4}$$
et que ce nombre est positif, ce qui permet de conclure.
- Si $x < 2$, alors $|x-2| = 2 - x$ et ce que nous devons montrer est donc qu'on a $2 - x \leq x^2 - 2x + 3$. Cette fois, on a
$$\left(x^2 - 2x + 3\right) - (2-x) = x^2 - x + 1 = \left(x^2 - \frac{1}{2}\right)^2 + \frac{5}{4}$$
et à nouveau, ce nombre est positif ; l'inégalité voulue est donc vérifiée.

Dans tous les cas, on a bien $|x-2| \leq x^2 - 2x + 3$.

Exemple 3.22. — Montrer qu'il existe deux nombres réels $a > 0$ et $b > 0$ vérifiant : a et b sont irrationnels, mais a^b est rationnel. *On donne pour indication de considérer* $\sqrt{2}^{\sqrt{2}}$.

Nous ne savons pas si $\sqrt{2}^{\sqrt{2}}$ est rationnel ou non. On peut cependant distinguer deux cas :

- S'il est rationnel, alors en choisissant $a = \sqrt{2}$ et $b = \sqrt{2}$, on constate que a et b sont irrationnels alors que a^b l'est.
- S'il n'est pas rationnel, alors en choisissant $a = \sqrt{2}^{\sqrt{2}}$ et $b = \sqrt{2}$, on obtient $a^b = \sqrt{2}^{\sqrt{2}\times\sqrt{2}} = \sqrt{2}^2 = 2$, et a^b est rationnel alors que a et b sont irrationnels.

5. Raisonnement par récurrence

5.1. Principe de récurrence ; exemples de rédaction. —

Comme nous l'évoquions au §1.2, la liste des axiomes couramment utilisés en mathématiques est très courte ; la possibilité d'effectuer des raisonnements par récurrence fait partie de ces axiomes.

Axiome 3.23 – Principe de récurrence

Fixons un entier naturel n_0. Supposons donnée, pour chaque entier $n \geq n_0$, une assertion $\mathcal{P}(n)$, et supposons que

1. *l'assertion $\mathcal{P}(n_0)$ est vraie,*
2. *pour tout entier $n \geq n_0$, on a $[\mathcal{P}(n) \implies \mathcal{P}(n+1)]$.*

L'assertion $\mathcal{P}(n)$ est alors vraie pour tout entier $n \geq n_0$.

***Exemple 3.24* (Un cas simple).** — Montrons le résultat suivant :
$$\forall n \in \mathbb{N}^\star, \quad 2^n \geq n.$$

- Pour $n = 1$, on a $2^n = 2$ et $n = 1$, donc $2^n \geq n$.
- Fixons à présent un entier naturel n et supposons que $2^n \geq n$; montrons qu'on a alors $2^{n+1} \geq n+1$.
  D'après notre hypothèse de récurrence, nous avons $2^{n+1} = 2 \times 2^n \geq 2n$.
  Or, $2n \geq n+1$, car $(2n) - (n+1) = n - 1 \geq 0$. Nous obtenons donc $2^{n+1} > (n+1)$, comme espéré.

***Exemple 3.25* (Bien écrire l'hypothèse de récurrence).** — Montrons l'assertion suivante :
$$\forall n \in \mathbb{N},\ \forall x \in \mathbb{R}, \quad |\sin(nx)| \leq n|\sin(x)|$$

Nous allons raisonner par récurrence sur l'entier n. Dans l'assertion à montrer, il y a cependant aussi une variable x. Il ne faut donc pas oublier de bien écrire ce qu'on va montrer.

Pour $n \in \mathbb{N}$, notons $\mathcal{P}(n)$ l'énoncé

$$\forall x \in \mathbb{R}, \quad |\sin(nx)| \leq n|\sin(x)|.$$

- Pour $n = 0$, on a pour tout réel x : $|\sin(nx)| = 0 = 0|\sin(x)|$. Ainsi l'inégalité est vérifiée.
- Fixons à présent un entier naturel, supposons que $\mathcal{P}(n)$ soit vraie et montrons $\mathcal{P}(n+1)$.
  Soit x un nombre réel. Partons du fait que

$$\sin[(n+1)x] = \cos(x)\sin(nx) + \sin(x)\cos(nx)$$

  et majorons à l'aide de l'inégalité triangulaire : on obtient

$$\begin{aligned} |\sin[(n+1)x]| &\leq |\cos(x)||\sin(nx)| + |\cos(nx)||\sin(x)| \\ &\leq 1 \cdot |\sin(nx)| + 1 \cdot |\sin(x)| \quad \text{(Propriétés de cos et sin)} \\ &\leq n|\sin(x)| + |\sin(x)| \quad \text{(Hypothèse de récurrence)} \\ &= (n+1)|\sin(nx)| \end{aligned}$$

  ce qu'il fallait démontrer.

Attention à la rédaction des récurrences. — Rédiger une récurrence est simple et ne nécessite pas de longue discussion : les exemples précédents devraient l'avoir montré. En début de L1, certaines habitudes parfois tolérées au lycée peuvent mener à des erreurs assez lourdes.

> Certaines erreurs, comme écrire « supposons que pour tout n, l'énoncé $\mathcal{P}(n)$ soit vrai » au cours d'un raisonnement par récurrence, sont à éviter absolument.

En effet, si le but du raisonnement est de démontrer que $\mathcal{P}(n)$ est vrai pour tout n, il est hors de question de supposer en cours de route ce que l'on veut montrer !

De même, si l'on vient de vérifier que $\mathcal{P}(0)$ est vrai, écrire immédiatement ensuite « supposons que $\mathcal{P}(n)$ soit vrai pour un certain entier n », alors qu'on vient de montrer qu'il est vrai pour $n = 0$, est assez maladroit.

Exemple 3.26. — Pour $n \in \mathbb{N}$, notons $\mathcal{P}(n)$ l'énoncé suivant :

$$\left(\sum_{\substack{k=1 \\ k \text{ impair}}}^{2n-1} k \right) := 1 + 3 + 5 + \cdots + (2n-3) + (2n-1) = n^2.$$

Montrons par récurrence que $\mathcal{P}(n)$ est vrai pour tout $n \in \mathbb{N}$.

- Pour $n = 0$, on a $\sum_{\substack{k=1 \\ k \text{ impair}}}^{2n-1} k = 1$, puisqu'il y a un seul terme dans la somme $\sum_{\substack{k=1 \\ k \text{ impair}}}^{2n-1} k$ et qu'il vaut 1.
- Fixons un entier $n \in \mathbb{N}$. Supposons qu'on ait

$$\left(\sum_{\substack{k=1 \\ k \text{ impair}}}^{2n-1} k \right) := 1 + 3 + 5 + \cdots + (2n-3) + (2n-1) = n^2$$

  et montrons qu'on a alors

$$\left(\sum_{\substack{k=1 \\ k \text{ impair}}}^{2(n+1)-1} k \right) := 1 + 3 + 5 + \cdots + (2n-3) + (2n-1) + (2n+1) = (n+1)^2.$$

On constate que la somme s'écrit

$$\left(\sum_{\substack{k=1\\ k \text{ impair}}}^{2(n+1)-1} k\right) = \left(\sum_{\substack{k=1\\ k \text{ impair}}}^{2n+1} k\right) = \left(\sum_{\substack{k=1\\ k \text{ impair}}}^{2n-1} k\right) + (2n+1),$$

et par notre hypothèse de récurrence cela vaut $(n^2) + (2n+1) = n^2 + 2n + 1 = (n+1)^2$: on obtient la conclusion souhaitée.

***Remarque 3.27* (De la nécessité de soigner l'initialisation).** — Pour chaque entier $n \in \mathbb{N}$, notons $\mathcal{P}(n)$ l'énoncé

« 4^n est divisible par 3 ».

- Si nous considérons un entier $n \in \mathbb{N}$ et si nous supposons que $\mathcal{P}(n)$ est vrai, alors on constate que $\mathcal{P}(n+1)$ est nécessairement vrai aussi : on a $4^{n+1} + 1 = 4 \cdot 4^n + 1 = 4 \cdot 4^n + 4 - 3 = 4 \cdot (4^n + 1) - 3$, et si $4^n + 1$ est supposé divisible par 3, alors $4 \cdot (4^n + 1) - 3$ est aussi divisible par 3.
- Notre propriété est donc héréditaire : s'il existe un n_0 tel que $\mathcal{P}(n_0)$ soit vraie, alors $\mathcal{P}(n)$ est vraie pour tout entier $n \geq n_0$.
- Mais cela ne permet pas de conclure quoi que ce soit : $\mathcal{P}(0)$ n'est pas vraie, $\mathcal{P}(1)$ n'est pas vraie non plus... En fait, il n'existe *aucun* entier n_0 tel que $\mathcal{P}(n_0)$ soit vraie.

5.2. Récurrence forte. — Voici une variante, parfois utile, du raisonnement par récurrence.

Théorème 3.28 – Récurrence forte

Fixons un entier naturel n_0. Supposons donnée, pour chaque $n \geq n_0$, une assertion $\mathcal{P}(n)$, et supposons que

1. *l'assertion $\mathcal{P}(n_0)$ est vraie,*
2. *pour tout $n \geq n_0$, si $\mathcal{P}(k)$ est vraie pour tous les entiers k vérifiant $n_0 \leq k \leq n$, alors $\mathcal{P}(n+1)$ est vraie.*

L'assertion $\mathcal{P}(n)$ est alors vraie pour tout entier $n \geq n_0$.

Démonstration à partir du principe de récurrence « standard » . — Pour chaque entier $n \geq n_0$, notons $\mathcal{A}(n)$ l'énoncé

$$\text{L'énoncé } \mathcal{P}(k) \text{ est vrai pour tout } k \in \{n_0, \dots, n\} \qquad (\mathcal{A}(n))$$

- L'énoncé $\mathcal{A}(n_0)$ affirme juste que $\mathcal{P}(k)$ est vrai pour $k = n_0$, donc il fait partie de nos hypothèses.
- Fixons à présent un entier $n \geq n_0$ et supposons que $\mathcal{A}(n)$ est vrai. Montrons alors $\mathcal{A}(n+1)$. Compte tenu de $\mathcal{A}(n)$, nous savons que $\mathcal{P}(k)$ est vraie pour tous les entiers k compris entre n_0 et n ; grâce à l'hypothèse 2. on sait alors que $\mathcal{P}(n+1)$ est vrai aussi ; ainsi, $\mathcal{P}(k)$ est vrai pour tout $k \in \{n_0, \dots, n+1\}$. Cela indique bien que $\mathcal{A}(n+1)$ est vrai.

Ainsi, $\mathcal{A}(n)$ est vrai pour tout entier $n \geq n_0$; mais cela a pour conséquence que $\mathcal{P}(n)$ est vrai pour tout $n \geq n_0$, comme espéré. □

Exemple 3.29. — Montrons l'assertion suivante :

Si n est un entier supérieur ou égal à 2, alors n admet au moins un diviseur premier.

- Si $n = 2$, l'énoncé à montrer est clair, puisque n est lui-même premier.
- Fixons à présent un entier $n \geq 2$ et supposons que pour tout $k \in \{2, \dots, n\}$, il existe au moins un nombre premier qui divise k. Montrons que le nombre $n+1$ admet au moins un diviseur premier.

  Deux cas peuvent se présenter :

  — Si $(n+1)$ est lui-même premier, alors il admet bien un diviseur premier, à savoir $(n+1)$ lui-même.

— Sinon, il existe un entier k qui divise $(n+1)$ et qui n'est égal ni à 1 ni à $(n+1)$; on a alors nécessairement $2 \leq k \leq n$. D'après notre hypothèse de récurrence, il existe au moins un nombre premier p qui divise k. Puisque k divise $(n+1)$, l'entier p est alors un diviseur premier de $(n+1)$.

Dans les deux cas, l'entier $(n+1)$ admet au moins un diviseur premier. □

5.3. Parties de $\mathbb{N}$: axiome du plus petit élément. — L'utilisation des récurrences est très liée à la structure de l'ensemble $\mathbb{N}$ des entiers naturels. Le principe de récurrence permet en fait de démontrer beaucoup des informations basiques les plus importantes sur la structure de $\mathbb{N}$. Par exemple, vous démontrerez au début du cours « Analyse 1 » la propriété suivante (voir la Proposition 1.20 du cours « Analyse 1 »).

Théorème 3.30 – Toute partie non vide de $\mathbb{N}$ admet un plus petit élément

Si A est une partie non vide de $\mathbb{N}$, alors il existe un unique entier a_0 vérifiant :

(i) $a_0 \in A$;

(ii) Pour tout $a \in A$, on a l'inégalité $a \geq a_0$.

L'entier a_0 est appelé le plus petit élément *de A.*

Ce théorème permet de parler de façon parfaitement rigoureuse du « plus petit entier vérifiant une certaine propriété », s'il existe effectivement de tels entiers. Voici une application immédiate mais importante, dont nous aurons besoin au chapitre 4 :

***Exemple 3.31* (Définition du PPCM).** — Fixons deux entiers naturels α et β et considérons l'ensemble

$$E = \{k \in \mathbb{N} \ / \ (k \text{ est multiple de } \alpha \text{ ET } k \text{ est multiple de } \beta)\,.\}$$

L'ensemble E est une partie de $\mathbb{N}$, et il contient l'entier $\alpha\beta$. C'est donc une partie non vide de $\mathbb{N}$. D'après l'axiome ci-dessus, il admet un plus petit élément. Ce plus petit élément est le plus petit entier qui soit à la fois multiple de α et de β : on l'appelle le *plus petit multiple commun*, ou PPCM, de α et β.

