Université Paul Sabatier - UFR MIG - Département de Mathématique.
Année scolaire 2009/2010.

Cours polycopié pour le module Mathématique II

Conventions.
Dans ce qui suit, les *mots en italiques* sont ceux que l'on est en train de définir. On emploie le symbole := lorsqu'une égalité sert à définir le membre gauche à partir du membre droit. Par exemple :
On appelle *carré* du réel x le réel $x^2 := x.x$.
On peut aussi introduire un terme sans définition complète et sans que sa connaissance soit exigible : on le mettra plutôt entre guillemets. Par exemple :
On résume les propriétés de l'addition dans $\mathbf{R}$ en disant que $(\mathbf{R}, +)$ est un "groupe commutatif".

À propos du module Math II (UE8). Tous les étudiants qui suivent le module Math II suivent par ailleurs le module Math I (UE2), qui vise essentiellement à consolider les acquis du secondaire afin de servir aux sciences exactes, comme à la suite de l'enseignement mathématique. *A contrario*, on adopte ici un style propre aux mathématiciens : mise en avant des fondements (axiomes et définitions), des concepts abstraits, des démonstrations.

Ce cours à destination des étudiants de l'UE de Mathématique II est assez détaillé et contient des compléments qui vont parfois au delà du programme prévu. Comme tout cours de Mathématique, il doit être lu avec un stylo et une feuille de papier blanche à la main pour vérifier pas à pas que toutes les assertions sont correctes. Chaque section de ce cours se termine par des exercices non corrigés à "consommer sans modération". En effet, en plus des exercices contenus dans les feuilles de TD communes à tous les étudiant(e)s et qui seront corrigés en séance de TD, il est conseillé de s'exercer à résoudre par soi-même ces exercices sans avoir une solution à coté : c'est grâce à ce ce travail personnel indispensable que l'on peut aller plus loin dans la compréhension et l'assimilation des notions mathématiques introduites. C'est la seule méthode connue à ce jour pour progresser en Mathématique.

Il existe plusieurs ouvrages que l'on peut consulter et qui se trouvent à la Bibliothèque Universitaire.

1. *Mathématiques. Tout-en-un pour la Licence. Niveau L1* sous la direction de Jean-Pierre Ramis et André Warusfel, Éditions Dunod. Ce livre est particulièrement conseillé, il contient de nombreux compléments, éclaircissements et exercices supplémentaires.

2. *Cours de Mathématiques du premier cycle*, par Jacques Dixmier, Éditions Gauthier-Villars.

3. *Mathématiques pour le DEUG, Analyse Première année*, par François Liret et Dominique Martinais, Éditions Dunod.

Chapitre 1

Suites numériques

Le but essentiel de ce chapitre est de présenter une étude rigoureuse des suites de nombres réels ; l'objectif principal étant de permettre une bonne maitrise des techniques de base de l'Analyse réelle élémentaire à savoir : calculer, majorer, minorer, approcher.

On commencera tout d'abord par tenter de définir ce que sont les nombres réels à partir des nombres rationnels en insistant sur la structure particulièrement riche de l'ensemble $\mathbf{R}$ des nombres réels. La construction des nombres réels n'est pas au programme de ce cours, mais compte tenu de leur importance en Mathématique, il nous a parru utile de donner en appendice à la fin de ce chapitre, une idée de cette construction suivant la méthode des coupures de Dedekind, la première construction apparu historiquement vers la fin du XIX^e siècle.

On introduira ensuite la notion de "convergence" qui est un concept fondamental majeur en Analyse et on insistera notamment sur son utilisation comme moyen d'approcher par exemple certains "nombres irrationnels" par des nombres rationnels (e.g. des décimaux).

On donnera enfin quelques exemples simples de suites récurrentes pour illustrer la méthode des itérations successives en montrant comment les suites convergentes peuvent être utilisées pour approcher les nombres réels solutions de certaines équations non linéaires fournissant ainsi un algorithme qui peut être utilisé concrètement dans la paratique (voir par exemple l'approximation de la racine carrée).

1.1 Introduction aux nombres réels

Les nombres réels sont connus et utilisés dans les calculs depuis fort longtemps. La découverte du premier nombre irrationnel $\sqrt{2}$ date probablement de l'époque de Pythagore (VI^e siècle av. J.C.). Mais il a fallu attendre la fin du XIX^e siècle pour que

les mathématiciens comme Peano, Dedekind et Cantor notamment aboutissent par une démarche rigoureuse à la première construction du corps des nombres réels.

On a d'abord défini les nombres entiers naturels de manière axiomatique (Peano), puis à partir des nombres entiers naturels, on a construit successivement les nombres entiers relatifs, les nombres rationnels et enfin les nombres réels et les nombres complexes. Il aura donc fallu attendre environ 25 siècles pour que l'on aboutisse à la belle chaine d'inclusions suivante :

$$\mathbf{N} \subset \mathbf{Z} \subset \mathbf{Q} \subset \mathbf{R} \subset \mathbf{C}.$$

Parmi ces inclusions c'est bien entendu l'inclusion $\mathbf{Q} \subset \mathbf{R}$ qui est la plus mystérieuse et la plus délicate. C'est celle-là que nous allons tenter d'explorer dans cette première section.

Avertissement : Seul le contenu du paragraphe 1.3 de cette section est vraiment **obligatoire** et doit être bien compris des étudiant(e)s. Cependant il leur est conseillé de lire les autres paragraphes ainsi que l'appendice correspondante au gré de leur curiosité et de leur besoin d'approfondissement.

1.1.1 Insuffisance des nombres rationnels

Nous supposerons connus l'ensemble $\mathbf{N}$ des entiers naturels muni de ses deux opérations internes, l'addition notée $+$ et la multiplication notée $\cdot$ ayant les propriétés habituelles (associativité, commutativité, distributivité, existence d'élément neutre) et d'une relation d'ordre total compatible avec ces opérations internes ayant la propriété fondamentale suivante :
Toute partie non vide de $\mathbf{N}$ *admet un plus petit élément et toute partie de* $\mathbf{N}$ *non vide et majorée admet un plus grand élément.*

Cependant l'équation $x + n = 0$, où $n \in \mathbf{N}$ est donné n'a pas de solution dans $\mathbf{N}$. Autrement dit il n'y a pas d'opposé dans $\mathbf{N}$. Pour pallier à cet inconvénient, on construit par "symétrisation" de l'addition sur N, l'ensemble $\mathbf{Z}$ des nombres entiers rationnels (ou relatifs) qui contient $\mathbf{N}$.

Rapellons que les opérations internes sur $\mathbf{N}$ et la relation d'ordre peuvent être prolongées à $\mathbf{Z}$ en deux opérations internes, l'addition encore notée $+$ et la multiplication notée $\cdot$ avec les mêmes proriétés de sorte que pour tout tout $n \in \mathbf{Z}$ l'équation $x + n = 0$ admette une solution unique dans $\mathbf{Z}$, notée $-n$, appelé l'opposé de n. Ces propriétés sont bien connues et nous ne les rappellerons pas ici mais elles se résument en disant que $(\mathbf{Z}, +, \cdot)$ est un "anneau commutatif intègre".

De plus il existe une "relation d'ordre total" sur $\mathbf{Z}$, notée $\leq$, compatible avec cette structure qui prolonge l'ordre naturel sur $\mathbf{N}$ et qui possède la propriété fondamentale suivante :
Toute partie non vide et minorée (resp. majorée) de $\mathbf{Z}$ *possède un plus petit (resp. plus grand) élément.*

L'importance des nombres entiers naturels sera mise en évidence au chapitre 2 sur les dénombrements, tandis que l'étude détaillé de la structure de $\mathbf{Z}$ fera l'objet du chapitre 3 sur l'Arithmétique.

Cependant si $q \in \mathbf{Z} \setminus \{0\}$ l'équation $q \cdot x = 1$ n'a pas de solution dans $\mathbf{Z}$, à moins que $q = \pm 1$. Autrement dit il n'y a pas d'inverse dans $\mathbf{Z}$.

Une construction classique très fréquente en mathématique, analogue à celle qui permet de construire $\mathbf{Z}$ à partir de $\mathbf{N}$, appellée le *passage au quotient*, permet de pallier cet inconvénient en construisant un "ensemble plus gros" $\mathbf{Q}$ ayant une structure analogue à celle de $\mathbf{Z}$ et dans lequel tout élément non nul admet un inverse.

Nous ne donnerons pas cette construction ici, mais rappelons qu'un nombre rationnel $x \in \mathbf{Q}$ est une fraction $x = p/q$ représentée par un couple d'entiers $(p, q) \in \mathbf{Z} \times \mathbf{Z}^\star$ avec la relation d'equivalence suivante : deux couples $(p, q) \in \mathbf{Z} \times \mathbf{Z}^\star$ et $(p', q') \in \mathbf{Z} \times \mathbf{Z}^\star$ représentent le même nombre rationnel s'ils définissent la même fraction i.e. $p \cdot q' = p' \cdot q$.

Il résulte des propriétés arithmétiques de $\mathbf{Z}$ que tout nombre rationnel $x \in \mathbf{Q}$ admet une représentation unique sous la forme $x = p/q$ où p, q sont des entiers tels que $q \geq 1$, $p \in \mathbf{Z}$ et p et q sont premiers entre eux.

Les opérations d'addition et de multiplication sur $\mathbf{Z}$ s'étendent naturellement à $\mathbf{Q}$ de sorte que $(\mathbf{Q}, +, \cdot)$ est un "corps commutatif".

De plus la relation d'ordre sur $\mathbf{Z}$ s'étend naturellement à l'ensemble $\mathbf{Q}$ et en fait un corps commutatif totalement ordonné.

Parmi les nombres rationnels il y a les nombres décimaux qui s'écrivent sous la forme $n10^m$, où $n \in \mathbf{Z}$ et $m \in \mathbf{Z}$.
La relation d'ordre sur $\mathbf{Q}$ possède une propriété simple mais importante que nous allons rappeler.

Proposition 1.1.1 (Propriété d'Archimède) *Soit* $a \in \mathbf{Q}$ *et* $b \in \mathbf{Q}$ *avec* $a > 0$. *Alors il existe un entier* $N \in \mathbf{N}$ *tel que* $Na > b$.

Démonstration. En effet si $b \leq 0$ la propriété est trivialement vraie avec $N = 1$.
Supposons que $b > 0$. Alors la relation $Na > b$ s'écrit $N > ba^{-1}$. Comme $ba^{-1} \in \mathbf{Q}$ et

que $ba^{-1} > 0$, il sécrit $ba^{-1} = p/q$, avec $p, q \in \mathbf{N}^*$ et l'entier $N := p+1$ vérifie l'inégalité $N > p \geq ba^{-1}$. □

Cette propriété est fondamentale. Elle signifie que dans $\mathbf{Q}$ il y a des nombres rationnels aussi petit que l'on veut. On dit que $(\mathbf{Q}, +, \cdot, \leq)$ est un "corps archimédien".

On s'est aperçu assez tôt que pour les besoins de la géométrie classique par exemple, le corps $\mathbf{Q}$ des nombres rationnels est insuffisant. Il lui manque beaucoup de nombres réels représentant des grandeurs géométriques (e.g. des longueurs) qui ne sont pas rationnels dont les plus célèbres sont $\sqrt{2}$ et π ; en fait l'ensemble $\mathbf{Q}$ est plein de "trous", en un sens que nous allons tenter d'expliquer.

Donnons un premier exemple simple qui illustre ce phénomène. Depuis Euclide, on sait construire à la règle et au compas, un carré du plan dont l'aire est le double de celle du carré unité par exemple. La longueur ℓ des cotés de ce carré vérifie l'équation $\ell^2 = 2 \cdot 1^2 = 2$. Il est facile de voir que ℓ est aussi égal à la longuer de la diagonale du carré unité (faire un dessin). Ce nombre est facile à construire à la règle et au compas et pourtant nous allons démontrer qu'il n'est pas rationnel.

Proposition 1.1.2 *Il n'existe pas de nombre rationnel $x \in \mathbf{Q}$ tel que $x^2 = 2$.*

Démonstration. Pour démontrer cette propriété, on raisonne par l'absurde en supposant le contraire pour aboutir à une contradiction. En effet supposons qu'il existe un nombre rationnel x tel que $x^2 = 2$. Comme $(-x)^2 = 2$, on peut supposer $x > 0$. Ecrivons $x = p/q$ sous forme irréductible, où p, q sont des entiers positifs non nuls et premiers entre eux tels que $x^2 = 2$. Alors $p^2 = 2q^2$, ce qui veut dire que p^2 est un entier pair. Cela implique que p est pair ; en effet le carré d'un nombre entier impair $n = 2k + 1$, avec $k \in \mathbf{N}$) est un nombre entier impair puisque $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$. Par conséquent, il existe un entier p' tel que $p = 2p'$. Il en résulte que $q^2 = 2p'^2$, ce qui implique de la même façon que q est pair. Ainsi p et q sont pairs donc divisibles par 2 et donc la fraction p/q n'est pas irréductible, ce qui est une contradiction. □

En fait le raisonnement précédent peut se généraliser en utilisant le théorème fondamental de l'arithmétique (Théorème d'Euclide) pour démontrer que si $m \in \mathbf{N}$ est un nombre entier naturel qui n'est pas le carré d'un autre entier (e.g. un nombre premier) alors l'équation $x^2 = m$ n'a pas de solution dans $\mathbf{Q}$.

En conclusion, on peut dire que l'ensemble $\mathbf{Q}$ des nombres rationnels possède des "trous" et ne suffit pas pour traiter des problèmes simples de géométrie classique.

1.1.2 Les nombres irrationnels existent réellement

Nous avons vu au paragraphe précédent que le corps des rationnels est incomplet en ce sens qu'il lui manque beaucoup d'éléments.

En effet nous avons démontré qu'il n'existe pas de nombre rationnel dont le carré est égal à 2. Autrement dit la "grandeur géométrique constructible" ℓ notée $\sqrt{2}$ dont le carré est 2 n'est pas un nombre rationnel. Il est bien connu des lycéens que la spirale de Pythagore permet de construire successivement à la règle et au compas toutes les grandeurs réelles dont le carré est un entier naturel $m \in \mathbf{N}^*$.

Dans la pratique nous avons besoin de connaitre des valeurs décimales approchées de ces nombres avec une certaine précision.

Nous allons présenter un procédé assez simple permettant par exemple de construire des nombres rationnels (décimaux) dont le carré est arbitrairement voisin de 2 par défaut et des nombres rationnels décimaux) dont le carré est arbitrairement voisin de 2 par excès. Ces nombres décimaux seront appelés respectivement des *approximants décimaux par défaut* et des *approximants décimaux par excès* de la grandeur réelle ℓ. C'est dans ce sens là que l'on peut dire que le nombre irrationnel $\sqrt{2}$ existe !

Nous allons appliquer le "procédé de dichotomie" pour démontrer cette propriété.

En effet observons d'abord que si $a, b \in \mathbf{Q}$ sont des nombres rationnels (décimaux), leur moyenne arithmétique $m := (a + b)/2 \in \mathbf{Q}$ est un nombre rationnel (décimal) vérifiant $a < m < b$. Si l'on représente les nombres rationnels par des points situés sur une droite orientée, le nombre rationnel m correspond au milieu du segment qui joint les points représentant les nombres a et b respectivement. Cequi coupe en deux ce segment, d'où le nom de "procédé de dichotomie" utilisé pour qualifier cette méthode.

Choisissons deux nombres rationnels (décimaux) $a_0, b_0 \in \mathbf{Q}^+$ tels $a_0^2 < 2 < b_0^2$. Le nombre a_0 (resp. b_0) peut être considéré comme un premier approximant rationnel (décimal) par défaut (resp. par excès) de la grandeur géométrique ℓ solution de l'équation $x^2 = 2$.

Considérons ensuite le nombre rationnel (décimal) $m_0 := \frac{a_0+b_0}{2}$. Alors, puisque l'équation $x^2 = 2$ n'a pas de solution dans $\mathbf{Q}$, il n'y a que deux cas possibles.
- Ou bien $m_0^2 < 2$, dans ce cas on pose $a_1 := m_0$ et $b_1 := b_0$.
- Ou bien $m_0^2 > 2$, auquel cas on pose $a_1 := a_0$ et $b_1 := m_0$.

Dans tous les cas on obtient un nouveau couple (a_1, b_1) de nombres rationnels (décimaux) positifs vérifiant $a_0 \leq a_1 < b_1 \leq b_0$, $a_1^2 < 2 < b_1^2$ et tels que $b_1 - a_1 = \frac{b_0-a_0}{2}$.

On obtient ainsi un nouvel approximant rationnel (décimal) par défaut a_1 de la grandeur ℓ tel que a_1^2 soit une valeur approchée par défaut de 2 et un nouvel approximant rationnel par excès b_1 de la grandeur ℓ tel que b_1^2 soit une valeur approchée par excès de 2 vérifiant $b_1 - a_1 = \frac{b_0 - a_0}{2}$, ce qui implique que l'une au moins des deux valeurs décimales approchées ainsi obtenues est plus précise que chacune des deux valeurs approchées précédentes.

En itérant ce procédé de dichotomie n fois, on construit successivement des approximants rationnels (décimaux) par défaut $a_0 \leq a_1 \leq \ldots \leq a_n$ et des approximants rationnels (décimaux) par excès $b_0 \geq b_1 \geq \ldots \geq b_n$ de la même grandeur ℓ tels qu'au rang n on ait $a_n^2 < 2 < b_n^2$ et l'écart entre les deux approximants est donné par $e_n := b_n - a_n = \frac{b_0 - a_0}{2^n}$.

Grâce à la propriété d'Archimède de $\mathbf{Q}$, étant donné $\varepsilon \in \mathbf{Q}_+^* := \{x \in \mathbf{Q}; x > 0\}$, on peut trouver un entier $N \in \mathbf{N}^*$ tel que $\frac{b_0 - a_0}{2^N} < \varepsilon$; il suffit pour cela de prendre $N > (b_0 - a_0)/\varepsilon$ puisque $2^N > N$. Ainsi a_N et b_N sont des approximants rationnels (décimaux) qui donnent des valeurs rationnelles (décimales) approchées à $\varepsilon-$près par défaut et par excès respectivement de la grandeur ℓ i.e. pour tout $a_N < \ell < b_N$ et $0 < b_N - a_N < \varepsilon$.

Mettons en pratique cette méthode en considérant par exemple comme premières valeurs approchés décimales par défaut et par excès de $\sqrt{2}$, les deux nombres réels suivants : $a_0 := 1,4$ et $b_0 := 1,5$ puisque $(1,4)^2 < 2 < (1,5)^2$. On a alors $a_0 \in \mathbf{Q}_+^*, b_0 \in \mathbf{Q}_+^*$ et $a_0 < \sqrt{2} < b_0$.

On a vu qu'au bout de n itérations, l'erreur par défaut ou par excès est dominée par $(b_0 - a_0) \cdot 2^{-n} = 10^{-1} \cdot 2^{-n}$. Si l'on souhaite déterminer une valeur approchée décimale de $\sqrt{2}$ à 10^{-3} près par exemple (i.e. avec deux décimales exactes), il suffit de choisir n tel que $10^{-1} \cdot 2^{-n} \leq 10^{-3}$; il suffit de prendre $n = 7$ et les nombres décimaux a_7 et b_7 fourniront une valeur approchée par défaut et par excès respectivement de $\sqrt{2}$ avec une erreur au plus égale à $1/1280 = 0,0008 < 10^{-3}$.

En effet on alors $m_0 = 1,45 > \sqrt{2}$ et donc on prend donc $a_1 = a_0 = 1,4$ et $b_1 = m_0 = 1,45$ de sorte que $m_1 = 1,425 > \sqrt{2}$. On prend alors $a_2 = a_1 = 1,4$ et $b_2 = m_1 = 1,425$ de sorte que $m_2 = 1,4125 < \sqrt{2}$. On pose alors $a_3 = m_2 = 1,4125$ et $b_3 = b_2 = 1,425$ de sorte que $m_3 = 1,41875 > \sqrt{2}$. On pose alors $a_4 = a_3 = 1,4125$ et $b_4 = m_3 = 1,41875$ de sorte que $m_4 = 1,415625 > \sqrt{2}$. On pose alors $a_5 = a_4 = 1,4125$ et $b_5 = m_4 = 1,415625$ de sorte que $m_5 = 1,4140625 < \sqrt{2}$. On pose alors $a_6 = m_5 = 1,4140625$ et $b_6 = b_5 = 1,415625 > \sqrt{2}$ de sorte que $m_6 = 1,41484375 > \sqrt{2}$. On pose alors $a_7 = a_6 = 1,4140625$ et $b_7 = m_6 = 1,41484375$

de sorte que $m_7 = 1,414453125 > \sqrt{2}$ et donc $a_8 = 1,4140625$ et $b_8 = 1,414453125$. Ce qui implique que $1,4140625 < \sqrt{2} < 1,414453125$.

On voit clairement que ce n'est qu'après 6 itérations que l'on obtient des valeurs approchées de $\sqrt{2}$ avec deux décimales exactes et une erreur au plus égale à $0,0016$ et que ce n'est qu'à la septième itération que l'erreur est réduite à moins de $0,0008 < 10^{-3}$ et que l'on obtient une valeur approchée avec 3 décimales exactes. On peut donc affirmer que $\sqrt{2} \approx 1,414$ à $10^{-3}-$près par défaut ce qui signifie que $1,414 < \sqrt{2} < 1,414 + 10^{-3} = 1,415$.

Le procédé de dichotomie est assez simple mais il "converge lentement" comme on vient de le voir. Cependant il permet de localiser la solution cherchée dans un intervalle assez petit.

Pour l'approximation de la racine carrée, nous donnerons un autre procédé qui "converge plus vite" i.e. qui permet d'atteindre une valeur approchée rationnelle (décimale) avec la même précision en beaucoup moins d'itérations.

En tout cas cet exemple simple montre clairement comment les suites convergentes apparaissent de façon naturelle dans la recherche d'une valeur approchée de la racine carrée.

Pour donner un sens rigoureux aux considérations heuristiques précédentes, nous allons introduire les concepts de "convergence" et de "limite" d'une suite, étudier les moyens d'établir cette convergence en donnant des règles de calcul des limites dans la pratique.

En conclusion, d'un point de vue géométrique il existe bien une grandeur réelle mesurable (correspondant à une longueur) mais non rationnelle ℓ notée $\sqrt{2}$ dont le carré est 2. Cette grandeur peut être approchée par des nombres rationnels aussi bien par défaut que par excès avec une précision $\varepsilon > 0$ aussi petite que l'on veut, donnée à l'avance. Cette grandeur sera représentée par un nombre réel irrationnel, élément d'un nouvel ensemble noté $\mathbf{R}$ et appelé *ensemble des nombres réels* (voir appendice pour une idée de la construction de cet ensemble).

1.1.3 La structure de corps archimédien complet des nombres réels

Nous avons déja observé que l'ensemble $\mathbf{Q}$ des nombres rationnels comportait beaucoup de "trous", ce qui le rendait insuffisant pour traiter certains problèmes de la géométrie élémentaire, puisque bon nombre de longueurs ne peuvent pas être calculèes de façon exacte à l'aide des nombres rationnels.

Pour pallier à ces inconvénients, il est apparu nécessaire de construire rigoureusement un nouvel ensemble noté $\mathbf{R}$ obtenu à partir de $\mathbf{Q}$ en "bouchant tous ses trous" ; l'objectif étant d'obtenir un ensemble "sans trous" au sens intuitif où ce serait un ensemble "continu" à l'image des points d'une droite.

Il existe plusieurs méthodes de construction de l'ensemble des nombres réels à partir des nombres rationnels. On démontre heureusement qu'elles sont toutes équivalentes au sens où les objets construits ont une structure de "corps commutatif archimédien complet" en un sens qui sera précisé ci-dessous et qu'un tel objet est unique à isomorphisme près (théorème difficile). Nous voilà rassurés, non ?

La construction présentée brièvement en appendice est assez intuitive et basée sur la notion de coupure.

Cependant, autant il est facile de comprendre le nombre irrationnel $\sqrt{2}$ en termes de coupure, autant il est vain d'essayer de chercher à quelle coupure correspond le nombre réel π.

En fait dans la pratique , pour les raisons invoquées plus haut, la façon dont on a défini l'ensemble des nombres réels importe peu. Ce qui est important et doit être connu et maitrisé, ce sont les propriétés du corps des nombres réels qui lui confère une structure particulièrement riche, avec cette idée intuitive qu'il s'obtient à partir de $\mathbf{Q}$ en "bouchant tous les trous" (certains étant plus faciles à boucher comme $\sqrt{2}$ que d'autres comme e et π).

En fait, nous verrons que tout nombre réel admet un développement décimal illimité, ce qui est une façon plus naturelle et plus intuitive de représenter les nombres réels : c'est ainsi que $1 = 0,999999999\cdots$, $\sqrt{2} = 1,414213562\cdots$, $e = 2,718281828\cdots$ et $\pi = 3,141592654\cdots$, etc $\cdots$

La construction des nombres réels basée sur les développements décimaux illimités, quoique naturelle et intuitive, n'en est pas moins délicate et techniquement sophistiquée (voir l'ouvrage de référence Cours de Mathématiques L1 tout en un). Dans tous les cas, l'ensemble ordonné $\mathbf{R}$ peut être représenté géométriquement par une droite affine orientée munie d'une origine O symbolisant le nombre réel 0. Chaque nombre réel x est alors représenté par un point unique M de la droite de telle sorte que si $x > 0$ (resp. $x < 0$) le segment OM soit orienté positivement (resp. négativement) et sa longueur soit égale à $|x|$. Il en résulte que l'ensemble $\mathbf{R}$ est d'une certaine façon "continu" (sans "trou") à l'image de la droite qui le représente géométriquement. Cette propriété se traduit en disant que l'ensemble $\mathbf{R}$ est "complet" comme cela sera expliqué ci-dessous.

Nous admettrons dans ce cours qu'il existe un ensemble $\mathbf{R}$ contenant $\mathbf{Q}$ muni de

deux opérations internes l'addition notée + et la multiplication notée $\cdot$ et d'une relation d'ordre total notée $\leq$ qui étendent les opérations internes et la relation d'ordre correspondantes sur $\mathbf{Q}$ de telle sorte que $(\mathbf{R}, +, \cdot, \leq)$ soit un "corps commutatif archimédien complet" dans le sens où les propriétés suivantes sont satisfaites.

Propriété 1 : L'addition + sur $\mathbf{R}$ vérifie les propriétés suivantes :

1. $\forall x \in \mathbf{R}, \forall y \in \mathbf{R}, \forall z \in \mathbf{R}, \quad x + (y + z) = (x + y) + z$,
   (*associativité* de l'addition).
2. $\forall x \in \mathbf{R}, \quad x + 0 = 0 + x = x$,
   (0 est l'*élément neutre* pour l'addition).
3. Pour tout $x \in \mathbf{R}$, il existe un nombre réel unique, noté $-x \in \mathbf{R}$ et appelé l'*opposé* de x, tel que $x + (-x) = (-x) + x = 0$,
4. $\forall x \in \mathbf{R}, \forall y \in \mathbf{R}, \quad x + y = y + x$,
   (*commutativité* de l'addition).

Ces quatre propriétés se résument en disant que $(\mathbf{R}, +)$ est un "groupe abelien" (ou commutatif).

Propriété 2 : La multiplication (ou produit) notée $\cdot$ vérifie les propriétés suivantes :

5. $\forall x \in \mathbf{R}, \forall y \in \mathbf{R}, \forall z \in \mathbf{R}, \quad x \cdot (y \cdot z) = (x \cdot y) \cdot z$,
   ("associativité" de la multiplication),
6. $\forall x \in \mathbf{R}, \quad x \cdot 1 = 1 \cdot x$,
   (1 est l'"élément unité"),
7. tout $x \in \mathbf{R} \backslash \{0\}$ admet un *inverse* unique noté $x^{-1} \in \mathbf{R}$ tel que $x \cdot x^{-1} = x^{-1} \cdot x = 1$,
8. $\forall x \in \mathbf{R}, \forall y \in \mathbf{R}, \forall z \in \mathbf{R}, \quad x \cdot (y + z) = x \cdot y + x \cdot z$,
   ("distributivité" de la multiplication par rapport à l'addition),
9. $\forall x \in \mathbf{R}, \forall y \in \mathbf{R}, \quad x \cdot y = y \cdot x$,
   ("commutativité" de la multiplication)

Les propriétés 1 à 9 se résument en disant que $(\mathbf{R}, +, \cdot)$ est un "corps commutatif".

Nous allons maintenant décrire les propriétés de la relation d'ordre $\leq$ sur le corps $\mathbf{R}$ des nombres réels et sa compatibilité avec les opérations algébriques.

Propriété 3 : La relation d'ordre $\leq$ sur $\mathbf{R}$ vérifie les propriétés suivantes :

10. Pour tout $x \in \mathbf{R}$ et $y \in \mathbf{R}$, on a ou bien $x \leq y$ ou bien $y \leq x$,
    ($\leq$ est une *relation d'ordre total*).
11. Pour tout $x \in \mathbf{R}, y \in \mathbf{R}$ et $z \in \mathbf{R}$ on a $x \leq y \Longrightarrow x + z \leq y + z$,
    (*compatibilité de l'addition* avec la relation d'ordre).
12. Pour tout $x \in \mathbf{R}, y \in \mathbf{R}$ et $a \in \mathbf{R}^+$ on a $x \leq y \Longrightarrow a \cdot x \leq a \cdot y$,
    (*compatibilité de la multiplication* avec la relation d'ordre).

13. Pour tout $x \in \mathbf{R}$ et tout $y \in \mathbf{R}_+^*$ il existe un entier $N > 1$ tel que $N \cdot y > x$ ("Propriété d'Archimède").

Propriété 4 : (*Propriété de la borne supérieure*).

14. Toute partie $A \subset \mathbf{R}$ non vide et majorée de $\mathbf{R}$ possède une borne supérieure.

Les propriétés de (1) à (14) se résument en disant que $(\mathbf{R}, +, \cdot, \leq)$ est un "corps commutatif archimédien complet".

Remarque.
Attention la propriété 12 n'est valable que si $a > 0$. Dans le cas où $a < 0$, on obtient l'inégalité renversée i.e.

$$x \leq y \text{ et } a < 0 \Longrightarrow a \cdot x \geq a \cdot y.$$

En effet si $x \leq y$ on obtient d'après (11), $x + (-y) \leq y + (-y)$ et donc $x - y \leq 0$. En appliquant de nouveau la propriété (11), on obtient $(-x) + x - y \leq -x$ et donc par associativité, on en déduit que $-y \leq -x$. En multipliant chaque membre de cette inégalité par $-a > 0$, on obtient l'inégalité $(-a) \cdot (-y) \leq (-a) \cdot (-x)$ i.e. $a \cdot x \geq a \cdot y$.

Pour expliquer la dernière propriété qui exprime que $\mathbf{R}$ est "complet" ("sans trous"), rappelons quelques définitions supplémentaires.

Rappelons d'abord que si $A \subset \mathbf{R}$ ests une partie non vide, le *plus grand élément* de A est l'unique nombre réel $M \in A$ tel que $\forall x \in A, a \leq M$. Ce nombre est noté $M = \max A$. On définit de la même façon le *plus petit élément* de A et on le note $\min A$. Il est clair que toute partie finie non vide de $\mathbf{R}$ admet un *plus grand élément* et un *plus petit élément*.

On dit qu'une partie $A \subset \mathbf{R}$ est *minorée* (resp. *majorée*) si par définition il existe un nombre réel $m \in \mathbf{R}$ (resp. $M \in \mathbf{R}$) tel que pour tout $x \in A$, on a $m \leq x$ (resp. $x \leq M$). Un tel nombre réel est appelé *un minorant* (resp. un *majorant*) de A.

Il est clair que si m (resp. M) est un minorant (resp. majorant) de A, alors tout nombre réel $m' < m$ (resp. $M' > M$ est encore un minorant (resp. majorant) de A.

Si $A \subset \mathbf{R}$ est une partie non vide et majorée de $\mathbf{R}$, on définit alors la *borne supérieure* de A dans $\mathbf{R}$ comme le nombre réel le plus petit de tous les majorants de A, lorsqu'il existe. On le note $\sup A$.

On définit de façon analogue la *borne inférieure* d'une partie non vide et minorée $A \subset \mathbf{R}$ comme le nombre réel le plus grand parmi tous les minorants de A, lorsqu'il existe. On le note $\inf A$.

Il est clair que si une partie non vide $A \subset \mathbf{R}$ possède un plus grand élément $M := \max A$, alors A admet une borne supérieure qui est égale à M i.e. $\sup A = \max A$. Mais la réciproque n'est pas vraie. En effet, l'ensemble $A := \{x \in \mathbf{R}; x < 1\}$ est non vide et majoré et ne possède pas de plus grand élément, mais il possède une borne supérieure qui est $\sup A = 1$ qui n'appartient pas à A. Par ailleurs, l'ensemble $B := \{x \in \mathbf{R}; x \leq 1\}$ a un plus grand élément qui est $\max B = 1$ et donc une borne supérieure égale à $\sup B = 1$ qui appartient à B.

Il faut observer que l'existence d'une borne supérieure pour une partie non vide et majorée de $\mathbf{R}$ n'est pas évidente. Pour s'en convaincre, il suffit de remarquer que cette notion peut se définir dans $(\mathbf{Q}, \leq)$ muni de sa relation d'ordre et de se reporter à l'exercice 5 de la page 29 qui donne un exemple de partie non vide et majorée de $\mathbf{Q}$ qui n'admet pas de borne supérieure dans $(\mathbf{Q}, \leq)$.

La propriété (14) est un théorème d'existence difficile à démontrer et qui découle de la construction de $\mathbf{R}$. Il affirme que si $A \subset \mathbf{R}$ est une partie non vide et majorée de $\mathbf{R}$, il existe un nombre réel $S \in \mathbf{R}$ qui est le plus petit des majorants de A et que l'on appelle la *borne supérieure* de A. Il en résulte que toute partie non vide et minorée de $\mathbf{R}$ admet une borne inférieure (en effet m est un minorant de A si et seulement si $-m$ est un majorant de $-A := \{-a; a \in A\}$ et donc $\inf A = -\sup(-A)$).

On résume les propriétés (1) à (14) en disant que $(\mathbf{R}, +, \cdot; \leq)$ est un corps commutatif archimédien *complet*. On démontre qu'un tel corps est *unique* à isomorphisme près. On ne s'attachera donc pas à une construction précise du corps des nombres réels mais plutôt à ses propriétés telles qu'elles sont énoncées ci-dessus et notamment la propriété de la borne supérieure qui distingue $\mathbf{Q}$ de $\mathbf{R}$ (voir exercice 5). C'est l'absence de borne supérieure dans $\mathbf{Q}$ pour certaines parties non vides et majorées de $\mathbf{Q}$ qui matérialise les "trous" de $\mathbf{Q}$ (voir Appendice 2).

Dans la pratique nous aurons besoin de la caractérisation suivante de la borne supérieure.

Caractérisation de la borne supérieure

Soit $A \subset \mathbf{R}$ une partie non vide et minorée de $\mathbf{R}$, alors le nombre réel $\sup A$ est caractérisé par les conditions suivantes : $S = \sup A$ si et seulement si

(i) Pour tout $x \in A, x \leq S$,

(ii) pour tout $\varepsilon > 0$, il existe $a \in A$ tel que $S - \varepsilon < a \leq S$.

La propriété (i) traduit le fait que S est un majorant de A et la propriété (ii) traduit le fait que tout nombre réel $S'(= S - \varepsilon) < S$ n'est pas un majorant de A autrement dit : S est un majorant de A et tous les majorants de A sont $\geq S$, donc S est le plus

petit des majorants de A.

Il faut bien observer qu'en général $S := \sup A$ n'appartient pas à A comme le montre l'exemple simple des nombres réels $x \in \mathbf{R}$ tels que $x < 1$ dont la borne supérieure est 1. Lorsque $S = \sup A \in A$, on dit que S est le plus grand élément de A et on le note $S = \max A$.

Nous allons maintenant introduire quelques notions qui résultent de ces propriétés et qui seront utiles dans la suite.

Valeur absolue sur R

Pour tout $x \in \mathbf{R}$, on définit la valeur absolue de x comme étant le plus grand des deux nombres réels x et $-x$:

$$|x| := \max\{x, -x\}$$

ce qui signifie que $|x| = x$ si $x \geq 0$ et $|x| = -x$ si $x \leq 0$ de sorte que $|x|$ est toujours un nombre réel positif.

Voici les propriétés essentielles de la valeur absolue :

V1. $\forall x \in \mathbf{R}, \forall y \in \mathbf{R}, \quad |x \cdot y| = |x| \cdot |y|\,,$

V2. $\forall x \in \mathbf{R}, \forall y \in \mathbf{R}, \quad |x + y| \leq |x| + |y|\,,$
(*inégalité triangulaire*)

V3. $|x| = 0 \Longleftrightarrow x = 0.$

Ces propriétés permettent d'exprimer la notion de voisinage et de proximité dans $\mathbf{R}$. En effet soit $a \in \mathbf{R}$ un nombre réel fixé et $\varepsilon > 0$ un nombre réel positif donné. Alors, un nombre réel variable x vérifie $|x - a| \leq \varepsilon$ si et seulement si x vérifie la double inégalité $a - \varepsilon \leq x \leq a + \varepsilon$. Cela veut dire que x est à une distance de de a au plus égale à ε ou encore que x est voisin de a à $\varepsilon-$près.

L'ensemble ainsi obtenu :

$$\bar{I}(a, \varepsilon) := \{x \in \mathbf{R}; a - \varepsilon \leq x \leq a + \varepsilon\} = [a - \varepsilon, a + \varepsilon],$$

est appelé l'intervalle fermé de centre a et de rayon ε. On peut aussi considérer l'intervalle ouvert de centre de centre a et de rayon ε défini comme suit :

$$I(a, \varepsilon) := \{x \in \mathbf{R}; a - \varepsilon < x < a + \varepsilon\} =]a - \varepsilon, a + \varepsilon[.$$

D'une manière générale, si $a \in \mathbf{R}$ et $b \in \mathbf{R}$ sont tels que $a < b$, on définit l'intervalle ouvert d'origine a et d'extrémité b par :

$$]a, b[:= \{x \in \mathbf{R}; a < x < b\}.$$

Il coïncide avec l'intervalle ouvert $I(c, \varepsilon)$, de centre $c := (a+b)/2$ et de rayon $\varepsilon := (b-a)/2$ (à vérifier !).

L'intervalle fermé d'origine a et d'extrémité b est défini par :

$$[a, b] := \{x \in \mathbf{R}; a \leq x \leq b\}.$$

Les intervalles définis par

$$]a, b] := \{x \in \mathbf{R}; a < x \leq b\}, \quad [a, b[:= \{x \in \mathbf{R}; a \leq x < b\}$$

sont dits semi-ouvert à gauche et semi-ouvert à droite respectivement.

Partie entière d'un nombre réel

Voici une conséquence importante de la propriété d'Archimède de $\mathbf{R}$.

Proposition 1.1.3 *Soit $x \in \mathbf{R}$. Alors il existe un entier $n \in \mathbf{Z}$ unique vérifiant la propriété suivante :*

$$(E) \qquad n \leq x < n + 1.$$

Le nombre entier n vérifiant la propriété (E) sera noté $n = \lfloor x \rfloor$ et appelé la *partie entière* de x. Par exemple $\lfloor 2 \rfloor = 2 = \lfloor 2, 5 \rfloor$, $\lfloor -2 \rfloor] = -2 = \lfloor -1, 5 \rfloor$ et $\lfloor -2, 5 \rfloor = -3$.
Démonstration. En effet, observons que si $x \in \mathbf{Z}$ est un nombre entier, alors $n := x$ vérifie la propriété requise et donc $\lfloor n \rfloor = n$.
Supposons maintenant que $x \ni \mathbf{Z}$. D'après la propriété d'Archimède, il existe un entier $N \in \mathbf{N}$ tel que $N > x$.
- Si $x \geq 0$, alors l'ensemble des entiers naturels $p \in \mathbf{N}$ tels que $p \leq x$ est non vide (il contient 0) et majoré par N, il admet donc un plus grand élément $n \in \mathbf{N}$. Cet entier vérifie clairement la propriété requise.
- Si $x < 0$, alors $-x > 0$ est un nombre réel qui n'est pas un entier et donc l'entier $N := \lfloor -x \rfloor \in \mathbf{N}$ vérifie la propriété $N < -x < N + 1$. Il en résulte que l'entier $n := -N - 1$ vérifie les inégalités $n < x < n+1$, ce qui prouve que $\lfloor -x \rfloor = n = -\lfloor -x \rfloor - 1$. □

Voici une propriété importante qui est une conséquence facile du résultat précédent.

Théorème 1.1.4 *Pour tous nombres réels a, b tels que $a < b$, il existe un nombre rationnel $r \in \mathbf{Q}$ (et donc une infinité) tel que $a < r < b$.*
On exprime cette propriété en disant que l'ensemble $\mathbf{Q}$ est dense dans $\mathbf{R}$.