Il est aussi possible, dans certaines circonstances, de parler du plus grand entier vérifiant une propriété donnée. Nous aurons besoin d'une définition :

Définition 3.32 – Partie majorée

Soit A une partie de $\mathbb{N}$. On dit que A est *majorée* s'il existe un entier $M > 0$ vérifiant

$$\forall x \in A, \quad x \leq M.$$

Lorsque M est un tel nombre, on dit que A est *majorée par M*, ou encore que M est un *majorant* de A.

Exemple 3.33. — Fixons un entier $N \in \mathbb{N}$ et considérons l'ensemble

$$A = \{k \in \mathbb{N} \ / \ k \text{ divise } N\}\,.$$

Il s'agit bien d'une partie de $\mathbb{N}$; de plus, pour tout élément x de A, on a $x \geq N$ (puisque tout entier naturel qui divise N est compris entre 1 et N). Ainsi A est majorée par N.

Le résultat d'existence et d'unicité suivant sera lui aussi prouvé dans le cours « Analyse 1 », proposition 1.20.

Proposition 3.34 – Toute partie non vide et majorée de $\mathbb{N}$ admet un plus grand élément

Si A est une partie non vide de $\mathbb{N}$. Si A est majorée, alors il existe un unique entier a_0 vérifiant :

(i) $a_0 \in A$;

(ii) Pour tout $a \in A$, on a $a \leq a_0$.

L'entier a_0 est appelé le plus grand élément *de A.*

***Exemple 3.35* (Définition du PGCD).** — Fixons deux entiers naturels α et β et considérons l'ensemble

$$E = \{k \in \mathbb{N} \ / \ (k \text{ divise } \alpha \text{ et } k \text{ divise } \beta)\,.\}$$

L'ensemble E est une partie de $\mathbb{N}$. De plus, pour tout $k \in E$, on a $k \leq \alpha$ puisque k divise α : ainsi E est majoré.

D'après la proposition ci-dessus, l'ensemble E admet un plus grand élément. Ce plus grand élément est le plus grand entier qui divise simultanément α et β : on l'appelle le *plus grand diviseur commun*, ou PGCD, de α et β. On le note $\text{PGCD}(\alpha, \beta)$

6. Raisonnement par l'absurde

Proposition 3.36 – Principe du raisonnement par l'absurde

Si P est un énoncé et si l'hypothèse « P est faux » mène à une contradiction logique, alors P est nécessairement vrai.

Exemple 3.37. — Montrons l'assertion suivante :

Il existe une infinité de nombres premiers.

Supposons que l'assertion soit fausse et que l'ensemble $\mathcal{P}$ des nombres premiers comporte un nombre fini d'éléments. On peut alors écrire $\mathcal{P} = \{p_1, \ldots, p_n\}$ où n est un entier naturel donnant le nombre d'éléments de $\mathcal{P}$: chaque nombre premier est alors l'un des p_i, $i \in \{1, \ldots, n\}$.

Introduisons alors le nombre

$$a = p_1 p_2 \cdots p_n + 1.$$

L'entier a est supérieur ou égal à 2. D'après la propriété vue à l'exemple 3.29, il admet donc un diviseur premier. Fixons un tel diviseur premier, notons-le q ; puisque q appartient à l'ensemble $\mathcal{P}$, c'est l'un des p_i.

On constate alors que q divise a, mais divise aussi le produit $p_1 p_2 \cdots p_n$: or, on a

$$1 = a - p_1 p_2 \cdot p_n$$

et on en déduit que q divise 1, donc que $q = 1$, alors que q est premier. C'est impossible ! L'ensemble $\mathcal{P}$ ne peut donc pas être fini. □

Exemple 3.38. — Comme nouvelle illustration du raisonnement par l'absurde, montrons que $\sqrt{2}$ est irrationnel. Autrement dit, montrons l'assertion suivante :

Il est impossible qu'il existe deux entiers a et b de $\mathbb{N}^\star$ vérifiant $\sqrt{2} = \frac{a}{b}$.

Supposons qu'il existe deux entiers a et b de $\mathbb{N}^\star$ vérifiant $\sqrt{2} = \frac{a}{b}$. Écrivons la fraction $\frac{a}{b}$ sous forme irréductible : introduisons le nombre $d = \text{PGCD}(a, b)$, écrivons $a = d \cdot p$ et $b = d \cdot q$ où p et q sont des entiers n'ayant aucun diviseur commun à l'exception du nombre 1. On a alors $\sqrt{2} = \frac{a}{b} = \frac{p}{q}$. Mais alors $2 = \frac{p^2}{q^2}$, d'où

$$2q^2 = p^2.$$

Cela montre que p^2 est un nombre pair. Dans cette situation, le nombre p est nécessairement pair (voir l'exemple 3.16). Si nous écrivons $p = 2k$ où k est un entier naturel, nous obtenons alors

$$2q^2 = (2k)^2 = 4k^2, \quad \text{d'où} \quad q^2 = 2k^2$$

ce qui montre que q^2 est pair, donc que q est lui-même pair (toujours grâce à l'exemple 3.16).

Nous constatons donc que p et q, qui devaient n'avoir aucun diviseur commun excepté 1, sont nécessairement tous les deux pairs. Nous obtenons ainsi une contradiction. □

Ne pas abuser du raisonnement par l'absurde. — Le raisonnement par l'absurde peut être très utile. Il existe des situations où on ne peut pas faire sans lui. Mais il est, en quelque sorte, *indirect* : il montre qu'une chose est vraie en montrant que son contraire est impossible. Si un raisonnement plus direct est possible, il vaut mieux éviter de se « jeter » sur le raisonnement par l'absurde : par exemple, pour prouver

$$\exists x \in \mathbb{R} \ / \ x^2 - 4x + 3 < 0,$$

- on peut dire que si ce n'était pas le cas, alors la fonction $x \mapsto x^2 - 4x + 3$ serait un polynôme du second degré sans racine réelle, alors que son discriminant $4^2 - 4 \times 1 \times 3$ est positif, ce qui est absurde...
- mais on peut aussi, après une courte réflexion au brouillon sur les racines de l'équation du second degré, constater que pour $x = 2$, on a $x^2 - 4x + 3 < 0$.

La seconde méthode a l'avantage de fournir un exemple concret, alors que le raisonnement par l'absurde ne peut, par sa nature même, pas le faire.

7. Existence et unicité d'un objet, raisonnement par analyse-synthèse

Nous avons vu au §2.1 que pour montrer une affirmation du type $\exists x \in E \ / \ \mathcal{P}(x)$, il suffisait de trouver un exemple concret d'objet x vérifiant l'assertion. Mais cela peut être difficile !

Comment faire si aucun exemple ne vient en tête naturellement ? Un chemin possible est *d'analyser les contraintes sur* x qu'impose le fait que $\mathcal{P}(x)$ soit vrai.

Exemple 3.39. — Montrer qu'il existe un unique entier relatif n vérifiant : $\begin{cases} n^2 - 3n - 18 = 0, \\ n^2 + 3n - 4 > 0. \end{cases}$

- Commençons par remarquer qu'un tel n doit vérifier $n^2 - 3n - 18 = 0$. Or, l'équation $x^2 - 3x - 18 = 0$, d'inconnue réelle x, est une équation du second degré de discriminant $(-3)^2 - 4 \times 1 \times (-18) = 9 + 4 \times 18 = 81$. Ce discriminant étant positif, il existe deux réels x vérifiant $x^2 - 3x - 18 = 0$: il s'agit de $\frac{-(-3)-\sqrt{81}}{2} = -3$ et de $\frac{-(-3)+\sqrt{81}}{2} = 6$.

  On a donc nécessairement $n = -3$ ou $n = 6$. Mais pour $n = -3$, on a $n^2 + 3n - 4 = -4 < 0$, donc il ne reste plus comme possibilité que $n = 6$.
- Heureusement, pour $n = 6$, on a $n^2 + 3n - 4 = 50$: l'entier $n = 6$ est donc une solution du problème initial, et notre analyse montre que c'est la seule solution.

On remarquera que notre raisonnement comportait deux étapes :

- dans un premier temps, en *analysant les contraintes*, nous avons montré qu'il n'y avait que peu d'entiers qui pouvaient convenir ;
- dans un second temps, nous avons *testé les candidats issus de notre analyse*, et constaté qu'il y en avait un qui convenait (ici, un seul).

Raisonner par analyse-synthèse pour démontrer l'existence d'un objet vérifiant certaines propriétés, c'est
- *analyser les contraintes* imposées par ces propriétés pour en déduire des objets-candidats,
- puis observer si, parmi les candidats obtenus, certains conviennent (c'est l'étape de *synthèse*).

Exemple 3.40. — Montrer qu'il existe une unique fonction $f : [-1,1] \to \mathbb{R}$ vérifiant

$$\forall x \in \mathbb{R},\ f(\cos(x)) = \cos(2x). \tag{7.1}$$

- *Analyse.* Considérons une fonction $f : [-1,1] \to \mathbb{R}$ vérifiant la contrainte (7.1), et voyons si nous pouvons comprendre qui est $f(a)$ lorsque $a \in [-1,1]$.

  Soit a un élément de $[-1,1]$. Compte tenu des propriétés de la fonction cos, nous savons qu'il existe un réel x vérifiant $a = \cos(x)$. On a alors

  $$f(a) = f(\cos(x)) = \cos(2x).$$

  On rappelle maintenant une formule de trigonométrie vue en Terminale : $\cos(2x) = 1 - 2\cos^2(x)$. On a donc nécessairement

  $$f(a) = 1 - 2a^2.$$

  Mais alors, il n'y a qu'une possibilité pour f : c'est la fonction

  $$\begin{array}{rccc} \varphi & : & \mathbb{R} & \to & \mathbb{R} \\ & & a & \mapsto & 1-2a^2. \end{array} \tag{7.2}$$

- *Synthèse.* Montrons à présent que la fonction φ obtenue en (7.2) est effectivement solution du problème. Pour tout réel x, on a

  $$\varphi(\cos(x)) = 1 - 2\cos(x)^2 = \cos(2x);$$

  la fonction φ vérifie donc bien la condition espérée.

Exemple 3.41 **(Partie paire et impaire d'une fonction).** — Soit f une fonction de $\mathbb{R}$ dans $\mathbb{R}$. Montrer qu'il existe un unique couple (p,i) formé de deux fonctions de $\mathbb{R}$ dans $\mathbb{R}$ vérifiant :
- p est paire et i est impaire ;
- $f = p + i$.

Nous raisonnons à nouveau par analyse-synthèse :
- *Analyse.* Supposons qu'on dispose de deux fonctions p et i vérifiant les contraintes ci-dessus. Pour tout $x \in \mathbb{R}$, on a alors nécessairement

  $$f(x) \quad = \quad p(x) + i(x) \tag{7.3}$$

  et

  $$f(-x) \quad = \quad p(-x) + i(-x) = p(x) - i(x). \tag{7.4}$$

  En sommant les équations (7.3) et (7.4), on obtient une expression pour $p(x)$:

  $$p(x) = \frac{1}{2}\left(f(x) + f(-x)\right) \tag{7.5}$$

  et en prenant la différence de (7.3) et (7.4), on obtient cette fois une expression pour $i(x)$:

  $$i(x) = \frac{1}{2}\left(f(x) - f(-x)\right). \tag{7.6}$$

  Il y a donc, étant donné f, *une seule possibilité pour p* et *une seule possibilité pour i*.
- *Synthèse.* Considérons les fonctions p et i telles que, pour tout x de $\mathbb{R}$, les valeurs $p(x)$ et $i(x)$ soient données par les formules (7.5) et (7.6). On constate alors que
  — la fonction p est paire : pour tout $x \in \mathbb{R}$, on a $p(-x) = \frac{f(-x)+f(-(-x))}{2} = p(x)$,
  — la fonction i est impaire : pour tout $x \in \mathbb{R}$, on a $i(-x) = \frac{f(-x)-f(-(-x))}{2} = -i(x)$,

— et on a bien $f = p + i$, puisque pour tout $x \in \mathbb{R}$, on a $p(x) + i(x) = \frac{f(x)+f(-x)+f(x)-f(-x)}{2} = f(x)$.
Les fonctions p et i proposées conviennent donc, et ce sont les seules à pouvoir convenir.

Exercices du chapitre 3

Démonstration et utilisation d'assertions quantifiées. —

***Exercice 3.1* (Démontrer des assertions avec $\forall$ et $\exists$, I).** — ★☆☆
Démontrer ou infirmer les assertions suivantes.

1. $\exists x \in \mathbb{Z},\ \exists y \in \mathbb{N},\quad x \leq -y^2$
2. $\forall x \in \mathbb{Z},\ \exists y \in \mathbb{N},\quad x \leq -y^2$
3. $\forall y \in \mathbb{N},\ \exists x \in \mathbb{Z},\quad x \leq -y^2$
4. $\exists x \in \mathbb{Z},\ \forall y \in \mathbb{N},\quad x \leq -y^2$

***Exercice 3.2* (Démontrer des assertions avec $\forall$ et $\exists$, II).** — ★☆☆
Démontrer les assertions suivantes.

1. $\forall a \in \mathbb{N}^\star,\ \exists b \in \mathbb{N}^\star,\ \exists x \in \mathbb{R},\ e^{ax} > b$
2. $\exists a \in \mathbb{N},\ \forall b \in \mathbb{R},\ \exists x \in \mathbb{R},\ \ln(x^2 + |a-5|^2) < b$

***Exercice 3.3* (Utiliser des hypothèses avec des $\forall$ et $\exists$, I).** — ★☆☆
Dans cet exercice, on fixe deux réels a et b et on considère l'application

$$\begin{array}{rccc} f & : & \mathbb{R} & \to & \mathbb{R} \\ & & x & \mapsto & ax^2 + b. \end{array}$$

1. Montrer que si l'on a : $\forall x \in \mathbb{R}, f(x) = 0$, alors on a nécessairement $a = b = 0$.
2. Montrer que si l'on a : $\exists x \in \mathbb{R} \ / \ f(x) = 0$, alors on a nécessairement $ab \leq 0$.

***Exercice 3.4* (Utiliser des hypothèses avec des $\forall$ et $\exists$, II).** — ★★☆
Dans tout l'exercice, on fixe une fonction $f : \mathbb{R}_\star^+ \to \mathbb{R}_\star^+$ et on suppose que f vérifie la propriété suivante :

$$\forall \varepsilon > 0,\ \exists x \in \mathbb{R}_+^\star,\quad 0 < f(x) < \varepsilon. \tag{$\star$}$$

1. On introduit la fonction $g : \mathbb{R}_\star^+ \to \mathbb{R}_\star^+$ définie par : $\forall x \in \mathbb{R}_\star^+,\ g(x) = 5f(x)^2$.
   Démontrer que g vérifie la propriété suivante :
   $$\forall \varepsilon > 0,\ \exists x \in \mathbb{R}_+^\star,\quad 0 < g(x) < \varepsilon.$$
2. On introduit la fonction $h : \mathbb{R}_\star^+ \to \mathbb{R}_\star^+$ définie par : $\forall x \in \mathbb{R}_\star^+,\ h(x) = f(x^2)$.
   Démontrer que h vérifie la propriété suivante :
   $$\forall \varepsilon > 0,\ \exists x \in \mathbb{R}_+^\star,\quad 0 < h(x) < \varepsilon.$$
3. On introduit la fonction $\varphi : \mathbb{R}_\star^+ \to \mathbb{R}_\star^+$ définie par : $\forall x \in \mathbb{R}_+^\star,\ \varphi(x) = \frac{1}{f(\sqrt{x})}$.
   Démontrer que φ vérifie la propriété suivante :
   $$\forall A > 0,\ \exists x \in \mathbb{R}_+^\star,\quad \varphi(x) > A.$$

Implications et équivalences. —

***Exercice 3.5* (Passer ou non par la contraposée...)** —

1. Soit x un nombre réel.
   (a) ★☆☆ Montrer que si $x^3 = 2$ alors $x < 2$.
   (b) ★☆☆ Montrer que si $x + 1$ est le carré d'un entier impair, alors x est un entier multiple de 4.
2. Soient a et b deux nombres réels vérifiant $a \leq b$.
   (a) ★☆☆ Montrer l'implication suivante : $(b - a > 0 \implies \exists \varepsilon > 0, (b-a)^2 > \varepsilon)$.
   (b) ★★☆ Montrer l'implication suivante : $(\forall \varepsilon > 0, \exists x \in \mathbb{R}, |a - x| + |b - x| < \varepsilon) \implies a = b$.

3. ★☆☆ Dans cette question, on fixe un entier $n \in \mathbb{N}^\star$, un nombre $M > 0$, et des nombres réels $x_1, \dots, x_n$. Montrer que si $x_1 + \cdots + x_n = M$, alors il existe un indice $i \in \{1, \dots, n\}$ tel que $x_i \geq \frac{M}{n}$.
4. ★★☆ Dans cette question, on fixe une fonction $f : \mathbb{R} \to \mathbb{R}$. Montrer que si f est paire et croissante, alors f est constante.

***Exercice 3.6* (Quelques équivalences à montrer).** — ★☆☆

1. Soient x et y deux réels. Montrer que $x^2 + y^2 = 0$ si et seulement si $x = y = 0$.
2. Soient x et y deux réels. Montrer que $xy + 2x + 2y = -4$ si et seulement si $x = -2$ ou $y = -2$.

Récurrences. —

***Exercice 3.7* (Récurrences simples).** — ★☆☆

1. Montrer que pour tout entier $n \in \mathbb{N}^\star$, on a $2^n + 3^n \leq 5^n$.
2. Montrer que pour tout entier $n \geq 4$, on a $(n!) \geq 2^n$.
3. Montrer que pour tout entier $n \in \mathbb{N}^\star$, on a $\sum_{k=1}^{n} k^3 = \left(\frac{n(n+1)}{2}\right)^2$.

***Exercice 3.8* (Récurrences fortes).** — ★☆☆ — *Les deux questions sont indépendantes*

1. On définit une suite $(F_n)_{n\in\mathbb{N}}$ de la manière suivante : $F_0 = 0$, $F_1 = 1$ et pour tout $n \in \mathbb{N}$, on définit $F_{n+2} = F_{n+1} + F_n$.
   (a) Calculer F_n pour $n \leq 5$.
   (b) Notons $\varphi = \frac{1+\sqrt{5}}{2}$ et $\varphi' = \frac{1-\sqrt{5}}{2}$. Montrer que pour tout $n \in \mathbb{N}$, on a $F_n = \frac{1}{\sqrt{5}}(\varphi^n - (\varphi')^n)$.
2. Montrer que pour tout entier $n \in \mathbb{N}^\star$, il existe des entiers naturels p et q vérifiant : $n = 2^p(2q + 1)$.

***Exercice 3.9* (L'affaire des crayons de couleur).** — ★★☆

On considère des boîtes de crayons de couleurs. Pour tout entier naturel $n \geq 1$, notons $\mathcal{P}(n)$ l'affirmation suivante :

Dans une boite quelconque de n crayons de couleurs, tous les crayons sont de la même couleur

Le raisonnement suivant prouve-t-il que $\mathcal{P}(n)$ est vraie pour tout entier naturel $n \geq 1$? Sinon, où est l'erreur ?

« Dans une boîte un seul crayon, les crayons ont bien sûr tous la même couleur. Donc $\mathcal{P}(1)$ est vraie. Soit maintenant n dans $\mathbb{N}^*$. Prenons une boîte de $n+1$ crayons. Si l'on enlève provisoirement un crayon, il reste n crayons qui, d'après $\mathcal{P}(n)$, sont tous de la même couleur. Remettons le crayon précédemment écarté et enlevons un autre crayon. Toujours d'après $\mathcal{P}(n)$, les n crayons restants sont tous de la même couleur. Mais comme les crayons qui ne sont pas sortis de la boite ont tous la même couleur , il s'ensuit que les $n+1$ crayons ont même couleur. Donc $\mathcal{P}(n+1)$ est vraie.
Ainsi, par récurrence, $\mathcal{P}(n)$ est vraie pour tout $n \geq 1$. »

Question subsidiaire : pour quelles valeurs de n l'implication $\mathcal{P}(n) \implies \mathcal{P}(n+1)$ est-elle vraie ?

***Exercice 3.10* (Bien choisir l'hypothèse de récurrence).** — ★★★

Dans cet exercice, on considère une fonction $g : \mathbb{R}_\star^+ \to \mathbb{R}$ et on suppose que pour tout $\varepsilon > 0$, il existe une constante $C_\varepsilon > 0$ qui vérifie :

$$\forall x \in \mathbb{R}_\star^+, \quad 0 \leq g(x) \leq C_\varepsilon x^\varepsilon.$$

On introduit, pour chaque $n \in \mathbb{N}$, une fonction $f_n : \mathbb{R}_\star^+ \to \mathbb{R}$ de manière suivante : f_0 est la fonction g, puis f_1 est la fonction $\sqrt{g}$, puis pour tout $n \in \mathbb{N}$, on a

$$f_{n+2} = (f_{n+1} + f_n)^2.$$

Démontrer que pour tout $n \in \mathbb{N}$ et pour tout $\varepsilon > 0$, il existe une constante $T_{\varepsilon,n}$ telle que la propriété suivante soit vérifiée :

$$\forall x \in \mathbb{R}_\star^+, \quad f_n(x) \leq T_{\varepsilon,n} x^\varepsilon.$$

Raisonnement par l'absurde. —

***Exercice 3.11* (Raisonnement par l'absurde, I).** — ★☆☆
Soit n un entier naturel non nul. Montrer qu'il est impossible que n^2+1 soit le carré d'un entier.

***Exercice 3.12* (Raisonnement par l'absurde, II).** — ★★☆

1. *Dans ces questions, on pourra s'inspirer de l'exemple 3.38.*
   (a) Montrer que $\sqrt{3}$ est irrationnel.
   (b) Montrer que le nombre $\frac{\ln 3}{\ln 2}$ est irrationnel.
2. *Ces questions sont de style différent.*
   (a) Montrer que si a, b, a' et b' sont quatre entiers et si $a+b\sqrt{2}=a'+b'\sqrt{2}$, alors $a=a'$ et $b=b'$.
   (b) Montrer que $\sqrt{2}+\sqrt{3}$ est irrationnel.

***Exercice 3.13* (Raisonnement par l'absurde, III).** — ★★☆
On fixe un entier $n\in\mathbb{N}^\star$ et on considère $(n+1)$ points $x_1,\dots,x_n,x_{n+1}$ appartenant tous à l'intervalle $[0,1]$. Montrer l'assertion suivante :

$$\exists (i,j)\in\{1,\dots,n+1\}^2 \quad : \quad i\neq j \text{ et } |x_i-x_j|\leq \frac{1}{n}.$$

Analyse-synthèse. —

***Exercice 3.14* (Analyse-synthèse, I).** — ★☆☆

1. Existe-t-il un entier $n\in\mathbb{Z}$ vérifiant $n^2+n-6=0$ et $2n^3+3n^2-4n<0$?
2. Trouver tous les réels $x\geq 0$ vérifiant : $\sqrt{x+15}-\sqrt{x}=\sqrt{15}$.
3. Existe-t-il une fonction $f:\mathbb{R}\to\mathbb{R}$ vérifiant : $\forall x\in\mathbb{R},\ f(\cos(x))=\sin(x)$?

***Exercice 3.15* (Analyse-synthèse, II).** — ★★☆ — *Les deux parties sont indépendantes.*

1. Dans cette question,
   - on travaille dans l'ensemble $E=\mathcal{F}(\mathbb{R},\mathbb{R})$ des fonctions de $\mathbb{R}$ dans $\mathbb{R}$,
   - on note H le sous-ensemble $\{f\in E\ /\ f(0)=0\}$ de E,
   - et on note c la fonction de $\mathbb{R}$ dans $\mathbb{R}$ définie par : $\forall x\in\mathbb{R},\ c(x)=1$.

   Montrer que pour toute fonction f de E, il existe un unique couple $(h,\alpha)\in H\times\mathbb{R}$ vérifiant $f=\alpha c+h$.
2. Dans cette question, on définit l'ensemble $A=\mathbb{R}\setminus\{-1,1,2,5\}$ et on considère la fonction $f:A\to\mathbb{R}$ définie par
   $$\forall x\in A,\quad f(x)=\frac{1}{(x+1)(x-1)(x-2)(x-5)}.$$
   Montrer qu'il existe un unique quadruplet $(a,b,c,d)\in\mathbb{R}^4$ vérifiant :
   $$\forall x\in A,\quad f(x)=\frac{a}{x+1}+\frac{b}{x-1}+\frac{c}{x-2}+\frac{d}{x-5}.$$
   On pourra commencer par évaluer $(x+1)f(x)$ en un réel x bien choisi.

***Exercice 3.16* (Analyse-synthèse, III).** — ★★★
Dans cet exercice, on détermine toutes les fonctions $f:\mathbb{R}\to\mathbb{R}$ qui sont deux fois dérivables et qui vérifient la propriété suivante :

$$\forall x\in\mathbb{R},\ \forall y\in\mathbb{R},\quad f(x+y)+f(x-y)=2\left(f(x)+f(y)\right). \tag{$\star$}$$

1. Considérons une fonction f solution.
   (a) Déterminer $f(0)$ et montrer que f est paire.

(b) Montrer que la fonction f'' est constante.
On pourra fixer y et dériver deux fois par rapport à x, puis fixer x et dériver deux fois par rapport à y.

2. Conclure.

CHAPITRE 4

ARITHMÉTIQUE DANS $\mathbb{Z}$

1. Divisibilité et division euclidienne

1.1. Notion de diviseur ; propriétés élémentaires. —

Définition 4.1 – Divisibilité dans $\mathbb{Z}$

Soient a et b deux entiers relatifs. On dit que b *divise* a, et on note $b|a$, lorsque
- b n'est pas nul
- et il existe un entier $k \in \mathbb{Z}$ vérifiant $a = kb$.

Lorsque b divise a, on dit aussi que b est un *diviseur* de a, ou encore que a est un *multiple* de b.

Remarque 4.2. — Si a est un entier relatif, alors 1 et -1 sont toujours des diviseurs de a. De plus, si b est un diviseur de a, alors $-b$ est aussi un diviseur de a.

Parmi les propriétés élémentaires d'usage constant, relevons les suivantes :

- *Diviseurs et combinaisons.* Soient a_1, a_2, b des entiers relatifs avec $b \neq 0$.
  Si $b|a_1$ et $b|a_2$, alors pour tous u_1, u_2 de $\mathbb{Z}$, on a
  $$b \,|\, (u_1 a_1 + u_2 a_2)\,.$$
- *Taille des diviseurs.* Si a et b sont positifs et non-nuls et si b divise a, alors $b \leq a$.
- *Entiers se divisant l'un l'autre.* Si a divise b et b divise a, alors on a $a = \pm b$.