Démonstration. On cherche deux nombres entiers $p \in \mathbf{Z}$ et $q \in \mathbf{N}^*$ tels que $a < p/q < b$ i.e. $qa < p < qb$. Pour ce faire, on commence par choisir, grâce à la propriété d'Archimède, il existe un entier $q > 1$ tel que $q(b-a) > 1$. Alors l'entier $p := \lfloor qa \rfloor + 1$ vérifie $qa < \lfloor qa \rfloor + 1 \leq qa + 1 < qb$ et donc $qa < p < qb$ de sorte que le nombre rationnel p/q convient. □

L'ensemble des nombres irrationnels $\mathbf{R} \setminus \mathbf{Q}$ possède la même propriété.

Corollaire 1.1.5 *Pour tous nombres réels a, b tels que $a < b$, il existe un nombre irrationnel $c \in \mathbf{R} \setminus \mathbf{Q}$ (et donc une infinité) tel que $a < c < b$.*

Démonstration. En effet, comme $a < b$, on $a/\sqrt{2} < b/\sqrt{2}$ et d'après le théorème précédent, il existe un nombre rationnel $r \in \mathbf{Q}$ tel que $a/\sqrt{2} < r < b/\sqrt{2}$, autrement dit $a < r\sqrt{2} < b$. Comme $\sqrt{2} \notin \mathbf{Q}$, on en déduit que $r\sqrt{2} \notin \mathbf{Q}$, ce qui prouve la propriété voulue. □

Remarque.
On sait qu'il est possible de "dénombrer" les nombres rationnels i.e. d'associer à chaque nombre rationnel un nombre entier naturel (un numéro en quelque sorte) de façon biunivoque ou en d'autres termes d'établir l'existence d'une bijection entre $\mathbf{N}$ et $\mathbf{Q}$. On dira que $\mathbf{Q}$ est *dénombrable*. Par contre on peut démontrer que l'ensemble $\mathbf{R}$ n'est pas dénombrable i.e. que si on essayait de quelque manière que ce soit d'attribuer un "numéro différent" à chaque nombre réel, après "épuisement" de tous les entiers, on en oublierait forcément au moins un (voir exercice 3 page 39). Il en résulte que $\mathbf{R} \setminus \mathbf{Q}$ n'est pas dénombrable, ce qui en quelque sorte signifie qu'il y a beaucoup plus de nombres irrationnels que de nombres rationnels.

Exercice 1.
Démontrer que la somme d'un nombre rationnel et d'un nombre irrationnel est un nombre irrationnel.

Exercice 2.
Soient x et y deux nombres rationnels strictement positifs tels que $\sqrt{x}$ et $\sqrt{y}$ soient irrationnels. Démontrer que $\sqrt{x} + \sqrt{y}$ est un nombre irrationnel.

Exercice 3.
Soient x et a deux nombres réels tels que $a \neq 0$ et $|x - a| < |a|$. Démontrer que $a - |a| < x < a + |a|$ et en déduire que x est du signe de a.

Exercice 4.
Soit $x \geq 0$ un nombre réel tel que $x \neq \sqrt{3}$. Posons $y := \frac{x+3}{x+1}$. Calculer $\frac{y-\sqrt{3}}{x-\sqrt{3}}$ et en

déduire que $y - \sqrt{3} < x - \sqrt{3}$.

Exercice 5.
Soit $x \in \mathbf{Q}$ tel que $x > 0$ et $x^2 > 2$. On pose :

$$x' := \frac{1}{2}\left(x + \frac{2}{x}\right).$$

1) Démontrer que $x' \in \mathbf{Q}$ et vérifie $0 < x' < x$ et $x'^2 > 2$.
2) On pose $A := \{x \in \mathbf{Q}^+; x^2 > 2\}$.
a) Démontrer que A est une partie non vide et minorée de $\mathbf{Q}$ qui n'a pas de plus petit élément dans $\mathbf{Q}$.
b) Démontrer que A n'a pas de borne inférieure dans $\mathbf{Q}$. Quelle est sa borne inférieure dans $\mathbf{R}$?
c) Soit $B := \{x \in \mathbf{Q}^+; x^2 < 2\}$. Démontrer que $x \in B \iff 2/x \in A$ et en déduire que B est une partie non majorée n'a pas de plus
Exercice 6.
Soient x, y deux nombres réels tels que $x < y$ et soient $z \in \mathbf{R}$ tel que $0 < z < y - x$. Démontrer qu'il existe un entier $m \in \mathbf{Z}$ tel que $x < mz < y$ (utiliser la propriété d'Archimède).

Exercice 7.
(difficile) On considère l'ensemble suivant :

$$A := \left\{x \in \mathbf{R}; \exists\ p \in \mathbf{Z}, \exists\ q \in \mathbf{Z}, x = p + q\sqrt{2}\right\}$$

et on pose $\alpha := \sqrt{2} - 1$.
1) Démontrer que pour tout $n \in \mathbf{Z}$ et $x \in A$, on a $nx \in A$.
2) Démontrer par récurrence que pour tout $n \in \mathbf{N}$, on a $\alpha^n \in A$.
3) Démontrer que $0 < \alpha < 1/2$. En déuire que pour tout $n \in \mathbf{N}^*$ on a $0 < \alpha^n < 1/n$.
4) Soient $x, y \in \mathbf{R}$ tels que $0 < x < y$. Démontrer qu'il existe un entier $n \in \mathbf{N}$ tel que $\alpha^n < y - x$ (utiliser la propriété d'Archimède).
5) En utilsant l'exercice 7, démontrer qu'il existe $a \in A$ tel que $x < a < y$.
Cette propriété se traduit en disant que l'ensemble A est dense dans $\mathbf{R}$. (Comparer avec le théorème 1.4).

1.2 Notion de convergence et limite d'une suite

On rappelle qu'une *suite* de nombres réels est une application $u : \mathbf{N} \longrightarrow \mathbf{R}$ qui à chaque entier $n \in \mathbf{N}$ associe un nombre réel $u(n)$ encore noté u_n. On parle alors de la suite $(u_n)_{n\geq 0}$ de terme général u_n, appelé aussi le *terme de rang* n de la suite $(u_n)_{n\geq 0}$. Il arrive que l'application u soit définie sur une partie infinie $I \subset \mathbf{N}$, on parle dans ce cas de la suite $(u_n)_{n\in I}$ indexée par I.

1.2.1 Suites convergentes

Nous allons introduire un concept fondamental en Analyse qu'il faudra bien maitriser et savoir utiliser.

Définition 1.2.1 *On dit que la suite $(u_n)_{n\geq 0}$ converge dans $\mathbf{R}$, s'il existe un nombre réel $\ell \in \mathbf{R}$ tel que pour tout $\varepsilon > 0$, il existe un rang $N \geq 1$ tel que pour tout $n \geq N$, on ait $|u_n - \ell| \leq \varepsilon$. On dira dans ce cas que la suite $(u_n)_{n\geq 0}$ converge vers ℓ.*

Il y a plusieurs remarques importantes à faire à propos de cette définition. Commençons d'abord par démontrer la propriété élémentaire suivante.

Proposition 1.2.2 *Soit $(u_n)_{n\geq 0}$ une suite de nombres réels qui converge vers ℓ. Alors le nombre réel ℓ est unique. On l'appelera la limite de la suite $(u_n)_{n\in\mathbf{N}}$ et on écrira $\ell = \lim_{n\to+\infty} u_n$.*

Démonstration. En effet, supposons que la suite (u_n) converge vers $\ell_1 \in \mathbf{R}$ et $\ell_2 \in \mathbf{R}$ et soit $\varepsilon > 0$ un nombre réel arbitraire. En appliquant la définition de la convergence à chacun de ces nombres réels, on aboutit à l'existence d'un entier $N_1 \geq 1$ (resp. $N_2 \geq 1$) tel que pour tout $n \geq N_1$ (resp. $n \geq N_2$) on ait $|u_n - \ell_1| \leq \varepsilon$ (resp. $|u_n - \ell_2| \leq \varepsilon$). Posons $N := \max\{N_1, N_2\}$ et écrivons $\ell_1 - \ell_2 = (\ell_1 - u_N) + (u_N - \ell_2)$. En appliquant l'inégalité triangulaire, on obtient $|\ell_1 - \ell_2| \leq |\ell_1 - u_N| + |u_N - \ell_2|$. Il en résulte grâce au choix de N que $|\ell_1 - \ell_2| \leq \varepsilon + \varepsilon = 2\varepsilon$. Comme $\varepsilon > 0$ est arbitrairement petit, il en résulte que $|\ell_1 - \ell_2| = 0$, d'où $\ell_1 = \ell_2$. □

Remarques.

1. Lorsque la suite $(u_n)_{n\geq 0}$ converge vers ℓ, la condition $|u_n - \ell| \leq \varepsilon$ se traduit, en raison de la présence de la valeur absolue, par la double inégalité

$$\ell - \varepsilon \leq u_n \leq \ell + \varepsilon,$$

   qui exprime le fait que u_n est voisin de ℓ à $\varepsilon-$près à partir d'un certain rang N qui dépend de ε, d'où l'importance de la valeur absolue dans la définition de la convergence. Autrement dit la suite $(u_n)_{n\geq 0}$ converge lorsque ses termes sont arbitrairement voisins de sa limite ℓ à partir d'un certain rang N suffisamment grand.
2. Dans les applications, lorsqu'une suite $(u_n)_{n\geq 0}$ converge, il arrive souvent qu'elle donne naissance à un nouveau nombre réel ℓ que l'on ne connait pas à priori. Lorsque $\varepsilon > 0$ est donné, l'entier N à partir duquel on a la double inégalité $|u_n - \ell| \leq \varepsilon$, est alors important d'un point de vue "qualitatif", puisqu'il fournit

le premier terme u_N qui vérifie $|u_N - \ell| \leq \varepsilon$. On dira que u_N est une *valeur approchée* (ou un *approximant*) de ℓ à $\varepsilon-$près. Le nombre réel ε doit être assez petit et représente l'erreur maximale commise dans l'approximation de ℓ par u_N. Il est dans ce cas important de trouver le plus petit entier $N(\varepsilon)$ vérifiant cette propriété. Il représente le nombre minimum d'opérations permettant de calculer ℓ avec une erreur au plus égale à $\varepsilon-$près.

Cependant d'un point de vue "qualitatif", pour démontrer qu'une suite converge, il n'est pas nécéssaire de trouver le plus petit entier $N(\varepsilon)$ satisfaisant aux exigences de la définition, ce qui peut être assez compliqué, il suffit d'en trouver un suffisamment grand.

3. Lorsqu'une suite converge, tous ses termes ont tendance à "s'accumuler" arbitrairement près (i.e. à ε près, ε étant arbitraire) autour d'un même nombre réel à savoir sa limite, à l'exception d'au plus un nombre fini d'entre eux N.
Il en résulte que la nature d'une suite (convergence ou non) ainsi que sa limite, lorsqu'elle existe, ne change pas si l'on modifie ou supprime un nombre fini de termes de cette suite. Par exemple, si $p \geq 1$ est un entier fixé, la suite $(u_{n+p})_{n\geq 0}$, dite tronquée au rang p, est de même nature que la suite $(u_n)_{n\geq 0}$ et a la même limite lorsque celle-ci existe (à vérifier !).

Donnons quelques exemples simples pour illustrer et manipuler ces définitions.

Exemples.

1. Une suite $(u_n)_{n\geq 0}$ est dite *constante* s'il existe $c \in \mathbf{R}$ tel que $u_n = c$ pour tout $n \geq 0$. La suite $(u_n)_{n\geq 0}$ est dite *stationnaire* s'il existe un rang $p \geq 0$ et un nombre réel $c \in \mathbf{R}$ tels que $u_n = c$ pour tout $n \geq p$. Dans ce cas la suite converge vers c (à démontrer en utilisant la définition).
2. La suite $(1/n)_{n\geq 1}$ converge vers 0. En effet pour tout $\varepsilon > 0$ donné, d'après la propriété d'Archimède, il existe un entier $N > 1$ tel que $N > 1/\varepsilon$. Il en résulte que si $n \geq N$ on a $0 < 1/n \leq 1/N \leq \varepsilon$. Le plus petit entier vérifiant cette propriété est facile à déterminer ici, c'est l'entier $N(\varepsilon) := \lfloor 1/\varepsilon \rfloor + 1$.
En fait la propriété d'Archimède ne dit rien d'autre que :
$$\lim_{n\to+\infty} \frac{1}{n} = 0.$$
3. Si $p \geq 1$ est un entier fixé, la suite $(1/n^p)_{n\geq 0}$ converge vers 0.
En effet, comme précédemment, en posant $N = \lfloor 1/\varepsilon \rfloor [1/\varepsilon^{1/p}] + 1$, on obtient pour tout $n \geq N$, $1/n^p \leq 1/N^p \leq \varepsilon$.

4. Posons $u_n := \frac{2n}{n+\sqrt{n}}$ pour $n \geq 1$ et montrons que $\lim_{n\to+\infty} u_n = 2$.
   En effet pour $n \geq 1$, on a :

$$u_n = \frac{2n}{n+\sqrt{n}} = \frac{2(n+\sqrt{n}) - 2\sqrt{n}}{n+\sqrt{n}} = 2 - \frac{2\sqrt{n}}{n+\sqrt{n}}.$$

   D'où $u_n - 2 = -\frac{2\sqrt{n}}{n+\sqrt{n}}$ et donc $|u_n - 2| \leq \frac{2}{\sqrt{n}}$, pour tout $n \geq 1$.
   Soit $\varepsilon > 0$, pour avoir l'inégalité $|u_n - 2| \leq \varepsilon$, il suffit d'avoir l'inégalité $\frac{2}{\sqrt{n}} \leq \varepsilon$ i.e. $n > 4/\varepsilon^2$. Pour cela il suffit de poser $N = [4/\varepsilon^2] + 1$. Alors pour $n \geq N$, on a $\frac{2}{\sqrt{n}} \leq \varepsilon$ et donc pour $n \geq N$, on a $|u_n - 2| \leq \varepsilon$. Ce qui prouve notre assertion. Observer que l'entier N trouvé ici n'est pas le plus petit possible, mais cela suffit à prouver la convergence !

1.2.2 Limites infinies

Lorsqu'une suite $(u_n)_{n\geq 0}$ ne converge pas, on dira par définition qu'elle *diverge*. En fait lorsqu'une suite diverge, elle peut avoir des comportements très variés. Nous allons décrire un type de comportement qui est étroitement lié à la notion de convergence (voir exercice 2).

Définition 1.2.3 *1) On dit qu'une suite $(u_n)_{n\geq 0}$ de nombres réels* a pour limite $+\infty$ *si pour tout nombre réel $A > 0$ il existe un rang $N > 1$ tel que pour tout $n \geq N$, on ait $u_n \geq A$. On dira aussi que la suite $(u_n)_{n\in\mathbf{N}^*}$ tend vers $+\infty$ et on écrira dans ce cas* $\lim_{n\to+\infty} u_n = +\infty$.
2) On dit que la suite $(u_n)_{n\geq 0}$ a *pour limite $-\infty$ si pour tout nombre réel $A > 0$ il existe un rang $N > 1$ tel que pour tout $n \geq N$, on ait $u_n \leq -A$. On dira aussi que la suite $(u_n)_{n\in\mathbf{N}^*}$ tend vers $-\infty$ et on écrira dans ce cas* $\lim_{n\to+\infty} u_n = -\infty$.

On peut faire les mêmes remarques à propos de cette définition que celles faites à propos de la convergence. Observons que la suite $(u_n)_{n\geq 0}$ tend vers $-\infty$ si et seulement si la suite $(-u_n)_{n\geq 0}$ tend vers $+\infty$. Une suite tend vers $+\infty$ lorsque ses termes deviennent arbitrairement grands à partir d'un certain rang. Cette propriété ne change pas si on modifie ou supprime un nombre fini de termes de la suite. Le lien entre les deux notions de limites (finies et infinies) sera établi plus loin.

Donnons quelques exemples pour illustrer cette définition.

Exemples.

1. Soit $p \geq 1$ un entier fixé. Alors on a :

$$\lim_{n\to+\infty} n^p = +\infty.$$

En effet, soit $A > 0$, alors en posant $N = \lfloor A^{1/p} \rfloor + 1$, on en déduit que pour tout entier $n \geq N$, on a $n^p \geq N^p \geq A$, ce qui prouve l'assertion.

2. Soit $a > 1$ un nombre réel. Montrons que :

$$\lim_{n \to +\infty} a^n = +\infty. \tag{1.1}$$

En effet, posons $b := a - 1$ de sorte que $b > 0$ et $a = 1 + b$ et vérifions par récurrence que pour tout $n \in \mathbf{N}$, on a :

$$(1 + b)^n \geq 1 + n \cdot b. \tag{1.2}$$

En effet cette inégalité est évidente pour $n = 0$. Supposons qu'elle soit vérifiée pour un entier $n \geq 0$. Alors on en déduit que $(1 + b)^{n+1} = (1 + b) \cdot (1 + b)^n \geq (1 + b) \cdot (1 + n \cdot b) = 1 + b + n \cdot b + n \cdot b^2 \geq 1 + (n + 1) \cdot b$. Ce qui prouve donc l'inégalité (1.2) au rang $n + 1$.
Pour démontrer (1.1), fixons $A > 0$ arbitraire et posons $N = \lfloor A/b \rfloor + 1$. Alors pour tout $n \geq N$, on a $n \cdot b > N \cdot b > A$. Par suite d'après (1.2), on en déduit que pour tout $n \geq N$, on a $(1 + b)^n > A$, ce qui prouve (1.1).

3. Soit $0 < q < 1$. Il résulte de l'exemple précédent que

$$\lim_{n \to +\infty} q^n = 0.$$

On pose pour $n \geq 1$, $S_n := \sum_{k=0}^{n} q^k = 1 + q + \ldots + q^n$. On vérifie facilement que

$$\forall n \geq 1, \quad (1 - q)S_n = 1 - q^{n+1}.$$

On en déduit alors que

$$\lim_{n \to +\infty} S_n = \frac{1}{1 - q}.$$

De plus on a l'inégalité fondamentale suivante

$$\forall n \geq 1, \ 1 + q + \ldots + q^n < \frac{1}{1 - q}.$$

Exercice 1.
Démontrer en utilisant la définition que la suite définie par $x_n := (-1)^n$, pour $n \in \mathbf{N}$ ne converge pas.

Exercice 2.
Etudier la suite définie par $y_n := (-1)^n/n$ pour $n \in \mathbf{N}^*$.
Etudier la suite définie par $z_n := (1/n)\sin(2\pi n/3)$ pour $n \geq 1$.

Exercice 3.
Démontrer que si (u_n) a pour limite $+\infty$ ou $-\infty$ alors il existe un rang $N \geq 1$ tel que pour tout $n \geq N$, $u_n \neq 0$ et que la suite $(1/u_n)_{n\geq N}$ converge vers 0.

Exercice 4.
Soit $(u_n)_{n\geq 0}$ une suite de nombres réels qui converge vers 0. On suppose qu'il existe un rang $N \geq 1$ tel que $u_n > 0$ pour tout $n \geq N$. Démontrer que la suite $(1/u_n)_{n\geq N}$ converge vers $+\infty$. Que peut-on dire si $(u_n)_{n\geq 0}$ converge vers 0 en changeant de signe ?

Exercice 5.
Soit $b > 1$. Démontrer que :

$$\lim_{n\to+\infty} \frac{b^n}{n!} = 0.$$

(Considérer l'unique entier $p \geq 1$ tel que $p \leq b < p+1$ et vérifier que pour $n \geq p+1$ on a $n! \geq (p+1)^{n-p}p!$.)
Exercice 6.
Calculer :

$$\lim_{n\to+\infty} \frac{3n^3 - 5n^2 + 3n - 7}{2n^3 - 3n^2 - 8n - 11}.$$

Exercice 7.
Soit $(x_n)_{n\in\mathbf{N}}$ une suite de nombres réels telle que $\lim_{n\to+\infty}(x_{n+1} - x_n) = \alpha \in \mathbf{R}$. Démontrer que $\lim_{n\to+\infty} \frac{x_n}{n} = \alpha$. (Se ramener au cas où $\alpha = 0$.)

Exercice 8.
Soit $(y_n)_{n\geq 0}$ une suite de nombres réels qui converge vers une limite $\ell \in \mathbf{R}$ et α un paramètre réel tel que $|\alpha| < 1$.
1) Démontrer qu'il existe une suite unique $(x_n)_{n\geq 0}$ de nombres réels telle que $x_0 = y_0$ et pour $n \geq 1$, $x_n - \alpha x_{n-1} = y_n$. (On exprimera les x_n en fonction des y_n).
2) Démontrer que :

$$\lim_{n\to+\infty} x_n = \frac{\ell}{1-\alpha}.$$

(On commencera par le cas où $\ell = 0$).