Démonstration. —
- Si $b|a_1$ et $b|a_2$, alors il existe des entiers k_1, k_2 vérifiant $a_1 = k_1 b$ et $a_2 = k_2 b$, et alors pour tous u_1, u_2 de $\mathbb{Z}$, on a $u_1 a_1 + u_2 a_2 = (u_1 k_1 + u_2 k_2) b$, ainsi $u_1 a_1 + u_2 a_2$ est multiple de b.
- Soient a et b deux entiers positifs et non-nuls. Supposons que b divise a : il existe donc un entier $k \in \mathbb{Z}$ tel que $a = bk$. Compte tenu des signes de a et b, un tel k vérifie nécessairement $k > 0$, et comme c'est un entier, on a en fait $k \geq 1$. De $a = kb$ et $k \geq 1$, comme a et b sont positifs, on déduit bien $a \geq b$.
- Si a divise b et b divise a, alors $|a|$ divise $|b|$ et $|b|$ divise $|a|$ (voir la remarque 4.2). Avec la propriété que nous venons de voir pour les entiers positifs, on a donc $|b| \leq |a|$ et $|a| \leq |b|$; c'est donc que $|a| = |b|$, autrement dit, que a et b sont soit égaux, soit opposés.

□

1.2. Division euclidienne. —

Théorème 4.3 – Existence et unicité de la division euclidienne dans $\mathbb{N}$

Soient a et b deux entiers naturels avec $b \neq 0$. Il existe un unique couple (q, r) d'entiers naturels vérifiant

$$a = bq + r \quad \text{et} \quad 0 \leq r < b.$$

Démonstration. —

- *Unicité sous réserve d'existence.* Supposons qu'il existe deux couples (q_1, r_1) et (q_2, r_2) vérifiant :

$$a = bq_1 + r_1 \text{ et } 0 \leq r_1 < b \quad \text{mais aussi} \quad a = bq_2 + r_2 \text{ et } 0 \leq r_2 < b$$

On a alors $bq_1 + r_1 = bq_2 + r_2$, d'où

$$b(q_2 - q_1) = r_1 - r_2, \tag{1.1}$$

ce qui montre que $r_1 - r_2$ est multiple de b.

Or, $(r_1 - r_2)$ est un entier strictement compris entre $-b$ et b : en effet, on a $r_1 < b$ et $r_2 \geq 0$, donc $r_1 - r_2 < b$, tandis que $r_1 \geq 0$ et $-r_2 > -b$, d'où $r_1 - r_2 > -b$.

Le seul multiple de b qui soit strictement compris entre $-b$ et b est $0 \times b = 0$. On en conclut que $r_2 - r_1 = 0$, puis avec (1.1) que $q_1 - q_2 = 0$. On a donc bien $(q_1, r_1) = (q_2, r_2)$.

- *Existence.*

En observant les contraintes que doivent vérifier les q et r dont on doit prouver l'existence, on peut faire la remarque suivante : l'entier q doit être tel bq ne dépasse pas a (puisqu'on veut $a = bq + r$ avec $r \geq 0$, mais tel que $bq + b$ dépasse a (puisqu'on veut $r < b$ et donc $bq + b > bq + r = a$).

Introduisons l'ensemble

$$E = \{k \in \mathbb{N} \ / \ bk > a\}.$$

Il s'agit d'une partie de $\mathbb{N}$; de plus, cette partie est non vide, puisque pour $k = a + 1$, on a $bk = ab + a \geq ab \geq b$ (la première inégalité parce que $a \geq 0$, la seconde car $b \geq 1$).

D'après l'axiome du plus petit élément, l'ensemble E admet un plus petit élément. Notons q l'entier tel que ce plus petit élément soit égal à $q + 1$ ce plus petit élément. On a alors
— $q + 1 \in E$, donc $b(q + 1) > a$, autrement dit $a - bq < b$;
— $q \notin E$, donc $bq \leq a$, autrement dit $a - bq \geq 0$
Si nous définissons $r = a - bq$, on a alors $a = bq + r$ et $0 \leq r < b$, comme espéré.

□

Exemple 4.4. — Pour obtenir la division euclidienne de 19 par 5, il suffit de constater que $19 = 3 \times 5 + 4$ et que $0 \leq 4 < 5$; par l'unicité dans le théorème ci-dessus, le reste de la division est nécessairement 4 et le quotient est nécessairement 3.

Théorème et définition 4.5 – Division euclidienne, cas des entiers relatifs

Soient a et b deux entiers relatifs. Il existe un unique couple (q, r) de $\mathbb{Z}^2$ vérifiant

$$a = bq + r \quad \text{et} \quad 0 \leq r < |b|.$$

Exemple 4.6. — Pour obtenir la division euclidienne de -19 par 5, il suffit de constater que $-19 = -20 + 1 = -4 \times 5 + 1$; le quotient est donc -4 et le reste est 1.

De même, pour obtenir la division euclidienne de -33, il suffit d'écrire $-33 = -35 + 2 = -7 \times 5 + 2$: le quotient est -7 et le reste est 2.

On remarquera ici le lien entre le reste dans la division d'un entier a par 5 et le reste de celle de $-a$.

Remarque 4.7. — Si a et b sont deux entiers relatifs, alors on a l'équivalence suivante :

b divise a $\iff$ le reste dans la division euclidienne de a par b est zéro.

Démonstration du théorème 4.5 (peut être omise en première lecture). — Concernant l'unicité sous réserve d'existence, la démonstration vue au théorème 4.3 s'applique avec pour seule modification d'y remplacer b par $|b|$. Nous prouvons donc ici l'existence.

Distinguons les différents cas possibles pour les signes de a et de b :

- Si $a \geq 0$ et $b > 0$, nous avons déjà prouvé le théorème.
- Supposons $a \leq 0$ et $b > 0$. L'entier $-a$ est positif, on peut donc considérer la division euclidienne de $-a$ par b : il existe deux entiers q' et r' vérifiant

$$-a = bq' + r' \quad \text{et} \quad 0 < r' < b.$$

Nous en déduisons

$$a = b(-q') + (-r').$$

Cette écriture ne peut pas fournir la division euclidienne de a par b : l'entier $-r'$ est négatif, alors que le reste cherché doit être entre 0 et b. Mais $-r'$ est compris entre $-b$ et 0 : en écrivant

$$a = b(-q') - b + b - r' = b(-q' + 1) + (b - r')$$

on obtient une écriture où $(b - r')$ est compris entre 0 et b, et n'est égal à b que si $r' = 0$.

Si $r' \neq 0$, en choisissant $r = b - r'$ et $q = -q' + 1$, on obtient bien

$$a = bq + r \quad \text{et} 0 \leq r < b$$

tandis que si $r' = 0$, en choisissant $r = 0$ et $q = -q'$, on a aussi $a = bq + r$ avec $0 \leq r < b$.

- Supposons $a \geq 0$ et $b < 0$. En effectuant la division euclidienne de a par $(-b)$, on peut trouver deux entiers (q', r') vérifiant

$$a = b(-q') + r' \quad \text{avec} \quad 0 \leq r' < -b.$$

Mais ici $-b = |b|$; si on choisir $q = -q'$ et $r = r'$, on a bien

$$a = bq + r \quad \text{avec} \quad 0 \leq r < |b|.$$

- Si $a \leq 0$ et $b < 0$, on s'inspire des deux cas précédents. En effectuant la division euclidienne de $-a$ par $-b$, on obtient un couple (q', r') d'entiers vérifiant

$$-a = -bq' + r' \quad \text{avec} \quad 0 \leq r' < -b;$$

si $r' \neq 0$ on choisit alors $r = b - r'$ et $q = q' - 1$ et $r = b - r'$, tandis que si $r' = 0$ on choisit simplement $q = q'$; dans les deux cas on obtient

$$a = bq + r \quad \text{avec} \quad 0 \leq r < b$$

comme espéré.

□

2. Congruences

Définition 4.8 – Congruence modulo n

Fixons un entier $n \neq 0$ et deux entiers a et b. On dit que a et b sont *congrus modulo* n, et on note $a \equiv b \mod n$, lorsque $a - b$ est un multiple de n.

Exemple 4.9. — Un entier a est pair si et seulement si on a la congruence $a \equiv 0 \mod 2$, et il est impair si et seulement si on a la congruence $a \equiv 1 \mod 2$.

Remarque 4.10. — Fixons un entier $n_0 \in \mathbb{N}^\star$.

- Si $a \in \mathbb{N}$ et si r est le reste de la division euclidienne de a par n_0, alors on a $a \equiv r \mod n_0$.
- De plus, l'unicité de la division euclidienne assure qu'il s'agit du seul entier compris entre 1 et $(n_0 - 1)$ qui soit congru à a modulo n_0.
- En fait, si a et b sont deux entiers relatifs, alors on a l'équivalence suivante :

$$(a \equiv b \mod n_0) \iff (a \text{ et } b \text{ ont le même reste dans la division euclidienne par } n_0).$$

Proposition 4.11 – Compatibilité entre congruences et addition ou multiplication

Soit n un entier naturel non nul. Soient a, a', b, b' quatre entiers relatifs.

- *Si $a \equiv a' \mod n$ et $b \equiv b' \mod n$, alors $a + b \equiv a' + b' \mod n$.*
- *Si $a \equiv a' \mod n$ et $b \equiv b' \mod n$, alors $ab \equiv a'b' \mod n$.*

Une conséquence de cet énoncé est que les congruences sont compatibles aussi avec les *soustractions* : si $b \equiv b' \mod n$, alors d'après le second point on a aussi $-b \equiv -b' \mod n$, et donc $a - b \equiv a' - b' \mod n$.

Remarque 4.12. — Malgré son apparence anodine, la proposition ci-dessus est un outil extrêmement puissant pour simplifier des calculs arithmétiques.

Montrons par exemple que pour tout entier naturel n non nul, le nombre $2^{3n} - 1$ est divisible par 7.

Soit $n \in \mathbb{N}$. On part du fait que $2^{3n} = (2^3)^n = 8^n$. Or $8 \equiv 1 \mod 7$, donc (en appliquant la règle de multiplicativité)

$$8^n \equiv 1^n \equiv 1 \mod 7$$

si bien que

$$8^n - 1 \equiv 0 \mod 7$$

ce qui était la conclusion souhaitée. Nous venons de montrer avec des calculs très simples que, par exemple, $4089 = 8^4 - 1$ et $262137 = 8^6 - 1$ sont divisibles par 7.

Démonstration de la proposition 4.11. —

- Montrer $(a + b) \equiv (a' + b') \mod n$, revient à montrer que $(a + b) - (a' + b')$ est divisible par n. Mais cet entier est égal à $(a - a') + (b - b')$; comme $a \equiv a' \mod n$ et $b \equiv b' \mod n$, il s'agit de la somme de deux entiers divisibles pas n, il est donc divisible par n.
- Pour montrer $ab \equiv a'b' \mod n$, nous devons montrer que $ab - a'b'$ est divisible par n. Pour cela, on réécrit cet entier de la manière suivante :

$$\begin{aligned} ab - a'b' &= ab \; \textcolor{red}{-ab' + ab'} - a'b' \\ &= a\,(b - b') - (a - a')\,b'. \end{aligned}$$

Puisque $b - b'$ est divisible par n, l'entier $a(b - b')$ l'est aussi ; de même $(a - a')b'$ est divisible par n, et donc $aa' - bb'$ est divisible par n, ce qu'il fallait démontrer.

□

3. Pgcd et ppcm

3.1. Pgcd de deux entiers. —

3.1.1. *Définition et propriétés élémentaires.* — Rappelons la définition, vue dans le chapitre précédent (exemple 3.35), du PGCD de deux entiers :

Définition 4.13 – PGCD de deux entiers relatifs

Soient a et b deux entiers relatifs, non tous les deux nuls. Le *plus grand diviseur commun* de a et b, noté $\text{PGCD}(a,b)$, est le plus grand entier naturel k qui divise à la fois a et b.

Remarque 4.14. — L'exemple 3.35 était formulé pour a et b positifs. Mais la démonstration de l'existence du PGCD peut s'appliquer, avec très peu de modifications, au cas où l'un des deux entiers a, b est négatif. Chercher ces modifications est un bon exercice.

Parmi les propriétés élémentaires du PGCD de deux entiers a et b, relevons les deux suivantes :

- Pour tout entier $k \in \mathbb{Z}$, on a $\text{PGCD}(ka, kb) = |k| \cdot \text{PGCD}(a,b)$
- Si a divise b, alors $\text{PGCD}(a,b) = |a|$.

3.1.2. *Relation de Bézout et propriété universelle.* —

La définition du PGCD comme « plus grand diviseur commun » est intuitivement très claire. Cependant, elle peut être délicate à manier en pratique : comme nous l'avons vu, la définition rigoureuse passe par la notion de plus grand élément d'une partie de $\mathbb{N}$, et elle est donc un peu technique.

Pour raisonner sur le PGCD sans devoir passer par la définition, le fait suivant s'avère souvent très pratique :

Proposition 4.15 – Relation de Bézout

Soient a et b deux entiers relatifs. Notons d le PGCD de a et b.
Il existe deux entiers relatifs u et v vérifiant :

$$au + bv = d$$

La démonstration qu'on va voir est théorique ; nous verrons plus loin (exemple 4.1 et exercice 4.12) comment trouver en pratique les couples (u,v) vérifiant $au + bv = d$.

Démonstration. — Considérons l'ensemble des nombres entiers positifs pouvant s'écrire comme « combinaison » de a et de b, en introduisant

$$\mathcal{I} = \left\{ k \in \mathbb{N}^\star \quad / \quad \exists (u,v) \in \mathbb{Z}^2, \quad k = au + bv \right\}.$$

Ce que nous devons montrer, c'est que d appartient à $\mathcal{I}$.

Que sait-on de $\mathcal{I}$? C'est une partie de $\mathbb{N}$, qui est non-vide puisqu'elle contient a. Grâce à l'axiome **??**, nous savons que $\mathcal{I}$ admet un plus petit élément. Notons μ ce petit élément.

Nous allons montrer qu'on a en fait $\mu = d$.

(i) Vérifions que μ divise a et b. Concentrons-nous sur a et montrons que le reste de la division euclidienne de a par μ est nul. Partons du fait que μ est un élément de $\mathcal{I}$: il existe donc u et v vérifiant

$$\mu = au + bv \tag{3.1}$$

Si nous écrivons la division euclidienne de a par μ sous la forme $a = q\mu + r$ avec $q \in \mathbb{Z}$ et $0 \leq r < \mu$, alors nous obtenons la formule suivante pour le reste r :

$$\begin{aligned} r &= a - q\mu \\ &= a - q\,(au + bv) \\ &= a\,(1 - qu) + b\,(qv)\,. \end{aligned}$$

Si r est non-nul, c'est donc qu'il appartient à $\mathcal{I}$; or $r < \mu$ et μ est le plus petit élément de $\mathcal{I}$ − il est donc impossible que r soit non-nul.

Nous avons donc bien $\mu | a$. Le même raisonnement permet de montrer que μ divise b.

(ii) De plus, si un entier positif k divise a et b, d'après la formule (3.1), il divise aussi μ. Mais alors $k \leq \mu$.

Ainsi, l'entier μ est un diviseur de a et b, et c'est le plus grand diviseur positif de a et b. On a donc bien $\mu = \text{PGCD}(a, b)$. □

Mentionnons une deuxième propriété, théorique mais très utile, du PGCD :

Proposition 4.16 – Propriété universelle du PGCD

Soient a et b deux entiers relatifs.

1. *Si $d = \text{PGCD}(a, b)$, alors*
   - *(i) d divise a et b*
   - *(ii) pour tout $k \in \mathbb{Z}$, si k divise a et b, alors k divise d*
2. *Si un entier δ vérifie (i) et (ii) ci-dessus, alors nécessairement $\delta = \text{PGCD}(a, b)$.*

Remarque 4.17. —
- La partie la plus concrète de cette proposition est 1.(*ii*) : elle signifie que si k est un diviseur commun à a et b, non seulement c'est un entier inférieur ou égal à $\text{PGCD}(a, b)$, mais c'est en fait un diviseur de $\text{PGCD}(a, b)$
- La propriété 2, plus abstraite, dit que le PGCD est le seul entier dont les diviseurs soient exactement les diviseurs communs de a et de b. Elle est souvent utile dans des discussions théoriques.

Démonstration de la propriété universelle. —

1. Notons $d = \text{PGCD}(a, b)$.
   (i) Le fait que d divise a et b fait partie de la définition du PGCD.
   (ii) Considérons maintenant un entier relatif k qui divise à la fois a et b, et rappelons que $d = \text{PGCD}(a, b)$ vérifie une relation de Bézout : il existe deux entiers u et v tels que
   $$d = au + bv.$$
   Mais alors, k divise a et b, donc divise aussi $au + bv$, et k divise d.
2. Si un entier δ vérifie (i) et (ii) ci-dessus, alors c'est un diviseur commun à a et à b, donc par définition du PGCD, on a $\delta \leq \text{PGCD}(a, b)$.
   De plus, l'entier $k = \text{PGCD}(a, b)$ est un diviseur commun à a et b, donc si δ vérifie la propriété (ii), on a $k | \delta$, et donc $k \leq \delta$, si bien que $\text{PGCD}(a, b) \leq \delta$

□

3.1.3. *Algorithme d'Euclide pour le calul du* PGCD *de deux entiers.* —

Proposition 4.18 – Propriété des restes pour le PGCD

Soient a et b deux entiers relatifs avec $b \neq 0$. Notons r le reste dans la division euclidienne de a par b. On a alors

$$\text{PGCD}(a, b) = \text{PGCD}(b, r)$$

Démonstration. — Notons q le quotient dans la division euclidienne de a par b ; on a donc

$$a = bq + r, \quad \text{ou encore} \tag{3.2}$$

$$r = a - bq. \tag{3.3}$$

Notons $d_1 = \text{PGCD}(a, b)$ et $d_2 = \text{PGCD}(a, r)$.

- Montrons que d_1 divise d_2. On sait que d_1 divise a et b ; d'après (3.3), on a donc aussi $d|r$; l'entier d est donc un diviseur commun de b et de r ; d'après la propriété universelle du PGCD, il divise $\text{PGCD}(b, r) = d_2$.
- Montrons à présent que d_2 divise d_1. Comme d_2 divise b et r, d'après (3.2) il divise aussi a ; c'est donc un diviseur commun à a et b, donc un diviseur de $\text{PGCD}(a, b) = d_1$.

Comme d_1 et d_2 sont positifs, on obtient $d_1 = d_2$ (voir le §1.1) □

Proposition 4.19 – Algorithme d'Euclide

Soient a et b deux entiers relatifs avec $b \neq 0$. On travaille avec deux variables α et β et on procède comme suit.

- Initialisation : *on commence avec $\alpha = a$ et $\beta = b$.*
- Boucle : *tant que $\beta \neq 0$, on effectue les deux substitutions*

$$\alpha \leftarrow \beta$$

$$\beta \leftarrow \text{ le reste de la division euclidienne de } \alpha \text{ par } \beta$$

- Conclusion : *on s'arrête quand $\beta = 0$.*

Le contenu de α donne alors le PGCD *de a et b.*

Justification de l'algorithme. — Notons d le PGCD de a et b.

- On remarque que d'après la propriété des restes ci-dessus, à chaque étape de l'algorithme on a $\text{PGCD}(\alpha, \beta) = d$.
- De plus, à chaque étape de l'algorithme, β diminue d'au moins une unité, puisque dans une division euclidienne $\alpha = \beta q + r$, le reste r vérifie $0 \leq r < \beta$. Partant de $\beta = b$, on a donc la certitude d'arriver à $\beta = 0$ en au plus b étapes.
- Enfin, une fois qu'on a $\beta = 0$, on a $\text{PGCD}(\alpha, \beta) = \alpha$; puisque $\text{PGCD}(\alpha, \beta) = d$ à chaque étape de l'algorithme, c'est qu'à l'étape terminale on a $\alpha = d$.

□

Exemple 4.20. — Choisissons $a = 48$ et $b = 30$, et appliquons l'algorithme d'Euclide.

Initialisation :	$\alpha = 48$	$\beta = 30$.	Division euclidienne de α par β : $48 = 1 \cdot 30 + 18$
Étape 1 :	$\alpha = 30$	$\beta = 18$.	Division euclidienne de α par β : $30 = 1 \cdot 18 + 12$
Étape 2 :	$\alpha = 18$	$\beta = 12$.	Division euclidienne de α par β : $18 = 1 \cdot 12 + 6$
Étape 3 :	$\alpha = 12$	$\beta = 6$.	Division euclidienne de α par β : $12 = 2 \cdot 6 + 0$
Conclusion :	$\alpha = 6$	$\beta = 0$.	Le pgcd des deux entiers de départ est 6 !

3.2. Pgcd d'une famille d'au moins 3 entiers. —

Définition 4.21 – Pgcd d'une famille d'entiers

Soient n un entier de $\mathbb{N}^\star$ et $(a_1, \dots, a_n)$ une famille de n entiers naturels.
On appelle *plus grand diviseur commun* de la famille $(a_1, \dots, a_n)$, et on note $\text{PGCD}(a_1, \dots, a_n)$, le plus grand entier positif qui divise chacun des a_i, $i \in \{1, \dots, n\}$.

L'existence de ce plus grand diviseur commun est justifiée par le fait que l'ensemble

$$E = \{k \in \mathbb{N}^\star \ / \ \forall i \in \{1, \dots, n\}, \quad k | a_i\}$$

est une partie de $\mathbb{N}$, non vide puisqu'elle contient 1, et majorée (par exemple par a_1).

Proposition 4.22 – Relation de Bézout dans le cas le plus général

Soient n un entier de $\mathbb{N}^\star$ et $(a_1, \dots, a_n)$ une famille de n entiers naturels.
Notons $d = \text{PGCD}(a_1, \dots, a_n)$; il existe des entiers $u_1, \dots, u_n$ vérifiant

$$d = u_1 a_1 + \cdots + u_n a_n.$$

Indication sur la démonstration. — Pour obtenir une démonstration de ce résultat, on peut imiter le cas de deux entiers et introduire l'ensemble

$$\mathcal{I} = \{k \in \mathbb{N}^\star \ / \ \exists (u_1, \dots, u_n) \in \mathbb{Z}^n \ : \quad k = u_1 a_1 + \cdots + u_n a_n\},$$

constater que c'est une partie non vide de $\mathbb{N}$, puis montrer que son plus petit élément n'est autre que le PGCD de $a_1, \dots, a_n$. □

La définition et le résultat ci-dessus généralisent bien sûr le cas de deux entiers. Cependant, on peut remarquer que le cas de plus de deux entiers peut se *ramener* au cas de deux entiers, grâce au résultat suivant.

Proposition 4.23 – Formule ramenant au cas de deux entiers

Soient n un entier de $\mathbb{N}^\star$ et $(a_1, \dots, a_n)$ une famille de n entiers naturels. On a l'égalité

$$\text{PGCD}(a_1, a_2, \dots, a_n) = \text{PGCD}\left(a_1, \text{PGCD}(a_2, \dots, a_n)\right).$$

Ainsi, pour calculer le PGCD de trois entiers a, b, c, on peut d'abord calculer $\text{PGCD}(b, c)$ (par exemple par l'algorithme d'Euclide), puis calculer $\text{PGCD}(a, \delta)$ (à nouveau par l'algorithme d'Euclide).

Démonstration de la Proposition. — Utilisons la propriété universelle du PGCD dans le cas de deux entiers. Notons δ le PGCD de $a_2, \dots, a_n$: nous devons montrer que le nombre $\Delta = \text{PGCD}\left(a_1, \dots, a_n\right)$ est égal à $\text{PGCD}(a_1, \delta)$.

(i) D'abord, le nombre Δ divise a_1 ; de plus, c'est aussi un diviseur commun à $a_2, \dots, a_n$, donc (par la propriété universelle) c'est un diviseur de leur PGCD δ. Par conséquent, Δ est un diviseur commun à a_1 et δ.

(ii) Ensuite, si k est un entier qui divise a_1 et δ, alors il divise tous les a_i, $i \in \{1, \dots, n\}$; en utilisant une relation de Bézout comme dans la proposition précédente, on constate donc que k divise Δ.

L'entier Δ remplit donc les deux conditions de la propriété universelle du PGCD de δ et a_1, on a donc $\Delta = \text{PGCD}(a_1, \delta)$, comme espéré.

□

3.3. Ppcm : définition et premières propriétés. — Considérons deux entiers relatifs a et b. La définition du ppcm vue, dans le cas où a et b sont positifs, au chapitre précédent (exemple 3.31), s'étend facilement au cas de signes quelconques : l'ensemble

$$E = \{ \quad k \in \mathbb{N}^\star \quad / \quad k \text{ est multiple de } a \text{ et de } b \quad \} \tag{3.4}$$

est une partie de $\mathbb{N}$, et n'est pas vide puisque $|ab|$ appartient à E. Il admet donc un plus petit élément. C'est lui qu'on appelle le ppcm de a et b :

Définition 4.24 – Ppcm de deux entiers relatifs

Soient a et b deux entiers relatifs. Le ppcm de a et b est le plus petit entier naturel non nul multiple commun de a et de b.

Comme le pgcd, le ppcm satisfait quelques propriétés élémentaires, par exemple :

Soient a et b deux entiers relatifs.
- Pour tout $k \in \mathbb{Z}$, on a $\text{ppcm}(ka, kb) = |k| \cdot \text{ppcm}(a, b)$.
- Si a divise b, alors $\text{ppcm}(a, b) = |b|$.

À nouveau, la définition du ppcm comme plus petit élément de l'ensemble E ci-dessus peut être délicate à manier techniquement. La propriété suivante est bien utile en pratique :

Proposition 4.25 – Propriété universelle pour le ppcm

Soient a et b deux entiers relatifs.
- *Si $\mu = \text{ppcm}(a, b)$, alors*

  (i) μ est multiple de a et de b ;

  (ii) pour tout entier k, si k est multiple de a et de b, alors k est multiple de μ.
- *Si un entier positif μ vérifie (i) et (ii) ci-dessus, alors $\mu = \text{ppcm}(a, b)$.*

Démonstration. —
- Si $\mu = \text{ppcm}(a, b)$, le fait que μ soit multiple commun de a et b fait partie de la définition.
- Considérons à présent un entier k multiple de a et b, et montrons que μ divise k. Bien sûr, on a $k \geq \mu$ puisque μ est le plus petit multiple commun de a et b. Effectuons alors la division euclidienne de k par μ : écrivons $k = \mu q + r$ avec $0 \leq r < \mu$. On a alors
$$r = k - \mu q$$
et puisque k et μ sont multiples de a, r l'est aussi ; de même r est nécessairement multiple de b. On constate donc que r est un multiple commun positif de a et de b. Si r était non-nul, il appartiendrait à l'ensemble E de (3.4), mais c'est impossible puisqu'il est strictement inférieur au plus petit élément μ de E. On en déduit donc que $r = 0$, autrement dit que μ divise k, comme espéré.
- Si maintenant un entier positif μ vérifie les propriétés (i) et (ii) de la proposition, c'est un multiple commun de a et b, donc $\mu \geq \text{ppcm}(a, b)$, et de plus l'entier $k = \text{ppcm}(a, b)$ est un multiple commun de a et b, donc d'après (ii) c'est un multiple de μ ; comme k et μ sont positifs on a alors nécessairement $k \geq \mu$. C'est donc que $\mu = k = \text{ppcm}(a, b)$, comme annoncé.