Exercice 9.
1) Soit $(x_n)_{n\in\mathbf{N}}$ une suite de nombres réels. On définit la suite de ses moyennes arithmétiques en posant :

$$y_n := \frac{x_0 + \ldots + x_n}{n+1}, \quad n \geq 0.$$

Démonter que si la suite $(x_n)_{n\geq 0}$ converge vers ℓ, alors la suite $(y_n)_{n\geq 0}$ converge vers ℓ. Etudier la réciproque.

2) Démontrer que le résultat est encore valable si $\ell = \pm\infty$.
3) On suppose que la suite $(x_n)_{n\geq 0}$ est monotone. Démontrer que si la suite des moyennes arithmétiques $(y_n)_{n\geq 0}$ converge vers ℓ, alors la suite $(x_n)_{n\geq 0}$ converge vers ℓ.

1.3 Propriétés élémentaires des suites et règles de calcul

Les propriétés énoncées dans ce paragraphe sont élémentaires et seront utiles dans la pratique.

1.3.1 Propriétés élémentaires des suites

Commençons par rappeler quelques définitions déja vues pour les parties de $\mathbf{R}$.

Définition 1.3.1 *1) On dit que la suite $(u_n)_{n\geq 0}$ est majorée dans $\mathbf{R}$ s'il existe un nombre réel B tel que $\forall n \in \mathbf{N},\ u_n \leq B$. On dit alors que B est un majorant de la suite $(u_n)_{n\geq 0}$ dans $\mathbf{R}$ ou que celle-ci est majorée par B.*
2) On dit que la suite $(u_n)_{n\geq 0}$ est minorée dans $\mathbf{R}$ s'il existe un nombre A tel que $\forall n \in \mathbf{N},\ u_n \geq A$.
3) On dit que la suite $(u_n)_{n\geq 0}$ est bornée si la suite est à la fois majorée et minorée.

Observons qu'une suite $(u_n)_n$ est bornée dans $\mathbf{R}$ si et seulement si il existe un réel $M > 0$ tel que $|u_n| \leq M$ pour tout $n \in \mathbf{N}$ (si $\forall n \in \mathbf{N}, A \leq u_n \leq B$, poser $M := \max\{|A|, |B|\}$).

On a alors les propriétés élémentaires suivantes.

Proposition 1.3.2 *Toute suite de nombres réels qui converge dans $\mathbf{R}$ est une suite bornée dans $\mathbf{R}$. Toute suite de nombres réels qui a pour limite $+\infty$ (resp. $-\infty$) est une suite non majorée (resp. non minorée) dans $\mathbf{R}$.*

Démonstration. En effet, supposons d'abord que $\ell := \lim_{n\to+\infty} u_n \in \mathbf{R}$ et fixons $\varepsilon = 1$. Il existe alors par définition un entier $N \geq 1$ tel que $\forall n \geq N, |u_n - \ell| \leq 1$. En posant $\alpha := \max\{1, |u_0 - \ell|, \ldots, |u_{N-1} - \ell|\}$, on en déduit que $\forall n \in \mathbf{N}, |u_n - \ell| \leq \alpha$, ce qui signifie que $\forall n \in \mathbf{N}, \alpha - \ell \leq u_n \leq \alpha + \ell$. La suite (u_n) est donc bornée.
Supposons maintenant que $\lim_{n\to+\infty} u_n = +\infty$. Alors par définition pour tout $A > 0$, il existe $N \in \mathbf{N}$ tel que $\forall n \geq N, u_n > A$. Il en résulte en particulier qu'aucun nombre réel $A > 0$ n'est un majorant de la suite (u_n) et donc celle-ci n'est pas majorée dans $\mathbf{R}$. Le même raisonnement montre que si $\lim_{n\to+\infty} u_n = -\infty$, la suite (u_n) n'est pas minorée dans $\mathbf{R}$. □

La réciproque de cette proposition est fausse comme le montrent les contre-exemples suivants.

Exemples.

1. La suite définie par $u_n := (-1)^n$ pour $n \geq 0$ est bornée mais elle n'a pas de limite (voir exercice 1).
2. La suite définie par $u_n := (-1)^n \cdot n$ pour $n \geq 0$ n'est ni majorée ni minorée et n'a pas de limite.

Le résulat suivant est utile dans la pratique.

Proposition 1.3.3 *Soient $(a_n)_{n\in\mathbf{N}}$ une suite qui converge vers 0 et $(u_n)_{n\in\mathbf{N}}$ une suite bornée. Alors la suite $(a_n u_n)_{n\in\mathbf{N}}$ converge vers 0.*

Démonstration. Par hypothèse il existe $M > 0$ tel que : $\forall n \in \mathbf{N}$, $|u_n| \leq M$. Il en résulte que pour tout $n \in \mathbf{N}$, on a $|a_n u_n| \leq M|a_n|$. Fixons $\varepsilon > 0$. Comme $\lim_{n\to+\infty} a_n = 0$, il existe un entier $N > 1$ tel que pour tout $n \geq N$, $|a_n| \leq M\varepsilon$. Comme $M\varepsilon$ est petit lorsque ε est petit, on en déduit que la suite $(a_n u_n)_{n\in\mathbf{N}}$ converge vers 0. □

1.3.2 Opérations algébriques sur les limites

Voici quelques propriétés simples qui seront utiles dans la pratique.

Proposition 1.3.4 *Soient $(u_n)_{n\in\mathbf{N}}$ et $(v_n)_{n\in\mathbf{N}}$ deux suites de nombres réels qui convergent vers les nombres réels a et b respectivement. Alors on a les propriétés suivantes :*
1) La suite $(u_n + v_n)_{n\in\mathbf{N}}$ converge vers $a + b$ i.e. *:*

$$\lim_{n\to+\infty}(u_n + v_n) = \lim_{n\to+\infty} u_n + \lim_{n\to+\infty} v_n. \tag{1.3}$$

("formule d'addition").
2) La suite $(u_n \cdot v_n)_{n\in\mathbf{N}}$ converge vers $a \cdot b$ i.e. *:*

$$\lim_{n\to+\infty}(u_n \cdot v_n) = (\lim_{n\to+\infty} u_n) \cdot (\lim_{n\to+\infty} v_n). \tag{1.4}$$

("formule du produit").
3) Si $b \neq 0$, il existe un rang $p \geq 0$ tel que $v_n \neq 0$ pour tout $n \geq p$ et la la suite $(u_n/v_n)_{n\geq p}$ converge vers a/b i.e. *:*

$$\lim_{n\to+\infty}(u_n/v_n) = (\lim_{n\to+\infty} u_n)/(\lim_{n\to+\infty} v_n). \tag{1.5}$$

("formule du quotient").

Démonstration. Les démonstrations de ces propriétés sont assez faciles et n'utilisent que la définition en plus de quelques manipulations algébriques simples. Donnons à titre d'exemple la démonstation de la dernière propriété.
Grâce à la propriété 2, on se ramène au cas où $u_n = 1$ pour tout n. Puisque $b \neq 0$, en considérant la suite v_n/b on on peut se ramener au cas ou $b = 1$. On applique la définition de la convergence de (v_n) vers 1 en prenant $\varepsilon := 1/2$ qui est strictement positif. Il existe alors un rang $N_0 \geq 1$ tel que pour tout $n \geq N_0$, $|v_n - 1| \leq 1/2$. Il en résulte grâce à l'inégalité triangulaire que pour tout $n \geq N_0$, on a $|v_n| \geq ||v_n| - 1| \geq 1 - 1/2 = 1/2 > 0$.
Fixons $n \geq N_0$ et observons que puisque $|v_n| \geq 1/2$, on a :

$$|\frac{1}{v_n} - 1| \leq 2|1 - v_n|.$$

Fixons $\varepsilon > 0$. Comme $\lim v_n = 1$, il existe un rang $N_1 \geq 1$ tels que pour tout $n \geq N_1$, $|v_n - 1| \leq \varepsilon$.
Posons $N := \max\{N_0, N_1\}$. Il résulte de ce qui précède que pour tout $n \geq N$ on a :

$$|\frac{1}{v_n} - 1| \leq 2\varepsilon,$$

ce qui prouve notre assertion. □

Les trois formules fondamentales énoncées pour les limites finies sont encore valables si l'une ou les deux limites sont infinies à condition que l'opération correspondante sur les limites ait un sens comme le montrent les résultats suivants.

Proposition 1.3.5 *Soit $(u_n)_{n\in\mathbf{N}}$ une suite de nombres réels qui converge vers vers un nombre réel $a \in \mathbf{R}$ et $(v_n)_{n\in\mathbf{N}}$ une suite de nombres réels qui a pour limite $+\infty$ (resp. $-\infty$). Alors on a les propriétés suivantes :*
1) la suite $(u_n + v_n)_{n\in\mathbf{N}}$ a pour limite $+\infty$ (resp. $-\infty$) ;
2) si $a \neq 0$, la suite $(u_n \cdot v_n)_{n\in\mathbf{N}}$ a une limite infinie de même signe que (resp. de signe opposé à) celle de (v_n) si $a > 0$ (resp. $a < 0$).

Proposition 1.3.6 *Soit $(u_n)_{n\in\mathbf{N}}$ et $(v_n)_{n\in\mathbf{N}}$ deux suites ayant des limites infinies. Alors on a les propriétés suivantes :*
1) si les deux suites $(u_n)_{n\in\mathbf{N}}$ et $(v_n)_{n\in\mathbf{N}}$ ont des limites infinies de même signe, la suite $(u_n + v_n)_{n\geq 0}$ a une limite infinie de même signe.
2) La suite $(u_n \cdot v_n)_{n\in\mathbf{N}}$ a pour limite $+\infty$ (resp. $-\infty$) si les deux suites $(u_n)_{n\in\mathbf{N}}$ et $(v_n)_{n\in\mathbf{N}}$ ont des limites infinies de même signe (resp. de signe opposés).

Remarque.
Les résultats précédents montrent que les règles de calcul pour les limites finies s'étendent

au cas des limites infinies sous certaines conditions qui peuvent être résumées suivant un tableau.
De façon plus précise, supposons que les suites $(u_n)_{n\geq 0}$ et $(v_n)_{n\geq 0}$ ont des limites a et b respectivement (finies ou infinies). Alors on a les propriétés suivantes :

1. Si a et b ne sont pas tous les deux infinis et de signes opposés, alors la formule d'addition des limites (1.3) est encore valable avec la convention :

   (i) $a + (+\infty) = +\infty$ si $a \neq -\infty$ et $b = +\infty$,

   (ii) $a + (-\infty) = -\infty$ si $a \neq +\infty$ et $b = -\infty$.

   Par exemple si $u_n := -1 + 1/n$ et $v_n := n$ pour $n \geq 1$ on a $\lim_{n\to+\infty} u_n = -1$ et $\lim_{n\to+\infty} v_n = +\infty$. On a bien $\lim_{n\to+\infty}(u_n + v_n) = +\infty = (-1) + (+\infty) = +\infty$.
   Dans le cas où $a = +\infty$ et $b = -\infty$, on ne peut rien dire en général sur la limite de la somme $u_n + v_n$ lorsque $n \to +\infty$ et la somme "$(+\infty) + (-\infty)$" n'est pas bien définie. On parle alors de la forme indéterminée "$(+\infty) + (-\infty)$". Une étude plus détaillée de la somme $u_n + v_n$ pour n assez grand permet parfois par "compensation" entre les "termes dominants" de lever cette indétermination et de conclure à l'existence ou non d'une limite de $u_n + v_n$ lorsque $n \to +\infty$.
   Par exemple, posons $u_n := n + n^\alpha$ et $v_n := -n$ pour $n \geq 1$, où α est un paramètre réel, alors on a $\lim_{n\to+\infty} u_n = +\infty, \lim_{n\to+\infty} v_n = -\infty$ alors que $\lim_{n\to+\infty}(u_n + v_n) = +\infty$ si $\alpha > 0, \lim_{n\to+\infty}(u_n + v_n) = 1$ si $\alpha = 0$ et $\lim_{n\to+\infty}(u_n + v_n) = 0$ si $\alpha < 0$.

2. Lorsque $a \neq 0$ et $b = \pm\infty$ le produit $a \cdot b$ peut être défini en posant $a \cdot b = \mathrm{sgn}(a) \cdot b$ avec les conventions $(-1)(+\infty) = +1(-\infty) = -\infty$ et $(+1)(+\infty) = (-1)(-\infty) = +\infty$. Dans ce cas, la formule du produit des limites (1.4) est encore valable.
   Par exemple si $u_n = -1 + 1/n$ et $v_n = n$ pour $n \geq 1$, alors $\lim_{n\to+\infty} u_n = -1, \lim_{n\to+\infty} v_n = +\infty$ et $\lim_{n\to+\infty} u_n v_n = \lim_{n\to+\infty}(-n + 1) = -\infty = (-1) \cdot (+\infty)$.
   Par contre dans le cas où $a = 0$ et $b = \pm\infty$, on ne peut rien dire sur la limite du produit $u_n \cdot v_n$ lorsque $n \to +\infty$ et on parle de la forme indéterminée "$0 \cdot (\infty)$". Là encore, seule une étude plus détaillée du produit $u_n \cdot v_n$ permet parfois par "compensation" de lever cette indétermination.
   Par exemple si $u_n := 1/n^\alpha$ et $v_n := n + 1$ pour $n \in \mathbf{N}$, où $\alpha > 0$ est un paramètre réel, on a $\lim_{n\to+\infty} u_n = 0, \lim_{n\to+\infty} v_n = +\infty$ alors que par compensation, on a $u_n \cdot v_n = n^{1-\alpha} + 1/n^\alpha$ pour $n \in \mathbf{N}$ et donc $\lim_{n\to+\infty} u_n v_n = +\infty$ si $\alpha < 1$ et $\lim_{n\to+\infty} u_n v_n = 1$ si $\alpha = 1$ et $\lim_{n\to+\infty} u_n v_n = 0$ si $\alpha > 1$.

3. Lorsque $b \neq 0$, le calcul de la limite du quotient (u_n/v_n) se ramène au cas précédent en convenant que $1/(\infty) = 0$. Dans ce cas le quotient a/b est bien défini et la formule du quotient des limites (1.5) est encore valable.
   Les cas d'indétermination $(\pm\infty)/0$ se traitent là encore par une étude plus détaillée du quotient u_n/v_n lorsque $n \to +\infty$ qui permet parfois de lever l'indetermination.

Exercice 1.
Calculer la limite suivante :

$$\lim_{n\to+\infty}(n^\alpha - n),$$

où $\alpha \in \mathbf{R}$ est un paramètre.

Exercice 2.
Posons $u_n := \sqrt{n+1} - \sqrt{n}$ pour $n \geq 0$.
1) Démontrer que

$$u_n = \frac{1}{\sqrt{n+1}+\sqrt{n}},\ \forall n \in \mathbf{N}^*.$$

En déduire $\lim_{n\to+\infty} u_n = 0$.
2) Calculer la limite suivante :

$$\lim_{n\to+\infty} \sqrt{n}(\sqrt{n+1} - \sqrt{n}).$$

Exercice 3.
On définit la suite $(u_n)_{n\geq 1}$ par la formule suivante :

$$x_n := 2\cos(1/n^2) + 3\sum_{p=1}^{n} \frac{1}{\sqrt{p+1}},\ n \in \mathbf{N}^*.$$

Démontrer que pour tout $n \geq 1$, $u_n \geq 3\sqrt{n+1} - 5$ et calculer la limite de la suite $(u_n)_{n\geq 1}$.

Exercice 4.
Etudier les limites des suites suivantes :

$$\begin{aligned} x_n &:= \sqrt{n^2+2n-1} - \sqrt{n^2+5n-6}, \\ y_n &:= \frac{n\sin(n!)}{n^2+n-1}, \\ z_n &:= (-1)^n \frac{3n-2}{n+5}. \end{aligned}$$

Exercice 5.
Soient P et Q deux polynômes à coefficients réels de degré p et $q \geq 1$ respectivement.
Calculer la limite suivante :

$$\ell := \lim_{n\to+\infty} \frac{P(n)}{Q(n)}.$$

1.3.3 Passage à la limites dans les inégalités

Voici maintenant des propriétés d'encadrement très utiles dans les calculs de limites. Ces propositions résultent facilement des définitions.

On notera $\overline{\mathbf{R}} := \mathbf{R} \cup \{-\infty, +\infty\}$, où $-\infty$ et $+\infty$ sont deux nouveaux éléments représentant les limites infinies avec la relation d'ordre suivante : pour tout $x \in \mathbf{R}$, $-\infty < x < +\infty$.

Proposition 1.3.7 (Principe de conservation des inégalités larges) *Soient $(u_n)_{n\in\mathbf{N}}$ et $(v_n)_{n\in\mathbf{N}}$ deux suites ayant pour limites a et b respectivement dans $\overline{\mathbf{R}}$. Supposons qu'il existe un rang $p \in \mathbf{N}$ tel que $u_n \leq v_n$ pour tout $n \geq p$. Alors on a $a \leq b$.*

Démonstration. Supposons que les limites a et b sont finies. Soit $\varepsilon > 0$. Par définition de la convergence de (u_n), il existe un rang $N_1 \in \mathbf{N}$ tel que pour tout $n \geq N_1$ on ait $|u_n - a| \leq \varepsilon$. De la même façon, il existe un entier $N_2 \in \mathbf{N}$ tel que pour tout $n \geq N_2$ on ait $|v_n - b| \leq \varepsilon$. Posons $N := \max\{N_1, N_2\}$. On a alors $a - \varepsilon \leq u_N \leq v_N \leq b + \varepsilon$. On en déduit que $a - \varepsilon \leq b + \varepsilon$, pour tout $\varepsilon > 0$, ce qui implique que $a \leq b$.
Dans le cas où l'une des limites est infinie, on procède de la même façon. □

Proposition 1.3.8 (Théorème des suites encadrées) *Soient $(u_n)_{n\in\mathbf{N}}$ une suite de nombres réels. On suppose qu'il existe deux suites de nombres réels $(a_n)_{n\in\mathbf{N}}$ et $(b_n)_{n\in\mathbf{N}}$ et un entier $p > 1$ tels que pour tout $n \geq p$ on ait $a_n \leq u_n \leq b_n$. Alors on a les propriétés suivantes :*

1. $\lim_{n\to+\infty} a_n = \ell = \lim_{n\to+\infty} b_n \implies lim_{n\to+\infty} u_n = \ell$.
2. $\lim_{n\to+\infty} a_n = +\infty \implies \lim_{n\to+\infty} u_n = +\infty$.
3. $\lim_{n\to+\infty} b_n = -\infty \implies \lim_{n\to+\infty} u_n = -\infty$.

Démonstration. Supposons que les limites a et b sont finies. Soit $\varepsilon > 0$. Par définition de la convergence de (a_n), il existe un rang $N_1 \in \mathbf{N}$ tel que pour tout $n \geq N_1$ on ait $a - \varepsilon \leq a_n \leq a + \varepsilon$. De la même façon, il existe un entier $N_2 \in \mathbf{N}$ tel que pour tout $n \geq N_2$ on ait $b - \varepsilon \leq b_n \leq b + \varepsilon$. Posons $N := \max\{N_1, N_2\}$. On a alors pour tout $n \geq N$, $a - \varepsilon \leq a_n \leq u_n \leq b_n \leq b + \varepsilon$. Comme $a = b$, il en résulte que pour tout $n \geq N$, $a - \varepsilon \leq u_n \leq a + \varepsilon$. Cela prouve que (u_n) converge vers a.
Les autres cas se traitent de la même façon et sont laissés en exercice. □

Attention, en général, on ne peut passer à la limite dans une inégalié que si on sait que chaque membre de cette inégalité a une limite. Dans le cas du théorème des suites encadrées, c'est le fait que les deux "suites extrêmes" tendent vers la même limite qui implique l'existence de la limite de la suite encadrée.

Exemple.
Posons pour $n \geq 1$:

$$u_n := \sum_{k=1}^{n} \frac{n}{k+n^2} = \frac{n}{1+n^2} + \ldots + \frac{n}{n+n^2}.$$

Ainsi u_n est la somme de n termes dont le plus petit est $\frac{n}{n+n^2}$ et le plus grand est $\frac{n}{1+n^2}$. Il en résulte que :

$$\forall n \geq 2,\ n \cdot \frac{n}{n+n^2} < u_n < n \cdot \frac{n}{1+n^2}.$$

Posons $a_n = \frac{n^2}{n+n^2}$ et $b_n := \frac{n^2}{1+n^2}$. En utilisant la définition (voir exemple 2 du paragraphe 1), on montre facilement que $\lim_{n\to+\infty} a_n = 1 = \lim_{n\to+\infty} b_n$. Comme $a_n < u_n < b_n$ pour tout $n \geq 1$, on en déduit grâce au théorème des suites encadrées que $\lim_{n\to+\infty} u_n = 1$.