□

En revanche, le ppcm ne satisfait généralement pas de relation de Bézout « utile ».

Évoquons brièvement le cas d'une famille de plus de trois entiers :

Définition 4.26 – PPCM : cas d'une famille de plus de deux entiers

Soit $n \in \mathbb{N}^\star$; soient $a_1, \dots, a_n$ des entiers relatifs. On appelle plus petit multiple commun de la famille $(a_1, \dots, a_n)$, et on note $\text{PPCM}(a_1, \dots, a_n)$, le plus petit entier positif et non-nul qui soit multiple de chacun des a_i, $i \in \{1, \dots, n\}$.

Comme pour le PGCD, on peut calculer un tel PPCM en se ramenant étape par étape au cas de deux entiers :

Proposition 4.27 – PPCM : formule ramenant au cas de deux entiers

Soit $n \in \mathbb{N}^\star$ avec $n \geq 2$; soient $a_1, \dots, a_n$ des entiers relatifs. On a l'égalité

$$\text{PPCM}(a_1, \dots, a_n) = \text{PPCM}\left(a_1, \text{PPCM}(a_2, \dots, a_n)\right).$$

Indication sur la démonstration. — Reprendre le principe de la démonstration effectuée pour le PGCD page 65, en adaptant l'argument. □

4. Entiers premiers entre eux

4.1. Définition et théorème de Bézout. —

Définition 4.28 – Nombres premiers entre eux

Soient a et b deux entiers relatifs. On dit que a et b sont *premiers entre eux* lorsque $\text{PGCD}(a, b) = 1$.

Exemple 4.29. — Les nombres 12 et 55 sont premiers entre eux : les diviseurs de 12 sont $1, 2, 3, 4, 6$ et 12, alors que les diviseurs de 55 sont $1, 5, 11$ et 55 ; leur seul diviseur commun est 1.

Exemple 4.30. — Fixons un nombre premier p et considérons un entier $a \in \mathbb{Z}$. Le PGCD de a et p est un entier qui divise p, il est donc égal soit à 1, soit à p. S'il est égal à p, c'est que p divise a. On obtient l'alternative suivante : si p est un nombre premier et a un entier quelconque, soit p divise a, soit a et p sont premiers entre eux.

Théorème 4.31 – Théorème de Bézout

Soient a et b deux entiers relatifs. On a l'équivalence :

$$\text{PGCD}(a, b) = 1 \iff \left(\exists (u, v) \in \mathbb{Z}^2 \ / \ ua + vb = 1. \right)$$

Démonstration. — Nous avons déjà vu à la proposition 4.15 que si a et b sont premiers entre eux, alors il existe deux entiers u et v vérifiant $au + bv = 1$.

Réciproquement, si on peut écrire $au + bv = 1$ avec $(a, b) \in \mathbb{Z}^2$, alors tout entier d qui divise à la fois a et b doit diviser $au + bv = 1$; on a alors nécessairement $d = 1$, si bien que $\text{PGCD}(a, b) = 1$. □

Étant donné un couple (a, b) d'entiers premiers entre eux, un couple (u, v) d'entiers vérifiant $ua + vb = 1$ est appelé un *couple de Bézout* pour (a, b).

Comment trouver des couples de Bézout ? — Si deux entiers a et b sont premiers entre eux, alors en effectuant l'algorithme d'Euclide, on constatera que le dernier reste vaut 1. Par exemple, $a = 40$ et $b = 29$ sont premiers entre eux, puisqu'en effectuant l'algorithme d'Euclide, les étapes successives donnent

Initialisation :	$\alpha = 48$	$\beta = 29$.	Division euclidienne de α par β : $48 = 1 \cdot 29 + 19$
Étape 1 :	$\alpha = 29$	$\beta = 19$.	Division euclidienne de α par β : $29 = 1 \cdot 19 + 10$
Étape 2 :	$\alpha = 19$	$\beta = 10$.	Division euclidienne de α par β : $19 = 1 \cdot 10 + 9$
Étape 3 :	$\alpha = 10$	$\beta = 9$.	Division euclidienne de α par β : $10 = 1 \cdot 9 + 1$
Conclusion :	$\alpha = 1$	$\beta = 0$.	Le pgcd des deux entiers de départ est 1.

L'observation importante est que *le reste, à chaque étape, est combinaison de a et b*, comme on le constate en reprenant les calculs ci-dessus :

Étape 0 :	$\alpha = 48$	$\beta = 29$.	Expression du reste : $19 = a - b$
Étape 1 :	$\alpha = 29$	$\beta = 19$.	Expression du reste : $10 = 29 - 19 = b - (a - b) = 2b - a$
Étape 2 :	$\alpha = 19$	$\beta = 10$.	Expression du reste : $9 = 19 - 10 = (a - b) - (2b - a) = 2a - 3b$
Étape 3 :	$\alpha = 10$	$\beta = 9$.	Expression du reste : $1 = 10 - 9 = (2b - a) - (2a - 3b) = -3a + 5b$

À la dernière étape, on a fini par obtenir une expression de 1 comme « combinaison » de a et b : on a

$$1 = -3a + 5b$$

(et effectivement, $5 \times 29 = 145$ alors que $3 \times 48 = 144$). Nous avons trouvé une une relation de Bézout !

Pour trouver un couple de Bézout pour deux entiers a et b premiers entre eux,
- Effectuer l'algorithme d'Euclide pour a et b en gardant trace des quotients et des restes,
- Remonter les calculs pour exprimer les restes successifs en fonction de a et b

4.2. Lemme de Gauss. —

Proposition 4.32 – Lemme de Gauss

Soient a, b, c trois entiers naturels.
Si a divise (bc) et si a est premier avec b, alors a divise c.

Exemple 4.33. — Si k est un entier et si 3 divise $5k$, alors k est multiple de 3.

Démonstration. — Nous devons montrer que c est multiple de a. Traduisons pour cela les deux hypothèses :
- Comme a divise bc, il existe un entier k vérifiant : $bc = ak$.
- Comme a et b sont premiers entre eux, d'après le théorème de Bézout, il existe deux entiers u et v tels que $au + bv = 1$.

On peut alors écrire l'entier c sous la forme suivante :

$$\begin{aligned} c &= c \cdot 1 = c \cdot (au + bv) \\ &= acu + bcv \\ &= acu + akv \\ &= a\,(cu + kv) \end{aligned}$$

et cela montre que a divise c. □

Corollaire 4.34 – Deux diviseurs premiers entre eux...

Soient p, q deux entiers non nuls et n un entier quelconque. Si p et q sont premiers entre eux et divisent tous les deux n, alors pq divise n.

Exemple 4.35. — Si n est un entier multiple à la fois de 2 et de 5, alors n est divisible par 10.

Démonstration. — Si p divise n, alors il existe un entier k vérifiant $n = pk$. Si q aussi divise n, on a alors $q|(pk)$ et $\text{PGCD}(p, q) = 1$; le lemme de Gauss indique alors que q divise k. Il existe donc un entier ℓ vérifiant $k = q\ell$; mais alors $n = pk = p(q\ell) = (pq)\ell$, et pq divise bien n. □

4.3. Applications au PGCD et PPCM. —

Lemme 4.36 – Quand on divise par le PGCD...

Soient a et b deux entiers non-nuls.

- *Si l'on note d le* PGCD *de a et b, alors les entiers $\frac{a}{d}$ et $\frac{b}{d}$ sont premiers entre eux.*
- *Si un entier k divise a, divise b et vérifie $\text{PGCD}(\frac{a}{k}, \frac{b}{k}) = 1$, alors $k = \text{PGCD}(a, b)$.*

Démonstration. —

- Si d est le PGCD de a et b, alors il vérifie une relation de Bézout : il existe un couple (u, v) d'entiers relatifs vérifiant $au + bv = d$; en divisant par d (qui est non-nul), on obtient
$$u\left(\frac{a}{d}\right) + v\left(\frac{b}{d}\right) = 1$$
ce qui prouve que $\frac{a}{d}$ et $\frac{b}{d}$ sont premiers entre eux.
- Si k est un diviseur commun de a et b, nous savons que k divise l'entier $d = \text{PGCD}(a, b)$. De plus, si les entiers $\frac{a}{k}$ et $\frac{b}{k}$ sont premiers entre eux, alors le théorème de Bézout indique l'existence de deux entiers u et v vérifiant
$$u\left(\frac{a}{k}\right) + v\left(\frac{b}{k}\right) = 1$$
autrement dit $ua + vb = k$. Puisque d divise a et b, on en déduit que d divise k. C'est donc que $d|k$, et on a déjà vu que $k|d$: on a donc $k = d$, comme espéré.

□

Proposition 4.37 – Pour des entiers premiers entre eux, le PPCM, c'est le produit

Si a et b sont deux entiers vérifiant $\text{PGCD}(a, b) = 1$, alors on a $\text{PPCM}(a, b) = ab$.

Démonstration. —

- Notons μ le PPCM de a et de b. Rappelons que ab est multiple de a et de b. D'après la propriété universelle du PPCM, c'est donc un multiple de μ.

- Vérifions maintenant que μ est multiple de ab. Partons du fait que μ est multiple de a, donc on peut écrire $\mu = ak$ avec $k \in \mathbb{Z}$. Or, μ est aussi multiple de b, donc b divise $\mu = ak$, et comme $\text{PGCD}(a, b) = 1$, d'après le lemme de Gauss, b divise k. On peut donc écrire $k = b\ell$ avec $\ell \in \mathbb{Z}$, si bien que

$$\mu = ak = (ab)\ell$$

ce qui montre que ab divise μ.

On a donc $(ab)|\mu$ et $\mu|(ab)$, d'où $\mu = ab$, comme espéré. □

Proposition 4.38 – En général, PPCM × PGCD = ab

Si a et b sont deux entiers relatifs non-nuls, on a toujours

$$\text{PPCM}(a, b) \cdot \text{PGCD}(a, b) = ab.$$

Démonstration. — Notons d le PGCD de a et de b. On sait que les entiers $\alpha = \frac{a}{d}$ et $\beta = \frac{b}{d}$ sont premiers entre eux, on a donc $\text{PPCM}(\alpha, \beta) = \alpha\beta$. En rappelant que $\alpha = \frac{a}{d}$ et $\beta = \frac{b}{d}$ et en chassant les dénominateurs, on obtient :

$$d^2 \cdot \text{PPCM}(\alpha, \beta) = ab.$$

Or, nous savons que $d \cdot \text{PPCM}(\alpha, \beta) = \text{PPCM}(d\alpha, d\beta)$ d'après une propriété du §3.3. Puisque $d\alpha = a$ et $d\beta = b$, c'est donc que $d \cdot \text{PPCM}(a, b) = ab$; comme $d = \text{PGCD}(a, b)$, voilà l'objectif atteint. □

5. Nombres premiers et théorème de factorisation

5.1. Nombres premiers et théorème d'Euclide. — Nous avons déjà évoqué brièvement les nombres premiers au chapitre 3. Voici un rappel des définitions et des résultats que nous avons vus.

Définition 4.39 – Nombre premier

Soit p un entier naturel. On dit que p est premier si $p \geq 2$ et si les seuls diviseurs de p sont 1 et p.

Exemple 4.40. — Voici, parmi les entiers de 1 à 100, la liste de ceux qui sont premiers (dans les cases vertes).

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Théorème 4.41 – Tout entier ≥ 2 admet au moins un diviseur premier

Soit n un entier supérieur ou égal à 2. Il existe au moins un nombre premier qui divise n.

Nous avons déjà vu la démonstration à l'exemple 3.29, dans le chapitre 3.

Théorème 4.42 – Théorème d'Euclide : il existe une infinité de nombres premiers

Pour tout entier $n \in \mathbb{N}$, il existe un nombre premier p qui vérifie $p > n$.

Nous avons déjà vu la démonstration à l'exemple 3.37, dans le chapitre 3.

5.2. Décomposition en produit de facteurs premiers et applications. —

5.2.1. *Existence.* — Tout entier naturel non nul peut s'écrire sous la forme d'un produit de nombres premiers, éventuellement avec des répétitions. C'est l'objet du théorème suivant.

Théorème 4.43 – Existence de la décomposition en produit de facteurs premiers

Soit n un entier naturel non nul. Il existe
- *un entier $k \in \mathbb{N}^\star$*
- *des nombres premiers $p_1, \dots, p_k$ deux à deux, distincts*
- *des entiers naturels non nuls $\alpha_1, \dots, \alpha_k$,*

vérifiant :

$$n = p_1^{\alpha_1}\ p_2^{\alpha_2}\ \cdots\ p_k^{\alpha_k}.$$

Remarque 4.44. — Ce résultat est d'une importance pratique considérable, y compris dans notre vie quotidienne. Beaucoup de ses applications pratiques, notamment à la cryptographie, sont liées au fait suivant : étant donné un « grand » entier n, il faut en général énormément de calculs pour *trouver* une décomposition comme dans le théorème, alors que si une proposition de décomposition est fournie, il est très facile de *vérifier* qu'elle est correcte.