Exercice 1.
Démontrer que :

$$\left(1 + \frac{1}{\sqrt{n}}\right)^n \geq 1 + \sqrt{n},\ \forall n \geq 0.$$

En déduire $\lim_{n\to+\infty} \left(1 + \frac{1}{\sqrt{n}}\right)^n$.

Exercice 2.
Soit $(u_n)_{n\geq 0}$ une suite de nombres réels strictement positifs.
1) On suppose qu'il existe un rang $p \geq 1$ et un nombre réel $\alpha \in]0,1[$ tels que pour tout $n \geq p$ on ait $u_{n+1} \leq \alpha u_n$. Démontrer par récurrence que pour tout $n \geq p$, $0 \leq u_n \leq \alpha^{n-p} u_p$ et en déduire que $\lim_{n\to+\infty} u_n = 0$.
2) Démontrer que si $\lim_{n\to+\infty} u_{n+1}/u_n < 1$ alors $\lim_{n\to+\infty} u_n = 0$. En déduire que si $\lim_{n\to+\infty} u_{n+1}/u_n > 1$, alors $\lim_{n\to+\infty} u_n = +\infty$.
3) *Application :* Soit $c > 1$ un nombre réel et $p \geq$ un entier. Calculer les limites suivantes :

$$\alpha := \lim_{n\to+\infty} \frac{c^n}{n!} \text{ et } \beta := \lim_{n\to+\infty} \frac{c^n}{n^p}.$$

L1 - Module UE8 (Mathématiques II) : Feuille de TD no 1 (Semaines 1 et 2)

Nombres réels

Exercice 1 Soient $x, y \in \mathbf{R}$ tels que $x \leq y$ et $z \in \mathbf{R}$.
1) Démontrer que

$$||x| - |y|| \leq |x \pm y|.$$

2) Démontrer l'équivalence suivante :

$$x \leq z \leq y \Longleftrightarrow |x - z| + |z - y| = |x - y|.$$

Exercice 2
1) Soit $x \in \mathbf{R}$, démontrer qu'il existe un entier unique N tel que $x < N \leq x + 1$; Exprimer N en fonction de la partie entière de x, notée $[x]$.
2) Calculer $[x + n]$ lorsque $x \in \mathbf{R}$ et $n \in \mathbf{Z}$.

Exercice 3
1) Démontrer que pour tout $n \in \mathbf{N}^*$,

$$\sqrt{n+1} - \sqrt{n} < \frac{1}{2\sqrt{n}} < \sqrt{n} - \sqrt{n-1},$$

(On pourra utiliser les quantités conjuguées).
2) Calculer la partie entière du nombre réel

$$a := \frac{1}{2} \sum_{n=1}^{10000} \frac{1}{\sqrt{n}} = \frac{1}{2} \left(1 + \frac{1}{\sqrt{2}} + \cdots + \frac{1}{\sqrt{10000}} \right).$$

Exercice 4
1) Démontrer que l'ensemble $A := \{x \in \mathbf{R}^* \,|\, x + \dfrac{1}{x} < 2\}$ est un intervalle majoré et en déduire $\sup A$.
2) Démontrer que l'ensemble $B := \{x \in \mathbf{R}^* \,|\, x + \dfrac{1}{x} \leq 2\}$ est majoré mais n'est pas un intervalle. Calculer $\sup B$.

Exercice 5
1) Soit $x \in \mathbf{Q}_+$ tel que $x^2 > 2$. On pose $y := \frac{1}{2}(x + 2/x)$. Démontrer que $y \in \mathbf{Q}_+$, $x > y$ et $y^2 > 2$.
2) En déduire que l'ensemble $A := \{x \in \mathbf{Q}_+ ; x^2 > 2\}$ est une partie non vide et minorée de $\mathbf{Q}$ qui n'a pas de plus petit élément, ni de borne inférieure dans $\mathbf{Q}$ (montrer que si A admet une borne supérieure $S \in \mathbf{Q}$ alors $S^2 > 2$ en raisonnant par l'absurde et en utilisant la propriété d'Archimède). Quelle est sa borne inférieure dans $\mathbf{R}$?

Limites de suites de nombres réels

Exercice 6
1. Etudier la nature des suites définies par $y_n := (-1)^n/n$ et $z_n := (1/n)\sin(2\pi n/3)$ pour $n \in \mathbf{N}^*$. Généraliser ces exemples.
2. Démontrer en utilisant la définition que la suite définie par $x_n := (-1)^n$, pour $n \in \mathbf{N}$ ne converge pas. Quel phénomène général expique cette divergence ?

Exercice 7
1. Calculer

$$\lim_{n\to+\infty} \frac{n!}{n^n}.$$

1. Soit $b > 1$. Démontrer que

$$\lim_{n\to+\infty} \frac{b^n}{n!} = 0.$$

(Considérer l'unique entier $p \geq 1$ tel que $p \leq b < p+1$ et vérifier que pour $n \geq p+1$ on a $n! \geq (p+1)^{n-p}p!$.)
2. Soit $p \in \mathbf{N}^*$ fixé. Calculer

$$\lim_{n\to+\infty} \frac{b^n}{n^p}.$$

3. Soit $b \in \mathbf{R}$ tel que $b > 1$ et $p \in \mathbf{N}^*$. Dans l'échelle de croissance à l'infini comparer les suites $(b^n)_{n\geq 1}$, $(n^p)_{n\geq 1}$, $(n!)_{n\geq 1}$ et $(n^n)_{n\geq 1}$.

Exercice 8 Soit a un nombre réel tel que $0 < a < 1$.
1. Démontrer que pour tout entier $n \geq 1$, on a $1 - a^n \leq n(1-a)$ et en déduire que :

$$0 \leq 1 - \left(1 - \frac{1}{n^2}\right)^n \leq \frac{1}{n}, \quad \forall n \in \mathbf{N}^*.$$

2. Calculer la limite suivante

$$\lim_{n\to+\infty} \left(1 - \frac{1}{n^2}\right)^n.$$

Exercice 9.
Calculer les limites des suites défines pour n assez grand par les formules suivantes :

$$x_n := \frac{3n^3 - 5n^2 - 7}{2n^3 - 8n - 11},\ y_n := \frac{70n^2 + 10n^2 + 50n + 170}{2n^3 - 90n - 110}, \quad z_n := \frac{n^5 - 30n^2 - 50n - 750}{200n^3 + 18n^2 + 150}.$$

Généraliser au cas d'une suite définie pour n assez grand par $u_n := P(n)/Q(n)$, où P, Q sont des polynômes non nuls à coefficients réels.

1.4 Suites monotones

Dans les exemples de suites convergentes que nous avons rencontrés jusqu'à présent, il était facile de deviner à priori la limite de la suite considérée. Pour le justifier, il suffisait d'appliquer la définition en utilisant quelques règles élémentaires de calcul des limites.

L'utilisation de la définition pour démontrer qu'une suite converge suppose que l'on en connaisse la limite à l'avance, ce qui est rarement le cas dans la pratique. En fait, nous verrons que certaines suites monotones de nombres réels permettent de donner naissance à des nombres irrationnels dont elle permettent de donner une approximation avec une précision donnée (voir exemple 1).

Il est donc fort souhaitable de trouver des conditions suffisantes (appelés "critères de convergence") permettant de décider qu'une suite converge sans en connaitre a priori la limite.

Le critère le plus simple concerne les suites monotones. Pour énoncer ce critère, nous rappelons quelques définitions.

Définition 1.4.1 *Soit $(x_n)_{n\in\mathbf{N}}$ une suite de nombre réels.*
1) On dit que la suite $(x_n)_{n\in\mathbf{N}}$ est croissante *(resp.* strictement croissante*) si pour tout entier $n \in \mathbf{N}$, on a $x_n \leq x_{n+1}$ (resp. $x_n < x_{n+1}$).*
2) On dit que la suite $(x_n)_{n\in\mathbf{N}}$ est décroissante *(resp.* strictement décroissante*) si pour tout entier $n \in \mathbf{N}$, on a $x_n \geq x_{n+1}$ (resp. $x_n > x_{n+1}$).*
3) On dit que la suite $(x_n)_{n\in\mathbf{N}}$ est monotone *(resp.* strictement monotone*) si elle est soit croissante (resp. strictement croissante), soit décroissante (resp. strictement décroissante).*

Définition 1.4.2 *Soit $(x_n)_{n\in\mathbf{N}}$ une suite de nombre réels.*
1) On dit que la suite $(x_n)_{n\in\mathbf{N}}$ est majorée *s'il existe un nombre réel M tel que $\forall n \in \mathbf{N}$, $x_n \leq M$. Autrement dit l'ensemble $X := \{x_n; n \in \mathbf{N}\}$ des valeurs de la suite est une partie majorée de $\mathbf{R}$. On dit dans ce cas que la suite $(x_n)_{n\in\mathbf{N}}$ est majorée par M ou que M est un* majorant de la suite $(x_n)_{n\in\mathbf{N}}$*. On notera $\sup_{n\in\mathbf{N}} x_n$ la borne supérieure de l'ensemble X et on l'appelera la* borne supérieure *de la suite.*
2) On dit que la suite $(x_n)_{n\in\mathbf{N}}$ est minorée s'il existe un nombre réel m tel que $\forall n \in \mathbf{N}$, $x_n \geq m$. Autrement dit l'ensemble $X := \{x_n; n \in \mathbf{N}\}$ des valeurs de la suite est une partie minorée de $\mathbf{R}$. On dit dans ce cas que la suite $(x_n)_{n\in\mathbf{N}}$ est minorée par m ou que m est un minorant de la suite $(x_n)_{n\in\mathbf{N}}$. On notera $\inf_{n\in\mathbf{N}} x_n$ la borne inférieure de l'ensemble X et on l'appelera la borne inférieure de la suite.

On peut maintenant énoncer le résultat fondamental suivant qui est une conséquence simple de la propriété de la borne supérieure de $\mathbf{R}$.

Théorème 1.4.3 (Critère de convergence des suites monotones) *Toute suite monotone de nombres réels possède une limite finie ou infinie. D'une manière plus précise, une suite monotone $(x_n)_{n\in\mathbf{N}}$ de nombre réels possède les propriétés suivantes :*
1) si la suite $(x_n)_{n\in\mathbf{N}}$ est croissante (resp. décroissante) alors elle converge si et seulement si elle est majorée (resp. minorée) ; dans ce cas, sa limite coïncide avec sa borne supérieure (resp. sa borne inférieure) dans $\mathbf{R}$*,*
2) si la suite $(x_n)_{n\in\mathbf{N}}$ est croissante (resp. décroissante) alors elle a pour limite $+\infty$ (resp. $-\infty$) si et seulement si elle est non majorée (resp. non minorée).

Démonstration. On peut supposer que la suite $(x_n)_{n\in\mathbf{N}}$ est croissante (le cas d'une suite décroissante s'y ramène en considérant la suite opposée $(-x_n)_{n\in\mathbf{N}}$.)
1) Si la suite $(x_n)_{n\in\mathbf{N}}$ est majorée, l'ensemble $X := \{x_n; n \in \mathbf{N}\}$ possède une borne supérieure $S := \sup X = \sup_{n\in\mathbf{N}} x_n$. Montrons que $(x_n)_{n\in\mathbf{N}}$ converge vers S. En effet soit $\varepsilon > 0$. Par définition de de la borne supérieure, il existe $a \in \{x_n; n \in \mathbf{N}\}$ tel que $S - \varepsilon \leq a \leq S$. Par définition de l'ensemble $\{x_n; n \in \mathbf{N}\}$ il existe un entier $N \geq 0$ tel que $a = x_N$ et donc $S - \varepsilon \leq x_N \leq S$. Comme la suite est croissante et que S est un majorant de la suite, on a pour tout $n \geq N$, $S - \varepsilon \leq x_N \leq x_n \leq S$. Il en résulte clairement que pour tout $n \geq N$, $|x_n - S| \leq \varepsilon$ ce qui prouve que la suite $(x_n)_{n\geq 0}$ converge vers S.
Inversement supposons que la suite $(x_n)_{n\geq 0}$ converge vers ℓ. Alors pour tout $\varepsilon > 0$ il existe $N \in \mathbf{N}$ tel que $\forall n \in \mathbf{N}, \ell - \varepsilon \leq x_n \leq \ell + \varepsilon$. Comme la suite est croissante, on a $x_n \leq x_N \leq \ell + \varepsilon$ pour $0 \leq n \leq N$. Il en résulte que $\forall n \in \mathbf{N}, x_n \leq \ell + \varepsilon$. Comme $\varepsilon > 0$ est arbitraire, on en déduit que $\forall n \in \mathbf{N}, x_n \leq \ell$, ce qui prouve que la suite $(x_n)_{n\geq 0}$ est bornée par ℓ et d'après ce qui précède, on a $\sup_{n\in\mathbf{N}} x_n = \ell$.
2) Si la suite $(x_n)_{n\in\mathbf{N}}$ n'est pas majorée, pour tout $A > 0$ il existe un rang $N \geq 1$ tel que $x_N > A$. Comme la suite est croissante, on en déduit que pour tout $n \geq N$, on a $x_n \geq x_N \geq A$, ce qui prouve que $\lim_{n\to+\infty} x_n = +\infty$. La réciproque de cette propriété est évidente. □

Donnons des exemples qui illustrent ce théorème.

Exemples.

1. (Un cas de convergence). Soit $(x_n)_{n\geq 1}$ la suite définie par :

$$x_n := 1 + \frac{1}{1!} + \cdots + \frac{1}{n!}$$

pour $n \geq 1$.
1) Il est clair que la suite $(x_n)_{n\geq 1}$ est strictement croissante puisque $x_{n+1} - x_n = \frac{1}{(n+1)!} > 0$, pour tout $n \geq 1$.
2) Montrons qu'elle est majorée. En effet on vérifie facilement par récurrence

l'inégalité suivante :

$$\forall n \geq 1, \quad n! \geq 2^{n-1}.$$

Il en résulte que pour tout $n \geq 1$, on a $x_n \leq 1 + \frac{1}{1} + \cdots \frac{1}{2^{n-1}} < 1 + 2 = 3$.
Il en résulte que la suite $(x_n)_{n\geq 1}$ converge et que sa limite notée e vérifie les inégalités $2,5 < e \leq 3$.

2. (Un cas de divergence). Soit $(u_n)_n$ la suite définie pour $n \geq 1$ par la formule suivante :

$$u_n := \sum_{k=1}^{n} \frac{1}{k} = 1 + \frac{1}{2} + \cdots + \frac{1}{n}.$$

Nous allons montrer que la suite (u_n) tend vers $+\infty$.
1) La suite $(u_n)_n$ est (strictement) croissante puisque $u_{n+1} - u_n = 1/(n+1) > 0$ pour tout $n \geq 1$.
2) Montrons qu'elle n'est pas majorée. En effet, observons d'abord que si $n \geq 1$ et $p \geq 1$, alors

$$u_{n+p} - u_n = \frac{1}{n+1} + \cdots + \frac{1}{n+p} \geq \frac{p}{n+p},$$

puisque cette expression est la somme de p termes dont le plus petit est $1/(n+p)$. Par suite $u_{2n} - u_n \geq 1/2$ pour tout $n \geq 1$ et en particulier on a :

$$\forall k \geq 1, \quad u_{2^k} - u_{2^{k-1}} \geq \frac{1}{2}.$$

En fixant un entier $p \geq 2$ et en additionnant membre à membre les p inégalités obtenues pour $k = 1, 2, \cdots, p$ on obtient :

$$\forall p \geq 2, \quad (u_2 - u_1) + \cdots + (u_{2^p} - u_{2^{p-1}}) \geq \frac{p}{2}.$$

Les termes se simplifient deux à deux par "téléscopage" et l'on obtient $u_{2^p} - u_1 \geq p/2$ pour tout $p \geq 2$ et donc $u_{2^p} \geq 1 + p/2$ pour tout $p \geq 2$, ce qui prouve que la suite (u_n) n'est pas majorée. Par conséquent d'après le théorème précédent, elle tend vers $+\infty$ i.e.

$$\lim_{n\to+\infty} \left(1 + \frac{1}{2} + \cdots + \frac{1}{n}\right) = +\infty.$$

Complément (*facultatif)* Nous allons démontrer que :

$$\lim_{n\to+\infty} \left(1 + \frac{1}{n}\right)^n = e.$$

On considère la suite définie pour $n \geq 1$ par la formule suivante :

$$y_n := \left(1 + \frac{1}{n}\right)^n.$$

Montrons que la suite $(y_n)_{n\in\mathbf{N}}$ est croissante et majorée. En effet, d'après la formule du binôme, pour $n \geq 2$, on a :

$$\left(1+\frac{1}{n}\right)^n = 1+\sum_{k=1}^{n}\frac{n(n-1)\cdots(n-k+1)}{k!n^k} \tag{1.6}$$
$$= 1+\sum_{k=1}^{n}\frac{1}{k!}\left(1-\frac{1}{n}\right)\cdots\left(1-\frac{k-1}{n}\right).$$

Posons pour $n \geq 2$ et $1 \leq k \leq n$:

$$a_n(k) := \frac{1}{k!}\left(1-\frac{1}{n}\right)\cdots\left(1-\frac{k-1}{n}\right).$$

Comme pour tout j tel que $0 \leq j \leq k-1$ on a $0 \leq 1-j/n) < 1-j/(n+1)$, il en résulte que $0 \leq a_n(k) < a_{n+1}(k)$. Cela implique que :

$$\sum_{k=1}^{n} a_n(k) < \sum_{k=1}^{n} a_{n+1}(k)$$
$$< \sum_{k=1}^{n+1} a_{n+1}(k).$$

Par conséquent, la suite $(y_n)_{n\geq 1}$ est strictement croissante. Comme pour $2 \leq k \leq n$ on a $a_n(k) < 1/k!$, il résulte de la formule (2.1) que :

$$\forall n \geq 2, \quad y_n < 1+\sum_{k=1}^{n}\frac{1}{k!}.$$

D'après l'exemple 1, la suite définie par $x_n := 1+\sum_{k=1}^{n}\frac{1}{k!}$ pour $n \geq 1$ est croissante et majorée. Il en résulte que la suite $(y_n)_{n\geq 1}$ est une suite croissante et majorée donc convergente. Pour calculer sa limite, nous allons utiliser la formule (2.1). Comme y_n est une somme de $n+1$ termes positifs, il résulte de la formule (2.1) que si p et n sont des entiers tels que $1 \leq p < n$, en gardant seulement les p premiers termes de cette somme, on obtient :

$$1+\sum_{k=1}^{p}\frac{1}{k!}\left(1-\frac{1}{n}\right)\ldots\left(1-\frac{k-1}{n}\right) < y_n < x_n. \tag{2.2}$$

Fixons l'entier $p \geq 1$. Le premier membre de l'inégalité (2.2) est une suite indéxée par $n \geq p$ qui s'écrit comme somme finie de $p+1$ suites indéxées par $n \geq p$ ayant chacune une limite finie lorsque $n \to +\infty$. Il résulte de la formule d'addition des limites que cette suite a pour limite la somme des limites qui est égale précisément à x_p. Alors en

passant à la limite lorsque $n \to +\infty$ dans les inégalités (2.2), on en déduit grâce au principe de conservation des inégalités que pour tout $p \geq 2$:

$$\forall p \in \mathbf{N}^*, \quad x_p = 1 + \sum_{k=1}^{p} \frac{1}{p!} \leq \lim_{n \to +\infty} y_n \leq \lim_{n \to +\infty} x_n = e.$$

En passant à la limite dans l'inégalité précédente lorsque $p \to +\infty$, on en déduit grâce au principe de conservation des inégalités que $\lim_{n \to +\infty} y_n = \lim_{n \to +\infty} x_n = e$.

Exercice 1.
Soit $(u_n)_{n \geq 0}$ la suite de nombres réels définie par $u_0 = 1$ et $u_{n+1} = \sqrt{u_n^2 + 2^{-n}}$ pour tout $n \in \mathbf{N}$.
1) Démontrer que pour tout $n \geq 1$,

$$1 \leq u_n < u_{n+1} < u_n + \frac{1}{2^{n+1}}.$$

En déduire que pour entier tout $n \geq 1$, $u_n < 2$.
2) En déduire que la suite $(u_n)_{n \geq 0}$ converge et encadrer sa limite.

Exercice 2.
On considère la suite définie par son premier terme x_0 et par la relation de récurrence :

$$x_{n+1} = \frac{x_n}{1 + n x_n^2}, n \geq 0.$$

1) Montrez que la suite est de signe constant .
2) On suppose que $x_0 > 0$.
Montrez que la suite $(x_n)_{n \geq 0}$ est monotone et qu'elle converge vers une limite que l'on calculera.

Exercice 3.
Soit $(u_n)_{n \in \mathbf{N}}$ une suite de nombres réels telle que :

$$u_{n+1} = \frac{u_n^2 + n^2}{n^2 + 1},$$

pour tout $n \in \mathbf{N}$.
1) Démontrer que si la suite $(u_n)_{n \in \mathbf{N}}$ converge , sa limite est nécéssairement égale à 1.
2) Démontrer que si $u_0 = 1$, la suite $(u_n)_{n \in \mathbf{N}}$ est constante.
3) Démontrer que pour tout $n \in \mathbf{N}$,

$$u_{n+1} - u_n = \frac{(u_n - 1)(u_n^2 - n^2)}{n^2 + 1},$$

4) Supposons que $0 \leq u_0 < 1$. Démontrer que pour tout $n \in \mathbf{N}$, $u_n < 1$ et en déduire que la suite $(u_n)_{n\in\mathbf{N}}$ converge.
5) Supposons qu'il existe un entier $p \geq 1$ tel que $1 < u_p \leq p^2$. Démontrer que pour tout $n \geq p$ on a $1 < u_{n+1} \leq u_n$ et en déduire que la suite $(u_n)_{n\in\mathbf{N}}$ converge.
6) Supposns que $1 < u_0 < \sqrt[4]{7}$. Démontrer que $1 < u_2 \leq 4$ et en déduire que la suite $(u_n)_{n\in\mathbf{N}}$ converge.
7) On suppose que $u_0 \geq 4$. Démontrer par récurrence que pour tout $n \in \mathbf{N}^*$, $u_n \geq 16n^3$. En déduire la limite de la suite $(u_n)_{n\in\mathbf{N}}$.

1.5 Suites adjacentes

Le théorème suivant est très intuitif et repose sur le critère de convergence des suites monotones.

Théorème 1.5.1 (Théorème des suites adjacentes) *Soient $(a_n)_{n\in\mathbf{N}}$ et (b_n) deux suites de nombres réels telles que*

$$\forall n \in \mathbf{N},\ a_n \leq a_{n+1} \leq b_{n+1} \leq b_n. \tag{1.7}$$

Alors les deux suites $(a_n)_{n\in\mathbf{N}}$ et $(b_n)_{n\in\mathbf{N}}$ convergent vers des nombres réels α et β respectivement qui vérifient les inégalités suivantes :

$$\forall n \in \mathbf{N}, a_n \leq \alpha \leq \beta \leq b_n.$$

Si de plus $lim_{n\to+\infty}(b_n - a_n) = 0$, alors $\alpha = \beta$.

Démonstration. C'est une conséquence immédiate du critère des suites monotones et du principe de conservation des inégalités larges. □

Si les deux suites $(a_n)_{n\in\mathbf{N}}$ et $(b_n)_{n\in\mathbf{N}}$ vérifient les inégalités (1.7) et si $lim_{n\to+\infty}(b_n - a_n) = 0$, on dira que ce sont des *suites adjacentes*. Le théorème affirme en particulier que deux suites adjacentes convergent vers une même limite, donnant ainsi naissance à un nombre réel ℓ dont $(a_n)_{n\geq 0}$ est une suite d'approximants par défaut et (b_n) est une suite d'approximants par excès.

Remarque.
Les hypothèses faites dans ce théorème traduisent le fait géométrique que les segments de la droite réelle à savoir $I_n := [a_n, b_n]$ pour $n \in \mathbf{N}$, forment une suite de *segments emboités* les uns dans les autres i.e. $I_{n+1} \subset I_n$ pour tout $n \in N$ (faire un dessin). La conclusion affirme que ces segments ont une intersection qui est encore un segment et que celui-ci est réduit à un point dans le cas où les longueurs des segments

(I_n) deviennent infiniment petites lorque n devient grand. En raison de cette propriété géométrique, on appelle également ce théorème le *théorème des segments emboités.*

Nous avons déja vu que le procédé de dichotomie appliqué à l'approximation de $\sqrt{2}$ donnait naissance à de telles suites. Donnons maintenant un autre exemple intéressant illustrant cette situation.

Exemple *(Le nombre réel e est irrationnel).*
Posons pour $n \geq 1$:

$$a_n := 1 + \frac{1}{1!} + \frac{1}{2!} \ldots + \frac{1}{n!}, \quad b_n := a_n + \frac{1}{n \cdot n!}.$$

Nous allons démontrer que ces deux suites sont adjacentes et convergent vers un nombre réel *irrationnel* noté e en l'honneur du fameux mathématicien L. Euler : c'est la base du logarithme neperien.
1) La suite (a_n) est strictement croissante. En effet $a_{n+1} - a_n = 1/(n+1)! > 0$ pour tout $n \geq 1$.
2) La suite $(b_n)_{n\geq 1}$ est strictement décroissante. En effet pour $n \geq 1$, on a

$$\begin{aligned} b_{n+1} - b_n &= a_{n+1} - a_n + \frac{1}{(n+1)(n+1)!} - \frac{1}{nn!} \\ &= \frac{1}{n!}\left(\frac{1}{n+1} + \frac{1}{(n+1)^2} - \frac{1}{n}\right) \\ &= -\frac{1}{n(n+1)(n+1)!} < 0 \end{aligned}$$

3) Il est clair que $\lim_{n\to+\infty}(b_n - a_n) = 0$. D'après le théorème des suites adjacentes, on en déduit qu'il existe un nombre réel, noté e tel que :

$$e := \lim_{n\to+\infty} a_n = \lim_{n\to+\infty} b_n.$$

Ce nombre réel, appelé le nombre d'Euler, satisafait à l'encadrement suivant : pour tout $n \in \mathbf{N}$,

$$1 + \frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{1}{n!} < e < 1 + \frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{1}{n!} + \frac{1}{nn!}. \tag{1.8}$$

Montrons que le nombre réel e est irrationnel i.e. $e\mathbf{R} \setminus \mathbf{Q}$. On raisonne par l'absurde en supposant le contraire à savoir que e est rationnel. Dans ce cas, il existe deux entiers naturels $p \geq 1$ et $q \geq 1$ premiers entre eux tels que pour tout entier $n \in \mathbf{N}$,

$$a_n < \frac{p}{q} < a_n + \frac{1}{nn!}.$$

En prenant $n = q$ et en observant que $N := qq!a_q$ est un entier naturel, on en déduit que l'entier naturel p vérifie les inégalités $N < p < N + 1$, ce qui est absurde.

Les inégalités (1.8) permettent de donner une valeur approchée de e avec une majoration précise de l'erreur d'approximation. En effet on a :

$$0 < e - \left(1 + \frac{1}{1!} + \ldots + \frac{1}{n!}\right) < \frac{1}{n\ n!}, \forall n \geq 1.$$

Ainsi pour obtenir une valeur approchée de e à 10^{-8} près par exemple, il suffit de choisir un entier n (le plus petit possible) tel que $n\ n! > 10^8$. Il est facile de vérifier que $n = 10$ suffit et qu'alors en calculant $a_{10} = 1 + \frac{1}{1!} + \ldots + \frac{1}{10!}$, on en déduit que $e \simeq 2,71828182\cdots$ à 10^{-8} près par défaut, ce qui signifie que $2,71828182 < e < 2,71828183$, autrement dit $e = 2,71828182\ldots$, les sept premières décimales obtenues étant exactes.

Note historique : L'irrationnalité du nombre réel e a été démontrée au 18^{eme} siècle par Leonhard Euler (1707-1783) et Johann Heinrich Lambert ($1728-1777$). Cela signifie que e n'est pas solution d'une équation linéaire (i.e. équation algébrique de degré 1) $ax + b = 0$ à coefficientes entiers $a, b \in \mathbf{Z}, a \neq 0$. Plus tard vers 1844, Joseph Liouville démontre que e n'est pas solution d'une équation quadratique (i.e. équation algébrique de degré 2) $ax^2 + bx + c = 0$ à coefficients entiers $a, b, c \in \mathbf{Z}, a \neq 0$ et conjecture que e est un nombre *transendant* dans le sens où il n'est solution d'aucune équation algébrique $a_n x^n + \ldots a_1 x + a_0 = 0$ à coefficients entiers $a_n, a_{n-1}, \ldots, a_0 \in \mathbf{Z}, a_n \neq 0$. Cette conjecture a été démontrée vers 1873 par Charles Hermite ($1822 - 1901$).

Exercice 1.
Soient $a, b > 0$ deux nombres réels positifs. On définit par récurrence deux suites $(u_n)_{n\geq 0}$ et $v_n)_{n\geq 0}$ en posant $u_0 = a, v_0 = b$ et pour tout $n \geq 0$:

$$u_{n+1} := \sqrt{u_n \cdot v_n}, \quad v_{n+1} := \frac{u_n + v_n}{2}.$$

(Le nombre réel u_{n+1} est appelé la moyenne géométriqe des nombres réels u_n et v_n et le nombre reél v_{n+1} est leur *moyenne arithmétique*).
1) Calculer u_1 et v_1 et les comparer.
2)Démontrer que pour tout $n \geq 1$:

$$u_n \leq u_{n+1} \leq v_{n+1} \leq v_n.$$

3) Démontrer que (u_n) et $v_n)$ convergent, puis que leurs limites sont égales.
4) En déduire que $(u_n)_{n\geq 1}$ et $(v_n)_{n\geq 0}$ sont des suites adjacentes et que leur limite commune ℓ vérifie :

$$\sqrt{a \cdot b} \ \leq \ \ell \ \leq \ \frac{a+b}{2}.$$

Le nombre réel ℓ est appelée la *moyenne arithmético-géométrique* des deux nombres réels a et b).

Exercice 2.
Soient $a, b > 0$ deux nombres réels positifs. On définit par récurrence deux suites $(x_n)_{n\geq 0}$ et $y_n)_{n\geq 0}$ en posant $x_0 = a, y_0 = b$ et pour tout $n \geq 0$:

$$\frac{1}{x_{n+1}} := \frac{1}{2}\left(\frac{1}{x_n} + \frac{1}{y_n}\right), \quad y_{n+1} := \frac{x_n + y_n}{2}.$$

(Le nombre réel x_{n+1} est appelé la *moyenne harmonique* des deux nombres réels x_n et y_n). On suppose que $a < b$.
1) Démonter que pour tout $n \in \mathbf{N}$,

$$y_{n+1} - x_{n+1} = \frac{(x_n - y_n)^2}{2(x_n + y_n)}.$$

2) Démonter que pour tout $n \in \mathbf{N}$,

$$0 < y_{n+1} - x_{n+1} \leq \frac{1}{2}(x_n - y_n).$$

3) Démontrer que la suite $(x_n)_{n\in\mathbf{N}}$ est croissante et que la suite $(y_n)_{n\in\mathbf{N}}$ est décroissante.
4) Démontrer que les deux suites $(x_n)_{n\in\mathbf{N}}$ et $(y_n)_{n\in\mathbf{N}}$ sont convergentes et ont la même limite.
5) Démontrer que la suite $(x_n \cdot y_n)_{n\in\mathbf{N}}$ est constante. En déduire la limite des suites $(x_n)_{n\in\mathbf{N}}$ et $(y_n)_{n\in\mathbf{N}}$.

Exercice 3.
(**R est non dénombrable**). Soit $I \subset \mathbf{R}$ un intervalle non vide et non réduit à un point, $(x_n)_{n\geq 0}$ une suite de nombres réels de l'intervalle I.
1) En s'inspirant du procédé de dichotomie, démontrer par récurrence sur $n \geq 0$ qu'il existe une suite décroissante de segments $[a_n, b_n] \subset I$ telle que pour tout $n \geq 0$ on ait $x_0, \cdots, x_{n+1} \notin [a_n, b_n]$ et $b_n - a_n \leq (b_0 - a_0)/3^n$.
En déduire qu'il existe un nombre réel $c \in I$ tel que $x_n \neq c$ pour tout $n \geq 0$.
2) En raisonnant par l'absurde, démontrer qu'il n'existe pas d'application surjective de $\mathbf{N}$ sur I et en déduire que I n'est pas dénombrable. En particulier $\mathbf{R}$ n'est pas dénombrable.

1.6 Développement décimal d'un nombre réel

La représentation décimale d'un nombre réel joue un rôle fondamental en Analyse. Elle permet de donner une valeur approchée décimale d'un nombre réel avec autant de précision que l'on veut. Par exemple $\sqrt{2} = 1,414213562\cdots$, $e = 2,718281828\cdots$ et

$\pi = 3,141592654\cdots$.

Rappelons que c'est dans le système décimal que nous représentons habituellement les entiers naturels à l'aide des nombres entiers $0, 1, \cdots 9$. Tout entier naturel non nul $a \in \mathbf{Z}*$ s'écrit $a = \pm \sum_{j=0}^{k} n_j 10^j$, où $n_0, \cdots n_k$ sont des entiers compris entre 0 et 9, appelés respectivement, chiffre des unités, des dizaines, $\cdots$. On écrit aussi $n = \pm n_0 n_1 \cdot n_k$: c'est l'écriture décimale de n.

Rappelons également qu'un nombre décimal d est un nombre rationnel qui peut sécrire sous la forme $d = a10^{-N}$, où $a \in \mathbf{Z}$ et $N \in \mathbf{N}$. Comme l'entier a sécrit $a = \sum_{j=0}^{k} n_j 10^j$, où $n_0, \cdots n_k$ sont des entiers compris entre 0 et 9, il en résulte que :

$$d = p_0 + \sum_{j=1}^{m} p_j 10^{-j},$$

où $p_0 := [d] \in \mathbf{Z}$ est la partie entière de d et $p_1, \cdots p_m$ sont des entiers naturels compris entre 0 et 9.

On écrit alors un tel nombre sous forme décimale $x = p_0, p_1 p_2 \cdots p_m$: c'est le développement décimal (limité) de d. C'est ainsi que le nombre décimal $23/4$ sécrit :

$$\frac{23}{4} = \frac{575}{100} = 5,75.$$

Nous allons démontrer que tout nombre réel admet un développement décimal illimité en général.

En effet soit $x \in \mathbf{R}$ qui n'est pas un entier. Notons $p_0 := [x] \in \mathbf{Z}$ sa partie entière et $\{x\} := x - [x] \in]0, 1[$ sa partie fractionnaire. On a alors $x := p_0 + \{x\}$. Il suffit donc de considérer le cas où $0 < x < 1$.

On supposera donc dans toute la suite que $x \in]0, 1[$. Posons $p_1 := [10x]$. Alors $0 \leq p_1 < 10$ et par définition de la partie entière de x, on a $p_1 \leq 10x < p_1 + 1$ et donc :

$$\frac{p_1}{10} \leq x < \frac{p_1}{10} + \frac{1}{10}.$$

Le nombre décimal $x_1 := \frac{p_1}{10}$ vérifie

$$x_1 \leq x < x_1 + \frac{1}{10}.$$

Posons $\varepsilon_1 := x - x_1$ et observons que si $\varepsilon_1 = 0$, on a $x = x_1$ et x est donc un nombre décimal. En général, l'inégalité précédente se traduit en disant que x_1 est un approximant décimal par défaut de x à 10^{-1} près et que p_1 est la première décimale exacte du

développement décimal de x.

Comme $0 \leq \varepsilon_1 < 1/10$, le nombre entier $p_2 := [10^2\varepsilon_1]$ est compris entre 0 et 9 et le nombre décimal $x_2 := \frac{p_1}{10} + \frac{p_2}{10^2}$ fournit un approximant décimal par défaut de x à 10^{-2} près puisque l'on a

$$x_2 \leq x < x_2 + \frac{1}{10^2}.$$

En continuant ainsi, on construit par récurrence une suite $(p_n)_{n\in\mathbf{N}^*}$ d'entiers compris entre 0 et 9 telle que le nombre décimal :

$$x_n := \sum_{k=1}^{n} \frac{p_k}{10^k}$$

vérifie

$$x_n \leq x < x_n + 10^{-n},$$

où $\varepsilon_k := x - x_k$ et $p_k := [10^k\varepsilon_{k-1}]$ pour $2 \leq k \leq n$. Cette propriété se traduit en disant que $x_n = 0, p_1 \cdots p_n$ est un approximant décimal par défaut de x à $10^{-n}-$près et que $p_1, \cdots, p_n$ sont les n premières décimales exactes du développement décimal de x.

Il faut observer que si x est un nombre décimal, il existe un entier $m \geq 1$ tel que $p_n = 0$ pour $n \geq m$ et donc $x = x_m = \sum_{k=1}^{n} \frac{p_k}{10^k}$.

Si x n'est pas un nombre décimal, on obtient une suite croissante de nombres décimaux $(x_n)_{n\geq 1}$ qui converge vers x, puisque $0 \leq x - x_n < 10^{-n}$ pour tout $n \in \mathbf{N}^*$. On écrira symboliquement ce résultat sous la forme :

$$x = \lim_{n\to\infty} x_n = \sum_{k=0}^{+\infty} \frac{p_k}{10^k}.$$

C'est le développement décimal (illimité si x n'est pas un nombre décimal) du nombre réel x.

Remarquons que par définition de x_n, on a $x_n \leq x < x_n + 10^{-n}$ et donc $10^n x_n \leq 10^n x < 10^n x_n + 1$. Comme $10^n x_n$ est un entier, il en résulte que $[10^n x] = 10^n x_n$ et on a la formule plus simple suivante :

$$x_n = \frac{[10^n x]}{10^n}, \quad n \in \mathbf{N}^*.$$

Par ailleurs, posons :

$$y_n := x_n + 10^{-n}, \quad n \in \mathbf{N}^*.$$

On obtient ainsi une suite décroissante de nombres décimaux qui converge vers x (à vérifier en exercice) et telle que :

$$x_n < x < y_n, \text{ pourtout } \ n \in \mathbf{N}.$$

Les deux suites de nombres décimaux (x_n) et (y_n) sont des suites adjacentes qui convergent vers x par défaut et par excès respectivement.

On démontre qu'un nombre réel x est rationnel si et seulement si il admet un développement décimal périodique à partir d'un certain rang i.e. il existe m ($m \geq 1$) entiers $p_1, \cdots p_m$ compris entre 0 et 9 tels que $10^n x = p_0, p_1 \cdots p_m \cdot p_1 \cdots p_m \cdots$.

L1 - Module UE8 (Mathématiques II) : Feuille de TD no 2 (Semaines 3 et 4)

Exercice 1.
1. Calculer les limites des suites suivantes :

$$x_n := \frac{2n^2 + (-1)^n n}{3n^2 + 7\sqrt{5n}}, \quad y_n := n \sin\left(\frac{\pi}{2n}\right), \quad u_n := n \ln\left(1 + \frac{1}{\sqrt{n}}\right),$$

définies pour $n \in \mathbf{N}^*$.
On admettra les équivalents usuels $\sin x \sim x$ et $\ln(1+x) \sim x$ au voisinage de 0.
2. On pose pour $n \in \mathbf{N}^*$, $v_n := 1 + \frac{1}{2n} - \sqrt{1 + \frac{1}{n}}$. Trouver une suite $(a_n)_{n \in \mathbf{N}*}$ de nombres réels positifs telle que $\lim_{n \to +\infty} a_n = 1$ et vérifiant la relation suivante :

$$\forall n \in \mathbf{N}^*, \ v_n = \frac{a_n}{8n^2}.$$

3. Calculer $\lim_{n \to +\infty} n^2 v_n$.

Exercice 2.
On définit la suite $(x_n)_{n \geq 1}$ par la formule suivante :

$$x_n := 2\cos(1/n^2) + 3 \sum_{p=1}^{n} \frac{1}{\sqrt{p+1}}, \ n \in \mathbf{N}^*.$$

1) Calculer x_1, x_2, x_3.
2) Démontrer que pour si n et p sont des entiers tels que $1 \leq p \leq n$, on a

$$\frac{1}{\sqrt{n+1}} \leq \frac{1}{\sqrt{p+1}} \leq \frac{1}{\sqrt{2}}.$$

3 Démontrer que pour tout $n \geq 1$, $x_n \geq 3\sqrt{n+1} - 5$ et calculer la limite de la suite $(x_n)_{n \geq 1}$. Trouver un entier N tel que $x_N \geq 235$.

Exercice 3.
Soit $(u_n)_{n \geq 0}$ la suite de nombres réels définie par $u_0 = 1$ et $u_{n+1} = \sqrt{u_n^2 + 2^{-n}}$ pour tout $n \in \mathbf{N}$.
1) Démontrer que pour tout $n \geq 1$,

$$1 \leq u_n < u_{n+1} < u_n + \frac{1}{2^{n+1}}.$$

En déduire que pour entier tout $n \geq 1$, $u_n < 2$.
2) En déduire que la suite $(u_n)_{n \geq 0}$ converge et encadrer sa limite.