Pour donner une idée plus concrète de ce qui est en jeu, indiquons qu'en 2009, factoriser le nombre

$$1230186684530117755130494958384962720772853569595334792197322452151726400507263657518745202199786469389956474942774063845925192557326303453731548268507917026122142913461670429214311602221240479274737794080665351419597459856902143413$$

a pris *deux ans* à une centaine de processeurs programmés pour utiliser les meilleurs algorithmes connus à l'époque. Il s'agit du produit de deux nombres premiers distincts : il est égal à

$$334780716989568987860441698482126908177047949837137685689124313889828837938780022876147116525317430877378144679994893674604366679959042824463379962795263227915816434308764267603228381573966511279233373417143396810270092798736308917.$$

Vérifier le résultat est bien sûr presque immédiat sur une machine ordinaire.

Démonstration de l'existence de la factorisation. — On raisonne par récurrence forte.

- Pour $n = 1$, le résultat est clair (prendre $k = 1$, $p_1 = 2$ et $\alpha_1 = 0$).
- Fixons un entier $n \in \mathbb{N}^\star$ et supposons que tout entier compris entre 1 et n puisse s'écrire sous la forme d'un produit de nombres premiers. Montrons alors que c'est aussi le cas pour le nombre $n+1$.

  Comme $(n+1)$ est supérieur ou égal à 2, d'après le lemme d'Euclide, il existe un nombre premier p qui divise $(n+1)$. Considérons alors le nombre $a = \frac{n+1}{p}$: puisque $p \geq 2$, on a $1 \leq a \leq \frac{n+1}{2} \leq n$; on peut donc appliquer l'hypothèse de récurrence à a.

  Ainsi, on sait qu'il existe un entier $k \in \mathbb{N}^\star$, des nombres premiers $p_1, \dots, p_k$ et des entiers $\alpha_1, \dots, \alpha_k$ vérifiant $a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. Pour écrire $n+1$, distinguons deux cas :
  — Si p n'est égal à aucun des p_i, $i \in \{1, \dots, k\}$, notons $p_{k+1} = p$ et $\alpha_{k+1} = 1$; on a alors

$$n + 1 = ap = p_1^{\alpha_1} \cdots p_k^{\alpha_k} \cdot p = p_1^{\alpha_1} \cdots p_k^{\alpha_k} \cdot p_{k+1}^{\alpha_{k+1}}$$

— Si p est l'un des p_i, disons p_{i_0}, alors on définit $\alpha'_{i_0} = \alpha_{i_0} + 1$ et $\alpha'_i = \alpha_i$ pour tout $i \in \{1, \dots, k\}$ qui n'est pas égal à i_0. On a alors $n+1 = p_1^{\alpha'_1} \dots p_k^{\alpha'_k}$.

Dans tous les cas, l'entier $n+1$ peut s'écrire comme un produit de nombres premiers.

□

5.2.2. *Notion de valuation p-adique et de support premier ; unicité de la décomposition.* —

Définition 4.45 – Valuation p-adique d'un entier

Soit n un entier relatif non nul. Si p est un nombre premier, on appelle *valuation p-adique* de n, et on note $\nu_p(n)$, le plus grand entier $k \in \mathbb{N}$ tel que p^k divise n.

Exemple 4.46. — Si $n = 200 = 8 \cdot 25 = 2^3 \cdot 5^2$, alors
- pour $p = 2$, on a $\nu_2(n) = 3$ (puisque 2^3 divise n, mais 2^4 ne divise pas n)
- pour $p = 3$, on a $\nu_3(n) = 0$ (puisque 3^0 divise n, mais 3^1 ne divise pas n)
- pour $p = 5$, on a $\nu_5(n) = 2$,
- et pour tout nombre premier p vérifiant $p > 5$, on a $\nu_p(n) = 0$.

Remarque 4.47. — Si on fixe un entier $n \in \mathbb{N}^\star$, un nombre premier p et un entier $k \in \mathbb{N}$, dire qu'on a $\nu_p(n) = k$, c'est dire qu'on peut écrire $n = p^k \cdot m$ où l'entier m n'est pas divisible par p.

Remarque 4.48. — Si a et b sont deux entiers relatifs, on a toujours

$$\nu_p(ab) = \nu_p(a) + \nu_p(b).$$

Démonstration. — Soient a et b deux entiers relatifs. Notons $k = \nu_p(a)$ et $k' = \nu_p(b)$. En utilisant la remarque précédente, on peut écrire $a = p^k(a')$ et $b = p^k(b')$ où a' et b' sont des entiers qui ne sont pas divisibles par p. On a alors

$$ab = p^{k+k'}(a'b')$$

et l'entier $a'b'$ n'est pas divisible par p : si c'était le cas, puisque p ne divise pas a' et vérifie donc $\text{PGCD}(p, a') = 1$, le lemme de Gauss garantirait $p|(b')$, ce qui est exclu. □

Remarque 4.49. — Les nombre premiers p vérifiant $\nu_p(n) > 0$ sont les nombres premiers qui divisent n. L'ensemble $\text{Supp}(n) = \{p \in \mathcal{P} \ / \ p \text{ divise } n\}$ est appelé le *support premier* de n : comme aucun nombre premier strictement supérieur à n ne peut diviser n, l'ensemble $\text{Supp}(n)$ est *fini*. Par exemple, les seuls diviseurs premiers de 200 sont $p = 2$ et $p = 5$, on a donc $\text{Supp}(200) = \{2, 5\}$.

Pour pouvoir aborder l'unicité de la décomposition en produit de facteurs premiers, remarquons que dans le théorème 4.43 (et en reprenant les notations de ce théorème), dans l'écriture

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}, \tag{5.1}$$

on peut interpréter les entiers k, $p_1, \dots, p_k$ et $\alpha_1, \dots, \alpha_k$ à l'aide des notions de support premier et de valuation p-adique :
- l'entier k est le nombre de nombres premiers figurant dans le support premier de n,
- les nombres premiers $p_1, \dots, p_k$ sont exactement ceux qui figurent dans le support premier de n,
- pour tout $i \in \{1, \dots, k\}$, l'entier α_i est la valuation p_i-adique de n.

On constate que ces quantités sont, à l'ordre près des facteurs, complètement déterminées par n : elles sont donc uniques, et la seule ambiguité possible dans l'écriture (5.1) est l'ordre dans lequel on écrit les p_i. Voici une manière de formuler plus précisément ce constat :

Théorème 4.50 – Unicité de la décomposition en produit de facteurs premiers

Soient n_1 et n_2 deux entiers naturels non nuls.
Si on a $\nu_p(n_1) = \nu_p(n_2)$ pour tout nombre premier p, alors on a nécessairement $n_1 = n_2$.

Exemple 4.51. — On ne peut avoir $3^k \cdot 5 \cdot 7^\ell = 3^\alpha \cdot 5^\beta$ que si $k = \alpha$, $\beta = 1$ et $\ell = 0$.
On ne peut jamais avoir $3 \cdot 11^k \cdot 19 = 3^\alpha \cdot 5 \cdot 19^\beta$.

Démonstration. — Raisonnons par contraposition : supposons $n_1 \neq n_2$ et démontrons qu'il existe nécessairement un nombre premier p vérifiant $\nu_p(n_1) \neq \nu_p(n_2)$.

Sans perte de généralité, supposons $n_1 < n_2$. Notons d le PGCD de n_1 et n_2 ; les entiers $a_1 = \frac{n_1}{d}$ et $a_2 = \frac{n_2}{d}$ sont premiers entre eux.

On remarque que *les supports premiers de a_1 et a_2 sont disjoints* : si p est un nombre premier apparaissant simultanément dans les supports premiers $\mathrm{Supp}(a_1)$ et $\mathrm{Supp}(a_2)$, il est nécessairement un diviseur commun de a_1 et de a_2, ce qui n'est pas possible puisque a_1 et a_2 sont premiers entre eux.

On remarque de plus qu'il est impossible qu'on ait $d = n_2$, puisque d divise n_1 et $n_1 < n_2$; ainsi $a_2 \neq 1$, et on en déduit que $a_2 \geq 2$.

Considérons alors un nombre premier p qui divise a_2 ; puisque p n'apparaît pas dans le support premier de a_1, on peut écrire $\nu_p(a_1) = 0$; ainsi

$$\nu_p(n_1) = \nu_p(d), \qquad \text{tandis que} \qquad \nu_p(n_2) = \nu_p(a_2) + \nu_p(d) > \nu_p(d).$$

on a donc nécessairement $\nu_p(n_1) \neq \nu_p(n_2)$. C'est ce qu'il fallait démontrer. □

5.2.3. *Application au calcul du* PGCD *et du* PPCM. —

Considérons les nombres $a = 120$ et $b = 45$. Pour calculer leur PGCD et leur PPCM, on peut utiliser l'algorithme d'Euclide puis la proposition 4.38. L'algorithme d'Euclide donne $\mathrm{PGCD}(a, b) = 15$, puis on constate que $\mathrm{PPCM}(a, b) = \frac{120 \times 45}{15} = 120 \times 3 = 360$.

Mais si on connaît déjà la décomposition en produit de facteurs premiers de a et de b, il est aisé d'obtenir ces résultats : en effet, on a

$$120 = 2^2 \times 3 \times 5$$
$$45 = 3^2 \times 5.$$

On constate que l'entier $3^1 \times 5$ divise a et b et on se convainc aisément qu'aucun autre diviseur commun à a et b ne peut dépasser $3^1 \times 5$. De même, l'entier $2^2 \times 3^2 \times 5$ est un multiple commun de a et b, et il s'agit visiblement du PPCM de a et de b.

Plus généralement, on a le résultat suivant.

Proposition 4.52 – Calcul du PGCD et du PPCM via la factorisation

Soient a et b deux entiers naturels non nuls. Notons δ le PGCD *de a et b et μ le* PPCM *de a et b.*
Pour tout nombre premier p, on a

$$\nu_p(\delta) = \min(\nu_p(a), \nu_p(b))$$
$$\nu_p(\mu) = \max(\nu_p(a), \nu_p(b))$$

Malgré sa formulation abstraite, ce résultat exprime un fait très concret, comme en atteste l'exemple suivant.

Exemple 4.53. — Si $a = 2^4 \times 3 \times 7^\alpha \times 11^3 \times 19^\beta$ et $b = 2 \times 5^2 \times 7^{\alpha'} \times 11$ avec $\alpha' > \alpha$, alors

$$\text{PGCD}(a,b) = 2 \times 7^\alpha \times 11 \quad \text{et} \quad \text{PPCM}(a,b) = 2^4 \times 3 \times 5^2 \times 7^{\alpha'} \times 11^3 \times 19^\beta.$$

Exercices du chapitre 4

Divisibilité et division euclidienne. —

Exercice 4.1. — ★☆☆

1. Déterminer le quotient et le reste de la division euclidienne de 43758 par 9877.
2. Combien y a-t-il d'entiers naturels ayant, dans la division euclidienne par 9877,
   - 7 pour quotient ?
   - 7 pour reste ?
   - 7 pour quotient et 7 pour reste ?

Exercice 4.2. — ★☆☆

1. Soit n un entier naturel. On suppose que le reste de la division euclidienne de n par 5 vaut 2 ou 3. Montrer que n^2+1 est divisible par 5.
2. Soit n un entier naturel. Montrer qu'il est impossible que 4 divise n^2+1.
   On pourra distinguer les cas n pair et n impair.

Exercice 4.3. — ★★☆

1. Quels sont les entiers $n \in \mathbb{N}$ tels que n divise $n+8$?
2. Quels sont les entiers $n \in \mathbb{N}$ tels que $(n-3)$ divise (n^3-3) ?
   On pourra faire apparaître n^3-3^3.

Exercice 4.4. — ★★☆

Soient a et b deux entiers. On suppose que 7 divise a^2+b^2. Montrer que 7 divise a et 7 divise b.
On pourra lister les restes possibles de a^2 et b^2 dans la division euclidienne par 7.

***Exercice 4.5* (Écriture d'un entier en base b).** — ★★★

Dans tout l'exercice, on fixe un entier $b \geq 2$.

1. Démontrer l'assertion suivante : pour tout entier $n \in \mathbb{N}^\star$, il existe un entier $p \geq 0$ et des nombres $c_0, c_1, \ldots, c_p$ appartenant tous à $\{0, \ldots, b-1\}$ et vérifiant

$$n = \sum_{i=0}^{p} c_k \cdot b^k \quad \text{et } c_p \neq 0.$$

   On pourra raisonner par récurrence forte et effectuer une division euclidienne par b.

2. Montrer que les entiers $c_0, c_1, \ldots, c_p$ de la question précédente sont uniquement déterminés par n, c'est-à-dire que si p et p' sont deux entiers et si $c_0, c_1, \ldots, c_p, d_0, \ldots, d_{p'}$ sont des entiers appartenant à $\{0, \ldots, b-1\}$, et si $c_p \neq 0$ et $d_{p'} \neq 0$, alors on a

$$\left(\sum_{k=1}^{p} c_k b^k = \sum_{k=1}^{p'} d_k b^k \right) \implies (p = p' \text{ et } \forall k \in \{1, \ldots, p\}, c_k = d_k).$$

3. Étant donné un entier n, les entiers $c_0, \ldots, c_p$ tels que $n = \sum_{k=0}^{p} c_k b^k$ s'appellent les *chiffres du développement de l'entier n en base b*. Déterminer les chiffres du développement en base 2 des entiers $2, 5, 64, 100, 2048, 5555$.