Exercice 4.
Soit $(u_n)_{n\in\mathbf{N}}$ une suite de nombres réels telle que :

$$\forall n \in \mathbf{N},\ u_{n+1} = \frac{u_n^2 + n^2}{n^2+1}.$$

1) Démontrer que si la suite $(u_n)_{n\in\mathbf{N}}$ converge , sa limite est nécéssairement égale à 1.
2) Démontrer que si $u_0 = 1$, la suite $(u_n)_{n\in\mathbf{N}}$ est constante.
3) Démontrer que pour tout $n \in \mathbf{N}$,

$$u_{n+1} - u_n = \frac{(u_n - 1)(u_n^2 - n^2)}{n^2+1},$$

4) Supposons que $0 \leq u_0 < 1$. Démontrer que pour tout $n \in \mathbf{N}$, $u_n < 1$ et en déduire que la suite $(u_n)_{n\in\mathbf{N}}$ converge.
5) Supposons qu'il existe un entier $p \geq 1$ tel que $1 < u_p \leq p^2$. Démontrer que pour tout $n \geq p$ on a $1 < u_{n+1} \leq u_n$ et en déduire que la suite $(u_n)_{n\in\mathbf{N}}$ converge.
6)(*Facultatif*) Supposons que $1 < u_0 < \sqrt[4]{7}$. Démontrer que $1 < u_2 \leq 4$ et en déduire que la suite $(u_n)_{n\in\mathbf{N}}$ converge.
7)(*Facultatif*) On suppose que $u_0 \geq 4$. Démontrer par récurrence que pour tout $n \in \mathbf{N}^*$, $u_n \geq 16n^3$. En déduire la limite de la suite $(u_n)_{n\in\mathbf{N}}$.

Exercice 5.
Soient $a, b > 0$ deux nombres réels positifs. On définit par récurrence deux suites $(u_n)_{n\geq 0}$ et $v_n)_{n\geq 0}$ en posant $u_0 = a, v_0 = b$ et pour tout $n \geq 0$:

$$u_{n+1} := \sqrt{u_n \cdot v_n},\quad v_{n+1} := \frac{u_n + v_n}{2}.$$

(Le nombre réel u_{n+1} est appelé la moyenne géométriqe des nombres réels u_n et v_n et le nombre reél v_{n+1} est leur *moyenne arthmétique*).
1) Calculer u_1 et v_1 et les comparer.
2)Démontrer que pour tout $n \geq 1$:

$$u_n \leq u_{n+1} \leq v_{n+1} \leq v_n.$$

3) Démontrer que (u_n) et $v_n)$ convergent, puis que leurs limites sont égales.
4) En déduire que $(u_n)_{n\geq 1}$ et $(v_n)_{n\geq 0}$ sont des suites adjacentes et que leur limite commune ℓ vérifie :

$$\sqrt{a \cdot b} \ \leq\ \ell\ \leq\ \frac{a+b}{2}.$$

Le nombre réel ℓ est appelée la *moyenne arithmético-géométrique* des deux nombres réels a et b).

1.7 Suites récurrentes

Il est assez rare dans les applications qu'une suite soit donnée par une "formule explicite" permettant d'en calculer la limite. Nous allons étudier ici les suites données par un "procédé itératif" dans lequel on connait le premier terme x_0 de la suite et une relation de récurrence :

$$(R) \qquad x_{n+1} = f(x_n),\ n \in \mathbf{N}$$

permettant de calculer le terme x_{n+1} à partir du terme précédent x_n à l'aide d'une même fonction f définie sur un intervalle $I \subset \mathbf{R}$. Une telle relation, dite relation de récurrence d'ordre 1, permet de calculer tous les termes de la suite $(x_n)_{n\geq 0}$ de proche en proche par récurrence à partir du premier terme x_0. En effet, connaissant le premier terme $x_0 \in I$, on peut calculer le terme suivant x_1 à partir de $x_0 \in I$ en appliquant la formule (R) pour $n = 0$, d'où $x_1 = f(x_0)$. Connaissant le terme x_1, on peut alors calculer le terme suivant x_2 grâce à la relation de récurrence (R) appliquée avec $n = 1$ à condition que $x_1 \in I$, d'où $x_2 = f(x_1$, et ainsi de suite... connaissant le terme x_n on peut calculer le terme x_{n+1} par la formule $x_{n+1} = f(x_n)$ à condition que $x_n \in I$.

Par conséquent si $x_0 \in I$ et si la fonction f vérifie la condition $x \in I \Longrightarrow y = f(x) \in I$, on peut définir par récurrence une suite $(x_n)_{n\in\mathbf{N}}$ unique vérifiant la relation de récurrence (R). On dira que la suite $(x_n)_{n\in\mathbf{N}}$ est une suite définie par itération successive de x_0 par f.

Il est possible en théorie de déduire de (R) une formule donnant le terme x_n en fonction de n et de x_0. En effet on définit les fonctions itérées de f en posant $f^1 := f$, $f^2 := f \circ f, \ldots, f^{n+1} = f^n \circ f = f \circ f^n$ pour $n \in \mathbf{N}^*$. On a alors $x_n = f^n(x_0)$ pour $n \geq 1$. Cette formule est en général difficilement exploitable car calculer les itérées f^n de f peut se révéler très compliqué lorsque n devient grand, même si la fonction de départ est assez simple (voir les exemples ci-dessous).

La théorie générale ayant pour objet l'étude du comportement de telles suites en fonction de la valeur initiale x_0 s'appelle les "systèmes dynamiques" et fait l'objet de recherches actuelles très actives. Ici nous allons nous contenter d'étudier quelques exemples simples de suites récurrentes.

Auparavant pour motiver l'introduction de cette méthode, rappelons une anecdote historique connue sous le nom de "paradoxe de Zénon", concernant Achille et la tortue. Le philosophe grec Zénon d'Élée , né quelques 500 ans avant J.C. environ, niait la réalité du mouvement en avançant le raisonnement suivant :
Si Achille, le plus véloce des coureurs grecs, s'aventurait à courir après une tortue, il ne la rattraperait jamais. En effet, supposons qu'au départ 1000 *pas séparent Achille de la tortue et qu'en une seconde Achille parcourt* 10 *pas tandis que la tortue n'en parcourt*

qu'un. Dans 100 *s, Achille aura parcouru les* 1000 *pas qui le séparent de la tortue et pendant ce temps là, la tortue aura parcouru* 100 *pas. Lorsqu'il aura parcouru ces* 100 *pas en* 10 *s, la tortue, elle, en aura fait* 10*. Pour couvrir ces 10 pas, il lui faudra* 1 *s, la tortue, elle, aura fait* 1 *pas et ainsi de suite... la tortue aura donc toujours de l'avance sur Achille.*
Il en concluait alors que le mouvement n'existe pas.

Il est clair par ailleurs que le temps T que mettra Achille pour rattraper la tortue est solution de l'équation

$$10x - x \;=\; 1000, \tag{1.9}$$

d'où $T = 1000/9 = 111,111\ldots$ i.e. 111 secondes et $1/9$ de seconde.

Le paradoxe de Zénon s'explique par le fait que son raisonnement peut être considéré comme une méthode de résolution approchée de l'équation (1.9).

En effet écrivons l'équation (1.9) sous la forme équivalente suivante :

$$x \;=\; 100 + \frac{x}{10}. \tag{1.10}$$

Si on néglige le terme $\frac{x}{10}$ (qui est petit devant x), on obtient une première valeur approchée $x_1 = 100$ de la solution x de l'équation (1.10).

En portant cette valeur x_1 dans le second membre de l'équation (1.10), on obtient une meilleure approximation de x, soit $x_2 = 100 + 10 = 110$. En portant de nouveau cette valeur x_2 dans le second membre de l'équation (1.10), nous obtenons l'approximation $x_3 = 100 + 11 = 111$. En poursuivant cette procédure, nous obtenons les approximations successives suivantes : $x_1 = 100$, $x_2 = 110$, $x_3 = 111$, $x_4 = 111,1\ldots$ c'est à dire les nombres obtenus par Zénon ; ce sont des approximations décimales du nombre rationnel solution $x = 1000/9$.

Il faut observer que cette méthode fournit une suite qui converge vers la solution cherchée en raison de la petitesse de $x/10$ devant x.

Nous allons nous inspirer de cette idée pour montrer comment les suites peuvent être utilisées pour approcher un nombre réel solution d'une équation de la forme $x = f(x)$, où f est une fonction convenable définie et *continue* sur un intervalle $I \subset \mathbf{R}$ tel que $f(I) \subset I$.

La notion de continuité sera étudiée plus tard. On admettra ici que toutes les fonctions usuelles à savoir les fonctions polynomiales, les fonctions rationnelles, les fonctions

algébriques, les fonctions trigonométriques, le logarithme et l'exponentielle sont continues sur leur ensemble de définition.

Nous allons présenter ici une étude sommaire des suites obtenues par un procédé itératif conduisant dans les bons cas à des approximations de la solution de l'équation $f(x) = x$, appelée *point fixe* de f dans I.

La méthode itérative, dite aussi *méthode des approximations successives*, consiste à choisir une "solution approchée" x_0 de l'équation $f(x) = x$ et à produire par itération des approximations successives $x_1 := f(x_0)$, $x_2 := f(x_1), \ldots, x_n := f(x_{n-1})$ à condition qu'à chaque fois que $x \in I$, on ait aussi $f(x) \in I$, autrement dit $f(I) \subset I$. On dit que la suite $(x_n)_{n\in\mathbf{N}}$ ainsi obtenue est une *suite récurrente* définie par son premier terme $x_0 \in I$ et la relation de récurrence $x_{n+1} = f(x_n)$ permettant pour tout n d'obtenir le terme de rang $n+1$ à partir du terme de rang n en appliquant la même fonction f. Notons f^n l'itérée d'ordre n de f définie par récurrence par $f^1 := f$ et $f^n := f \circ f^{n-1}$ pour $n \geq 2$ qui est bien définie puisque $f(I) \subset I$. Alors on a $x_n = f^n(x_0)$ pour $n \geq 1$. Cette suite est appelée la *suite des itérés* de x_0 par f.

Si la fonction f a de bonnes propriétés et si l'approximation initiale x_0 est bien choisie, on peut espérer que le procédé itératif convergera vers une solution de l'équation $f(x) = x$ dans I, appelée un *point fixe* de f dans I.

C'est ce que suggère le résultat suivant que nous admettrons.

Proposition 1.7.1 *Soit $f : I \longrightarrow \mathbf{R}$ une fonction continue telle que $f(I) \subset I$. Si pour une valeur initiale $x_0 \in I$, la suite des itérés $(x_n)_{n\in\mathbf{N}}$ de x_0 par f converge vers un nombre réel ℓ et que $\ell \in I$, alors ℓ vérifie l'équation $f(\ell) = \ell$ i.e. ℓ est un point fixe de f dans I.*

La méthode itérative a l'avantage de fournir un algorithme (programmable sur ordinateur) pour résoudre numériquement bon nombre d'équations non linéaires.

Nous nous contenterons ici de donner quelques propriétés simples permettant d'étudier quelques exemples bien choisis et donnerons en appendice un théorème de point fixe utile dans la pratique.

Proposition 1.7.2 *Soit I un intervalle de $\mathbf{R}$, $f : I \longrightarrow \mathbf{R}$ une fonction croissante telle que $f(I) \subset I$ et $x_0 \in I$. Alors on a les propriétés suivantes :*
1) Si $f(x_0) > x_0$, la suite des itérés $x_n := f^n(x_0), n \in \mathbf{N}$ est croissante.
2) Si $f(x_0) < x_0$, la suite $x_n := f^n(x_0), n \in \mathbf{N}$ est décroissante.
3) Si $f(x_0) = x_0$ la suite est constante.
Si de plus f est continue sur I et si la suite $(x_n)_{n\geq 0}$ converge vers un nombre réel $\ell \in I$, alors ℓ est une solution de l'équation $f(x) = x$ dans I.

Ce résultat affirme que lorsque f est une fonction croissante de I dans I, pour toute valeur initiale $x_0 \in I$, la suite (x_n) de ses itérés par f est une suite monotone dont le sens de variation est donné par le signe de $f(x_0) - x_0$ et que si elle converge dans I, alors sa limite est un point fixe de f dans I. Mais attention, ce résultat ne dit rien sur l'existence de cette limite. Ce problème doit être étudié au cas par cas.

Démonstration. On vérifie par récurrence sur $n \geq 0$ que, puisque f est croissante, pour tout $n \geq 1$, le nombre réel $x_{n+1} - x_n = f(x_n) - f(x_{n-1})$ est du signe de $x_1 - x_0 = f(x_0) - x_0$. Par conséquent si $f(x_0) \leq x_0$, la suite $(x_n)_{n\geq 0}$ est décroissante et si $f(x_0) \geq x_0$, la suite est croissante. La dernière affirmation résulte de la proposition précédente. □

Proposition 1.7.3 *Soient I un intervalle de $\mathbf{R}$ et $f : I \longrightarrow \mathbf{R}$ une fonction décroissante telle que $f(I) \subset I$. Alors pour tout $x_0 \in I$, les deux suites $(x_{2n})_{n\geq 0}$ et $(x_{2n+1})_{n\geq 0}$ sont monotones. Si de plus f est continue sur I et si ces deux suites convergent dans I, leurs limites respectives sont des solutions de l'équation $f^2(x) = x$ dans I.*

Démonstration. En effet puisque f est décroissante sur I et que $f(I) \subset I$, la fonction $g := f^2 = f \circ f$ est une fonction croissante sur I telle que $g(I) \subset I$. Il résulte de la proposition 1.7.1 précédente que si $x_0 \in I$, la suite récurrente définie par son premier terme $y_0 := x_0$ et la relation de récurrence $y_{n+1} := g(y_n)$ pour $n \geq 0$ est une suite monotone croissante si $g(y_0) \geq y_0$ (i.e. $(x_2 \geq x_0)$) et décroissante si $g(x_0) \leq x_0$ (i.e. $(x_2 \leq x_0)$. Comme $y_n = g^n(y_0) = f^{2n}(x_0) = x_{2n}$ pour $n \geq 0$, il en résulte que la suite $(x_{2n})_{n\geq 0}$ est monotone.
De la même façon la suite récurrente $(z_n)_{n\geq 0}$ définie par son premier terme $z_0 := x_1$ et la relation de récurrence $z_{n+1} = g(z_n)$ pour $n \geq 0$ est monotone croissante si $g(z_0) \geq z_0$ (i.e. $x_3 > x_1$).
Comme $z_n = g^n(z_0) = f^{2n}(f(x_0)) = x_{2n+1}$ pour $n \geq 0$, il en résulte que la suite $(x_{2n+1})_{n\geq 0}$ est monotone.
Si f est continue sur I alors la fonction g est continue sur I et d'après la proposition 1.7.1, si les deux suites récurrentes (y_n) et (z_n) définies par la fonction g convergent dans I, leurs limites sont des points fixes de $g = f^2$ dans I. □

Donnons quelques exemples simples qui montrent comment on peut utiliser ces résultats dans la pratique. Il est conseillé de représenter graphiquement f dans un repère orthonormé du plan en faisant apparaitre le(s) point(s) d'intersection du graphe de f avec la première bissectrice. Ce sont les abscisses de ces points d'intersection qui donnent les points fixes de f.

Exemple.
On fixe deux paramètres a, b et on considère la suite récurrente définie par son premier

terme x_0 et la relation de récurrence linéaire

$$x_{n+1} = ax_n + b,\ n \in \mathbf{N}.$$

Alors $x_1 = ax_0 + b$, $x_2 = ax_1 + b = a^2x_0 + ab + b$, $x_3 = a^3x_0 + a^2b + ab + b, ...$ On voit facilement par récurrence que pour tout $n \in \mathbf{N}^*$, $x_n = a^nx_0 + a^{n-1}b + \cdots ab + b$. Observons que si $b = 0$, la suite $(x_n)_{n\in\mathbf{N}}$ est une suite géométrique de raison a.

1. Si $a = 1$, on obtient $x_n = x_0 + nb$, pour tout $n \in \mathbf{N}$. C'est une suite arithmétique de raison b dont le comportement dépend simplement de b : si $b = 0$ la suite est constante et converge donc vers x_0 ; si $b \neq 0$, la suite a pour limite $+\infty$ si $b > 0$ et $-\infty$ si $b < 0$.
2. Si $a \neq 1$, l'application affine $f(x) = ax + b$ a un point fixe unique $\xi = \frac{b}{1-a}$. Il en résulte que si $x_0 = \frac{b}{1-a}$, la suite (x_n) converge est constante et converge donc vers $\frac{b}{1-a}$.
   Par ailleurs, on sait que

   $$a^{n-1} + \cdots a + 1 = \frac{a^n - 1}{a - 1},$$

   ce qui implique que pour tout $n \in \mathbf{N}^*$,

   $$x_n = x_0a^n + b\frac{a^n - 1}{a - 1} = (x_0 + \frac{b}{a - 1})a^n - \frac{b}{a - 1}.$$

   Si $|a| < 1$, on sait que $\lim_{n\to+\infty} a^n = 0$ et donc

   $$\lim_{n\to+\infty} x_n = \frac{b}{1 - a}.$$

   Si $|a| > 1$ et $x_0 \neq \frac{b}{1-a}$, on en déduit que la suite a une limite infinie de même signe $x_0 - \frac{b}{1-a}$.

On peut facilement interpréter géométriquement ces résultats sur un dessin qu'il est conseillé de faire.

Donnons maintenant un exemple simple qui relève de l'application de la proposition 1.7.2.

Exemple.
On considère ici la suite définie par son premier terme $x_0 \geq 0$ et la relation de récurrence

$$x_{n+1} = x_n^2 + \frac{1}{9},\ n \in \mathbf{N}.$$

Ici on a $x_{n+1} = f(x_n)$, où $f(x) := x^2 + 1/9$ est une fonction polynomiale quadratique. Comme $x_0 \geq 0$, on considère f définie sur l'intervalle fermé $I := [0, +\infty[$. La fonction

f est continue sur I et vérifie $f(I) \subset I$. De plus f est strcitement croissante sur I. D'après la proposition 1.7.2, la suite (x_n) est une suite monotone de l'intervalle I dont le sens de monotonie dépend du signe de $f(x_0) - x_0$ et en cas de convergence, sa limite vérifie l'équation $f(x) = x$ dans I i.e. c'est un point fixe de f dans I.
L'équation $f(x) = x$ dans I s'écrit $x \geq 0$ et $x^2 - x + 1/9 = 0$. Il est facile de vérifier que cette équation a deux solutions dans I :

$$\xi_1 = \frac{3 - \sqrt{5}}{6},\ \xi_2 = \frac{3 + \sqrt{5}}{6} \text{ avec } \xi_1 < \xi_2.$$

Comme $f(x) - x = (x - \xi_1)(x - \xi_2)$, le signe de $f(x_0) - x_0$ dépend de la position relative de x_0 par rapport aux deux points fixes ξ_1 et ξ_2.

1. Si $0 \leq x_0 < \xi_1$, on a $f(x_0) - x_0 > 0$ et donc puisque f est strictement croissante, on en déduit que $x_0 < f(x_0) < f(\xi_1)$ i.e. $0 \leq x_0 < x_1 < \xi_1$. Puisque f est strictement croissante sur $[0, +\infty($, on en déduit par récurrence que pour tout $n \in \mathbf{N}$, $x_n < x_{n+1} < \xi_1$. La suite $(x_n)_{n\in\mathbf{N}}$ est donc strictement croissante et majorée par ξ_1. Il en résulte qu'elle converge vers une limite ℓ vérifiant $0 \leq \ell \leq \xi_1$. Comme f est continue, on en déduit que $f(\ell) = \ell$. D'où $\ell = \xi_1$.
2. Si $\xi_1 < x_0 < \xi_2$, on a $f(x_0) - x_0 < 0$ et puisque f est strictement croissante, on en déduit que $f(\xi_1) < f(x_0) < f(\xi_2)$. D'où $\xi_1 < x_1 < x_0 < \xi_2$. On en déduit par récurrence que pour tout $n \in \mathbf{N}$, $\xi_1 < x_{n+1} < x_n < \xi_2$. La suite $(x_n)_{n\geq 0}$ est donc strictement décroissante et minorée ; elle converge donc vers une limite ℓ vérifiant les inégalités $\xi_1 \leq \ell < x_n$ pour tout $n \in \mathbf{N}$. Autrement dit ℓ est un point fixe de f différent de ξ_2 d'où $\ell = \xi_1$.
3. Si $x_0 > \xi_2$, on a $f(x_0) - x_0 > 0$. D'où $\xi_2 < x_0 < x_1$. La suite $(x_n)_{n\in\mathbf{N}}$ est alors (strictement) croissante. Si elle avait une limite finie ℓ, on aurait $\ell \in I$ et $x_n < \ell$ pour tout $n \in \mathbf{N}$. Le nombre réel ℓ serait un point fixe d e $\ell > \xi_2$, ce qui est impossible. Par conséquent $\ell = +\infty$.