PGCD *et* PPCM *: manipulations élémentaires.* —

***Exercice 4.6* (Calculs).** — ★☆☆

1. Déterminer le PGCD et le PPCM de
   - 12 et 18
   - 385 et 567

Exercice 4.7. — ★☆☆
En utilisant l'algorithme d'Euclide, déterminer le PGCD de $17^{63}-1$ et $17^{42}-1$.

Exercice 4.8. — ★★☆
Déterminer tous les couples d'entiers n, m vérifiant les conditions suivantes :

$$1 \leq n \leq m$$
$$m+n = 256$$
$$\text{PGCD}(m,n) = 16.$$

***Exercice 4.9* (Pour manier le cas de trois entiers).** — ★★☆
Notons $a = 91$, $b = 77$ et $c = 143$.

1. Déterminer l'entier $d = \text{PGCD}(a,b,c)$
2. Trouver des entiers u, v, w vérifiant $ua + vb + wc = d$.

Nombres premiers entre eux. —

***Exercice 4.10* (Autour du théorème de Bézout).** — ★☆☆

1. Montrer que pour tout $n \in \mathbb{N}^\star$, les entiers n et $n+1$ sont premiers entre eux.
2. Existe-t-il un entier $k \neq 1$ ayant la propriété « pour tout $n \in \mathbb{N}^\star$, les entiers n et $n+k$ sont premiers entre eux » ?
3. Soit n un entier naturel. Montrer que les entiers $9k+4$ et $2k+1$ sont premiers entre eux.

***Exercice 4.11* (Recherche d'un couple de Bézout).** — ★☆☆

1. Déterminer deux entiers relatifs u_0 et v_0 vérifiant : $35u_0 + 13v_0 = 1$.
2. Déterminer tous les couples $(u,v) \in \mathbb{Z}^2$ vérifiant $35u + 13v = 1$.

***Exercice 4.12* (Un cas simple d'équation diophantienne).** — ★★☆
Déterminer tous les couples $(x,y) \in \mathbb{Z}^2$ vérifiant :

$$27x + 45y = 63.$$

Congruences. —

Exercice 4.13. — ★☆☆
Calculer 8^{999} modulo 13.

***Exercice 4.14* (Inversion modulo n).** — ★☆☆

1. Soit n un entier naturel non nul. Soit a un entier premier avec n. Montrer qu'il existe un entier u vérifiant $au \equiv 1 \mod n$.
2. Déterminer un entier u vérifiant : $3u \equiv 1 \mod 11$.

***Exercice 4.15* (Théorème des restes chinois).** — ★★☆
Dans cet exercice, on fixe deux entiers n_1 et n_2 et on suppose $\text{PGCD}(n_1,n_2) = 1$. On fixe également deux entiers a_1 et a_2 quelconques, et on cherche à déterminer les entiers x qui vérifient

$$\begin{cases} x \equiv a_1 \mod n_1 \\ x \equiv a_2 \mod n_2 \end{cases}. \qquad (\star)$$

1. Montrer qu'il existe deux entiers e_1 et e_2 vérifiant : $\begin{cases} e_1 \equiv 1 \mod n_1 \\ e_1 \equiv 0 \mod n_2 \end{cases}$ et $\begin{cases} e_2 \equiv 0 \mod n_1 \\ e_2 \equiv 1 \mod n_2 \end{cases}$.
2. Notons $x_0 = a_1e_1 + a_2e_2$.
   Montrer qu'un entier x vérifie ($\star$) si et seulement si on a $x \equiv x_0 \mod (n_1n_2)$.

Exercice 4.16. — ★★☆
Déterminer les entiers a, b vérifiant $3^a7^b \equiv 1 \mod 10$. *On remarquera que* $3^4 \equiv 1 \mod 10$.

***Exercice 4.17* (Critères de divisibilité).** — ★★☆ – *long*

1. Montrer qu'un entier naturel est divisible par 3 si et seulement si la somme de ses chiffres (dans l'écriture en base 10) est divisible par 3.
2. Montrer qu'un entier naturel est divisible par 9 si et seulement si la somme de ses chiffres est divisible par 9.
3. Soit n un entier naturel. Notons $c_0, c_1, \dots, c_k$ les chiffres de son écriture en base 10 (par exemple si $n = 2768$, on a $k = 3$, $c_3 = 2$, $c_2 = 7$, $c_1 = 6$ et $c_0 = 8$). Montrer que n est divisible par 11 si et seulement si on a $\sum_{i=0}^{k}(-1)^i c_i \equiv 0 \mod 11$.
4. Trouver un critère de divisibilité par 7.
5. *Applications.*
   - Le nombre 771463 est-il divisible par 3 ? 9 ? 11 ? 7 ?
   - Le nombre 978381778401775 est-il divisible par 11 ?

Exercice 4.18. — ★★★
Montrer qu'il existe un multiple de 23 dont l'écriture en base 10 ne comporte que des 1.

Nombres premiers. —

Exercice 4.19. — ★☆☆
Soient a et n deux entiers. On suppose $a \geq 2$ et $n \geq 2$, et on suppose que $a^n - 1$ est premier.

1. Montrer que $a = 2$.
2. Montrer que n est premier.

Exercice 4.20. — ★★☆
Soit p un nombre premier différent de 2 et de 3. Montrer que $p^2 \equiv 1 \mod 24$.
Indication : étudier les restes de $(p-1)$ *et* $(p+1)$ *modulo* 3 *et* 4.

***Exercice 4.21* (Petit théorème de Fermat).** — ★★☆
Dans tout l'exercice, on fixe un nombre premier p.

1. Démontrer que pour tout entier k vérifiant $1 < k < p$, le coefficient binomial $\binom{p}{k}$ est divisible par p.
2. En déduire que pour tout entier $n \in \mathbb{Z}$, on a $(n+1)^p \equiv n^p + 1 \mod p$
3. En déduire que pour tout entier $a \in \mathbb{N}^\star$, on a $a^p \equiv a \mod p$ (on pourra raisonner par récurrence).
4. Montrer que pour tout $a \in \mathbb{N}^\star$ non divisible par p, on a
$$a^{p-1} \equiv 1 \mod p.$$

***Exercice 4.22* (Application du théorème de factorisation, II).** — ★☆☆
Soient a, b, c des éléments de $\mathbb{N}^\star$; on note $n = 2^a7^b11^c$.

1. Déterminer, en fonction de a, b et c, le nombre de diviseurs de n.
2. Soient a', b', c' des éléments de $\mathbb{N}^\star$; notons $m = 2^{a'}3^{b'}11^{c'}$.Déterminer tous les diviseurs communs à n et m ainsi que le PGCD de n et m.

***Exercice 4.23* (Application du théorème de factorisation, II).** — ★★☆
Trouver les couples d'entiers (a, b) vérifiant : $\text{PGCD}(a, b) = 42$ et $\text{PPCM}(a, b) = 1680$.

Exercices divers. —

***Exercice 4.24* (Forme irréductible d'un nombre rationnel.)** — ★★☆

1. Soit r un nombre réel. On suppose que r peut s'écrire sous la forme $r = \frac{n}{m}$ avec $n \in \mathbb{Z}$ et $m \in \mathbb{Z}^\star$. Montrer qu'il existe un unique couple $(p, q) \in \mathbb{Z} \times \mathbb{N}^\star$ d'entiers *premiers entre eux* vérifiant $r = \frac{p}{q}$.

   Lorsque p et q sont deux entiers premiers entre eux, on dit que la fraction $\frac{p}{q}$ est *irréductible*.

2. Soit n un élément de $\mathbb{N}^\star$. Montrer que la fraction $\dfrac{15n^2 + 8n + 6}{30n^2 + 21n + 13}$ est irréductible.

***Exercice 4.25* (Indicatrice d'Euler).** — ★★★ – *long*
Pour tout $n \in \mathbb{N}^\star$, on note

$$\varphi(n) = \text{ le nombre d'entiers } k \in \{1, \dots, n\} \text{ vérifiant } \text{PGCD}(k, n) = 1.$$

1. ★☆☆ Que valent $\varphi(3)$, $\varphi(12)$ et $\varphi(30)$?
2. ★☆☆ Vérifier que si p est un nombre premier, alors $\varphi(p) = p - 1$.
3. ★☆☆ Soient p et q deux nombres premiers distincts. Montrer qu'on a $\varphi(pq) = (p - 1)(q - 1)$.
4. ★★☆ Soit p un nombre premier et k un élément de $\mathbb{N}^\star$. Que vaut $\varphi(p^k)$?
5. ★★★ Soient a et b deux entiers premiers entre eux. En utilisant le théorème des restes chinois (exercice 4.15), démontrer l'égalité $\varphi(ab) = \varphi(a)\varphi(b)$.
6. ★☆☆ Soit n un entier avec $n \geq 2$. En s'appuyant sur la décomposition de n en produit de facteurs premiers, donner une formule pour $\varphi(n)$.

***Exercice 4.26* (Idéaux de $\mathbb{Z}$).** — ★★☆ – *long*
Soit $\mathcal{I}$ une partie de $\mathbb{Z}$. On dit que $\mathcal{I}$ est un *idéal de* $\mathbb{Z}$ lorsque $\mathcal{I}$ lorsque les trois propriétés suivantes sont vérifiées :

$$\text{l'ensemble } \mathcal{I} \text{ est non vide,} \tag{P_1}$$

$$\text{si } x \text{ et } y \text{ sont deux éléments de } \mathcal{I}, \text{ alors } x + y \text{ est aussi un élément de } \mathcal{I}, \tag{P_2}$$

$$\text{si } x \text{ est un élément de } \mathcal{I}, \text{ alors pour tout } k \in \mathbb{Z}, \text{ on a } kx \in \mathcal{I}. \tag{P_3}$$

1. (a) Vérifier que si $\mathcal{I}$ est un idéal de $\mathbb{Z}$, alors $\mathcal{I}$ contient le nombre 0.
   (b) Soit a un élément de $\mathbb{Z}$. On note $a\mathbb{Z}$ l'ensemble $\{ka,\ k \in \mathbb{Z}\}$. Vérifier que $a\mathbb{Z}$ est un idéal de $\mathbb{Z}$.
   (c) Soient a et b deux éléments de $\mathbb{Z}$. Donner une condition nécessaire et suffisante sur a et b pour que soit vérifiée l'inclusion $a\mathbb{Z} \subset b\mathbb{Z}$.
2. Dans cette question, on vérifie que tout idéal de $\mathbb{Z}$ est de la forme $a\mathbb{Z}$ pour un certain $a \in \mathbb{Z}$.
   (a) Soit $\mathcal{I}$ un idéal de $\mathbb{Z}$. Vérifier que si $I \neq \{0\}$, alors $\mathcal{I} \cap \mathbb{N}^\star$ admet un plus petit élément.
   (b) En utilisant la division euclidienne, conclure.
3. Dans cette question, on fixe deux entiers a et b et on note $\delta = \text{PGCD}(a, b)$ et $\mu = \text{PPCM}(a, b)$. Démontrer les égalités suivantes :
$$(a\mathbb{Z}) \cap (b\mathbb{Z}) = \mu\mathbb{Z}$$
$$(a\mathbb{Z}) + (b\mathbb{Z}) = \delta\mathbb{Z}$$
   où la notation $a\mathbb{Z} + b\mathbb{Z}$ désigne l'ensemble des nombres qui peuvent s'écrire sous la forme $x + y$ où $x \in a\mathbb{Z}$ et $y \in b\mathbb{Z}$.

BIBLIOGRAPHIE

[1] René Cori & Daniel Lascar, *Logique mathématique*, Dunod, 2003.

Ouvrage de logique mathématique, qu'il n'est pas nécessaire pour vous de consulter, mais où j'ai puisé l'exemple 1.20.

[2] Paul Halmos, *Introduction à la théorie des ensembles*, Jacques Gabay, 2000.
Traduction de : *Naive Set Theory*, paru en 1960.

Ouvrage classique de présentation de la théorie des ensembles. Lecture profitable uniquement si vous souhaitez en savoir plus sur les subtilités théoriques des chapitres 1 et 2.

[3] Roger Mansuy, *Tout-en-un Mathématiques MPSI*, Vuibert, 2019.

Ouvrage général, destiné aux élèves de classes préparatoires. Quelques-uns des exercices de ce polycopié en sont issus, et le livre contient des problèmes dont certains sont de niveau élevé.

[4] Roger Godement, *Cours d'algèbre* ; 3ème édition, Hermann, 1997.

Ouvrage général et classique, écrit en 1963, et qui reste une référence sur l'ensemble de l'algèbre des trois premières année de licence. Il couvre donc beaucoup plus que le contenu de vos cours de L1. Le style en est à la fois très classique et très personnel. Il y a beaucoup d'exercices.

[5] Claude Deschamps, & Frédéric Moulin *et coll.*, *Tout-en-un Maths MPSI* ; 5ème édition, Dunod, 2018.

Ouvrage général, destiné aux élèves de classes préparatoires. Quelques-uns des exercices de ce polycopié en sont issus ; le livre contient de nombreux exercices corrigés.

Remarque générale : les ouvrages mentionnés ci-dessus sont ceux que j'ai utilisés pour rédiger ce polycopié, et dans lesquels j'ai puisé une partie des exemples et des exercices du fascicule. Ce ne sont pas forcément les plus adaptés à votre travail personnel : pour chercher des ouvrages de travail, vous pouvez consulter la bibliographie générale diffusée séparément.