Donnons maintenant un exemple simple qui relève de l'application de la proposition 1.7.3.

Exemple.
Soit $(x_n)_{n\geq 0}$ la suite récurrente définie par son premier terme $x_0 > 0$ et la relation de récurrence $x_{n+1} := 1 + 1/x_n$ pour $n \geq 0$.
Dans cet exemple $x_{n+1} = f(x_n)$ pour tout $n \geq 0$, où $f :]0, +\infty[\longrightarrow]1, +\infty[\subset]0, +\infty[$ est la fonction définie par $f(x) := 1 + 1/x$ pour $x > 0$.
La fonction f est continue, décroissante sur $]0, +\infty[$ et vérifie $f(]0, +\infty[) \subset]0, +\infty[$. Par conséquent la fonction $g = f^2 = f \circ f$ est une fonction continue croissante sur $]0, +\infty[$ telle que $g(]0, +\infty[) \subset]0, +\infty[$ et $x_{n+1} = g(x_{n-1})$ pour $n \geq 1$.
Un calcul simple montre que :

$$g(x) = f(f(x)) = \frac{2x + 1}{x + 1}, x > 0.$$

Comme g est croissante sur $[0,+\infty[$, $\lim_{x\to+\infty} g(x) = 2$ et $g(0) = 1$ il en résulte que $g([0,+\infty[) \subset [1,2[$.
Il en résulte alors en appliquant la proposition 1.7.3 que pour chaque $x_0 > 0$ fixé, les deux sous-suites $(x_{2n})_{n\geq 0}$ et $(x_{2n+1})_{n\geq 0}$ sont des suites monotones bornées de l'intervalle $]0,+\infty[$. Elles possèdent donc des limites finies ℓ_1 et ℓ_2 respectivement qui sont dans $[0,+\infty[$. Pour déterminer ces limites il suffit de passer à la limite dans l'équation $x = g(x)$.
Par conséquent chacune des deux suites converge vers une limite finie qui est un point fixe de g dans $[0,+\infty[$. Or le seul point fixe de g dans $[0,+\infty[$ est $\xi = \frac{1+\sqrt{5}}{2}$. Les deux sous-suites $(x_{2n})_{n\geq 0}$ et $(x_{2n+1})_{n\geq 0}$ convergent donc vers la même limite ξ et donc la suite (x_n) converge vers $\xi = \frac{1+\sqrt{5}}{2}$, appelé *nombre d'or*.

Donnons enfin un exemple simple qui ne relève pas d'une application directe des propositions précédentes mais qui illustre une méthode générale, dite "méthode de Newton", pour approcher les solutions de certaines équations non linéaires qu type $F(x) = 0$, où F est une fonction continue sur un intervalle ayant d'assez bonnes propriétés que nous ne préciserons pas ici.

Exemple *(Approximation de la racine carrée d'un nombre réel).*
Nous avons déjà décrit dans l'introduction la méthode de dichotomie pour construire deux suites de nombres rationels approchant par défaut et par exès respectivement le nombre irrationnel $\sqrt{2}$. Cette méthode s'applique à d'autres équations avec plus ou moins de succès. Nous allons décrire sur un exemple simple une autre méthode pour réaliser cette approximation en beaucoup moins d'étapes pour une précision donnée.
En effet considérons une valeur approchée initiale (même grossière) x_0 de $\sqrt{2}$. Soit $e_0 := \sqrt{2} - x_0$ l'erreur absolue commise en approchant $\sqrt{2}$ par x_0. Alors $(x_0 + e_0)^2 = 2$ et donc $x_0^2 + 2x_0e_0 + e_0^2 = 2$. Si x_0 est assez proche de $\sqrt{2}$, l'erreur absolue e_0 sera assez petite de sorte que de $\varepsilon_0 := e_0^2$ sera négligeable devant e_0. Par conséquent, puisque $2 = (x_0 + e_0)^2 = x_0^2 + 2x_0e_0 + \varepsilon_0$, on en déduit que :

$$e_0 = (2 - x_0^2)/(2x_0) + (-1/2x_0)\varepsilon_0$$

et donc :

$$\sqrt{2} = x_0 + e_0 = x_0 + (2 - x_0^2)/(2x_0) + (-1/2x_0)\varepsilon_0 = x_0/2 + 1/x_0 + (-1/2x_0)\varepsilon_0.$$

Comme ε_0 est négligeable devant e_0, le nombre $(-1/2x_0)\varepsilon_0$ est également négligeable devant e_0 de sorte que le nombre réel $x_1 := x_0/2 + 1/x_0$ réalise une nouvelle approximation de $\sqrt{2}$.
Ainsi à partir d'une approximation x_0 de $\sqrt{2}$, on a obtenu une nouvelle approximation x_1 donnée par la formule $x_1 := x_0/2 + 1/x_0$.
En réitérant ce processus, à partir de l'approximation x_1 de $\sqrt{2}$, on obtiendra une nouvelle approximation x_2 donnée à partir de x_1 par la même formule que celle qui donne

x_1 en fonction de x_0, soit $x_2 = x_1/2 + 1/x_1$.
En réitérant indéfiniment ce processus, on voit par récurrence que si au rang n on a obtenu une approximation x_n de $\sqrt{2}$, ce processus d'approximation fournit au rang $n+1$ une approximation x_{n+1} donnée par la formule $x_{n+1} = x_n/2 + 1/x_n$.
Le même calcul que précédemment montre que l'erreur absolue $e_n := \sqrt{2} - x_n$ commise en approchant $\sqrt{2}$ par x_n est telle que $e_n = -e_{n-1}^2/(2x_n)$ qui est négligeable devant e_{n-1}, lorsque e_{n-1} est assez petit. On obtient ainsi une suite récurrente qui semble converger (faire un dessin).
C'est ce que nous allons démontrer.
Le procédé heuristique décrit précédemment s'applique également à l'approximation de la solution de l'équation $x^2 = a$, où $a \in \mathbf{R}^+$, n'est pas le carré d'un nombre rationnel. On est alors conduit à considérer la suite récurrente définie comme suit. Choisissons $x_0 \in \mathbf{Q}, x_0 > 0$ et posons pour $n \geq 0$:

$$x_{n+1} := \frac{1}{2}(x_n + \frac{a}{x_n}).$$

Nous allons démontrer qu'en fait la suite (x_n) converge vers $\sqrt{a}$ quelque soit la valeur initiale choisie $x_0 > 0$. Nous donnerons également une estimation de l'erreur d'approximation $e_n := \sqrt{a} - x_n$ au rang $n \geq 1$ en fonction de n et de l'erreur initiale $e_0 := \sqrt{a} - x_0$.
Observons que la fonction $f(x) := \frac{1}{2}(x + \frac{a}{x})$ définie sur $]0, +\infty[$ possède les deux propriétés suivantes :
Propriété 1 :

$$f(x) \geq \sqrt{a}, \forall x > 0.$$

En effet pour $x > 0$, on a $f(x) - \sqrt{a} = \frac{1}{2}(x + a/x) - \sqrt{a} = \frac{1}{2x}(x^2 - 2\sqrt{a} + 2) = \frac{1}{2x}(x - \sqrt{a})^2 \geq 0$.
Propriété 2 :

$$f(x) - x \leq 0, \forall x \geq \sqrt{a}.$$

En effet pour $x > 0$, on a $f(x) - x = \frac{1}{2x}(x^2 + a) - x = \frac{1}{2x}(a - x^2) \leq 0$ si $x \geq \sqrt{a}$.
Il résulte de la propriété 1 que pour tout $x_0 > 0$, on a $x_1 := f(x_0) \geq \sqrt{a}$. D'après la Propriété 2, on montre par récurrence que pour tout $n \geq 1$ $x_n \geq \sqrt{a}$ et $x_{n+1} \leq x_n$.
Ainsi la suite $(x_n)_{n \geq 1}$ est décroissante et minorée par 0 elle converge donc vers un nombre réel $\ell \geq 0$.
Comme pour $n \geq 1$, on a $x_n = \frac{1}{2x_{n-1}}(x_n^2 + a)$ et donc $2x_n x_{n-1} = x_n^2 + a$ pour tout $n \geq 1$. En passant à la limite dans cette équation, on obtient $2\ell^2 = \ell^2 + a$ et donc $\ell^2 = a$. Comme $\ell \geq 0$, on en déduit que $\ell = \sqrt{a}$.
Nous allons démontrer que l'erreur d'approximation d'ordre $n \geq 1$ définie par $e_n := \sqrt{a} - x_n$ vérifie la relation :

$$e_{n+1} = \frac{e_n^2}{2x_n}. \tag{1.11}$$

En effet, pour $n \geq 1$, on a

$$\begin{aligned} e_{n+1} &= x_{n+1} - \sqrt{a} \\ &= \frac{1}{2x_n}(x_n^2 + a) - \sqrt{a} \\ &= \frac{1}{2x_n}(x_n - \sqrt{a})^2 == \frac{1}{2x_n} e_n. \end{aligned}$$

Supposons que $a > 1$. Alors d'après (1.11), on $x_n > 1$ pour tout $n \geq 1$ et donc d'après (1.11) on a $e_{n+1} \leq e_n^2/2$ pour tout $n \geq 1$. On en déduit par récurrence que :

$$e_n \leq \frac{e_0^2}{2^n}, \forall n \geq 1.$$

En utilisant cette estimation on peut tout de suite déterminer le nombre d'itérations suffisantes pour approcher $\sqrt{a}$ avec une précision donnée à l'avance.
Soit par exemple à déterminer une approximation de $\sqrt{2}$ à 10^{-3} près. On doit alors choisir un entier $n \geq 1$ tel que $e_n \leq 10^{-3}$ pour obtenir une approximation x_n de $\sqrt{2}$ à 10^{-3} près. Il suffit pour cela que l'on ait $\frac{e_0^2}{2^n} \leq 10^{-3}$. On a intérêt à choisir x_0 le plus près possible de $\sqrt{2}$ de facon à ce que e_0 soit assez petit et qu'alors le nombre d'itérations suffisant n soit le moins grand possible. Comme on voit facilement que $1,4 < \sqrt{2} < 1,5$ en prenant $x_0 = 1,5$ on en déduit que $0 < e_0 = 1,5 - \sqrt{2} < 0,1$. Il suffit donc de choisir n tel que $(0,1)^2/2^n \leq 10^{-3}$ i.e. $2^n > 10$ et donc $n = 4$ convient. Ainsi si $x_0 = 1,5$ la valeur x_4 est une approximation par excès de $\sqrt{2}$ à 10^{-3} près i.e. $x_4 - 10^{-3} < \sqrt{2} < x_4$. Calculons x_4. On a alors successivement $x_1 = \frac{1}{2x_0}(x_0^2 + 2)$ ...

La méthode utilisée ici pour déterminer une valeur approchée de la racine carrée porte le nom de "méthode de Héron"'. C'est un cas particulier d'une méthode plus générale, dite "méthode de Newton" qui permet de déterminer une approximation de la solution de certaines equations du type $F(x) = 0$.

Complément :

Soit $\alpha \in \mathbf{R}^+$ un paramètre réel. Considérons la suite récurrente définie par son premier terme $x_0 \in \mathbf{R}$ et la relation de récurrence $x_{n+1} := x_n^2 + \alpha$ pour $n \geq 0$.
Il s'agit d'étudier suivant les valeurs du paramètre $\alpha \geq 0$ et du terme initial x_0, la nature de la suite $(x_n)_{n\geq 0}$.
On a $x_{n+1} = f_\alpha(x_n)$ pour $n \geq 0$, où $f_\alpha(x) := x^2 + \alpha$ pour $x \in \mathbf{R}$ est une fonction polynomiale de degré 2 qui est donc une fonction continue sur $\mathbf{R}$.
1) Observation générale : On vérifie facilement ("à la main") que la fonction f_α est une fonction paire, croissante sur $[0, +\infty[$ à valeurs dans $[\alpha, +\infty[\subset [0, +\infty[$.
La suite $(x_n)_{n\geq 1}$ est donc une suite récurrente de premier terme $x_1 \in [0, +\infty[$ définie par la fonction croissante $f_\alpha : [0, +\infty[\longrightarrow [0, +\infty[$. Il résulte alors de la proposition

6.2 que la suite $(x_n)_{n\geq 1}$ est donc une suite monotone et par conséquent, elle possède une limite finie ou infinie $\ell \geq 0$. De plus si cette limite ℓ est finie, elle est solution de l'équation $f_\alpha(x) = x$ dans $[0, +\infty[$ d'après la proposition 6.1

2) Résolution de l'équation $f_\alpha(x) = x$ dans $[0, +\infty[$.

Il s'agit donc de résoudre l'équation $x^2 - x + \alpha = 0$ dans $[0, +\infty[$. Le discriminant de cette équation du second degré est $\Delta = 1 - 4\alpha$. Par conséquent :

- Si $\alpha > 1/4$, l'équation $x^2 - x + \alpha = 0$ n'a pas de solution dans $\mathbf{R}$.
- Si $\alpha < 1/4$, l'équation $x^2 - x + \alpha = 0$ a deux solutions $\xi_1 = (1 - \sqrt{1 - 4\alpha})/2 < 0$ et $\xi_2 = (1 + \sqrt{1 - 4\alpha})/2 > 0$.
- Si $\alpha = 1/4$, l'équation $x^2 - x + \alpha = 0$ a une solution double $\xi_1 = \xi_2 = 1/2$.

3) Nature de la suite

Il y a donc trois cas à considérer suivant les valeurs de α.

(i) Cas où $\alpha > 1/4$.

Dans ce cas, le trinôme du second degré $x^2 - x + \alpha$ n'a pas de solution réelle et $f(x) - x = x^2 - x + \alpha > 0$ pour tout $x \in \mathbf{R}$. Comme f_α est croissante sur $[0, +\infty[$ à valeurs dans $[0, +\infty[$, on en déduit grâce à la la proposition 6.2 que la suite $(x_n)_{n\geq 1}$ est une suite croissante. Si sa limite ℓ était finie, elle serait solution de l'équation $x^2 - x + \alpha = 0$. Comme cette équation n'a pas de solution dans ce cas, il en résulte alors que $\ell = \lim_{n\to+\infty} x_n = +\infty$.

(ii) Cas où $\alpha = 1/4$.

Comme dans ce cas $f_\alpha(x) - x = x^2 - x + \alpha = x^2 - x + 1/4 = (x - 1/2)^2 \geq 0$ pour tout $x \in \mathbf{R}$, il résulte de la proposition 6.2 que la suite $(x_n)_{n\geq 1}$ est strictement croissante sauf si $x_0 = 1/2$ auquel cas la suite est constante. De plus dans le cas présent l'équation $f_\alpha(x) = x$ a une solution double égale à $1/2$.

- Si $x_0 > 1/2$, comme f_α est croissante sur $[0, +\infty[$ et que $f_\alpha(1/2) = 1/2$, on en déduit par récurrence sur $n \geq 0$ que $x_n > 1/2$ pour tout $n \geq 1$.

Ainsi $(x_n)_{n\geq 1}$ est une suite croissante telle que $x_n \geq x_0 > 1/2$ pour tout $n \geq 1$. D'après le principe de prolongement des inégalités, la limite ℓ de la suite (x_n) vérifie l'inégalité $\ell \geq x_0 > 1/2$. Si ℓ était finie, ℓ serait solution de l'équation $f_\alpha(x) = x$ et on en déduirait que $\ell = 1/2$, ce qui est absurde. Par conséquent $\ell = \lim_{n\to+\infty} x_n = +\infty$.

- Si $0 \leq x_0 \leq 1/2$, on montre que puisque f_α est croissante sur $[0, +\infty[$ on a $x_n \leq 1/2$ et donc la suite (x_n) est croissante et majorée. Elle converge donc vers $1/2$.

Pour les autres valeurs de x_0, on se ramène aux cas précédents grâce à la parité de f_α. En effet,

- si $-1/2 \leq x_0 < 0$, alors $0 \leq -x_0 \leq 1/2$ et donc $x_1 = f_\alpha(x_0) = f_\alpha(-x_0) > 1/2$ et donc d'après le premier cas $(x_n)_{n\geq 0}$converge vers $1/2$.
- Si $x_0 < -1/2$, alors $-x_0 > 1/2$ et donc $x_1 = f_\alpha(x_0) = f_\alpha(-x_0) > 1/2$ et donc d'après le premier cas $(x_n)_{n\geq 0}$ tend vers $+\infty$.

(iii) Cas où $0 < \alpha < 1/4$. Dans ce cas f_α a deux points fixes $\xi_1 < 0 < \xi_2$ et $f(x) - x = (x - \xi_1)(x - \xi_2)$ pour $x \in \mathbf{R}$.

- Si $x_0 > \xi_2$, alors $f(x_0) - x_0 > 0$ et donc la suite $(x_n)_{n\geq 0}$ est croissante et sa limite

vérifie l'inégalité $\ell \geq x_0 > \xi_2$. Si ℓ était fini, il serait égal à l'un des deux points fixes ξ_1 et ξ_2, ce qui est impossible. Par conséquent $\ell = +\infty$.
- Si $\xi_1 < x_0 < \xi_2$, comme $f(x) - x < 0$, pour $\xi_1 < x < \xi_2$, on en déduit par récurrence que $\xi_1 < x_{n+1} < x_n < \xi_2$, pour tout $n \in \mathbf{N}$. La suite $(x_n)_{n\geq 0}$ est alors décroissante et minorée ; elle converge donc vers une limite ℓ vérifiant $\xi_1 \leq \ell < x_0 < \xi_2$. Comme ℓ est nécessairement un point fixe de f_α, on en déduit que $\ell = \xi_1$.
- Si $0 \leq x_0 < \xi_1$, comme $f_\alpha(x) - x > 0$ pour $x < \xi_1$ et $f([0, \xi_1]) \subset [0, \xi_1]$, la suite (x_n) est croissante et majorée par ξ_1 elle converge donc vers ξ_1.
Pour $x_0 < 0$, on a $x_1 = f(x_0) = f(-x_0)$ avec $-x_0 > 0$ et on est donc ramené aux cas précédents.

L1- Module UE8 (Mathématiques II) : Feuille de TD no 3 (Semaine 5)

Exercice 1.
On fixe un nombre réel $a \geq 0$.
1) Démontrer que l'on définit une suite de nombres réels positifs $(u_n)_{n\geq 0}$ en posant :

$$u_0 = a \ , \quad u_{n+1} = \frac{u_n}{1+u_n} + 1, \quad \text{si } n \geq 0.$$

2) Calculer $u_{n+1} - u_n$ en fonction de u_n et en déduire que la suite $(u_n)_{n\geq 0}$ est décroissante.
3) Démontrer que la suite $(u_n)_{n\geq 0}$ est c onvergente et déterminer sa limite ℓ.
4) Démontrer que $|u_{n+1} - \ell| \leq \frac{1}{1+\ell} \ |u_n - \ell|$.
En déduire une majoration de $|u_{n+1} - \ell|$ en fonction de n et de a.

Exercice 2.
Soit $a \in \mathbf{R}$ un paramètre réel tel que $a > 4$.
1. Démontrer qu'on peut définir une suite $(x_n)_{n\geq 0}$ par récurrence en posant $x_0 = a$ et

$$x_{n+1} = \frac{x_n - 6}{x_n - 4}, \quad n \geq 0.$$

Que se passe-t-il si $a \leq 4$?
2. Démontrer que l'application $x \longmapsto \frac{x-6}{x-4}$ possède deux points fixes α, β avec $\alpha < \beta$ que l'on déterminera.
3. On suppose que $a \notin \{\alpha, \beta\}$. On pose :

$$y_n := \frac{x_n - \alpha}{x_n - \beta}, \quad n \geq 0.$$

Calculer y_{n+1} en fonction de y_n et en déduire la limite de $(x_n)_{n\geq 0}$.

Exercice 3.
Soit $(x_n)_{n\geq 0}$ la suite définie par son premier terme $x_0 \neq -1$ et la relation de récurrence :

$$x_{n+1} = \frac{3x_n - 1}{x_n + 1}, \quad n \geq 0.$$

1) Démontrer que l'application $x \longmapsto \frac{3x-1}{x+1}$ possède un seul point fixe $q \in \mathbf{R}$.
2) On suppose que $x_0 \neq q$ et on pose $y_n := \frac{1}{x_n - q}$ pour $n \geq 0$. Calculer y_{n+1} en fonction de y_n et en déduire la limite de la suite $(y_n)_{n\geq 0}$.
3) Calculer la limite de la suite $(x_n)_{n\geq 0}$.

Exercice 4.
Considérons la suite de Fibonacci définie par ses deux premiers termes $u_0 = 1, u_1 = 1$ et la relation de récurrence linéaire d'ordre 2 suivante :

$$(F) \qquad u_{n+2} = u_{n+1} + u_n, \quad n \geq 0.$$

Pour calculer le nombre u_{21} par exemple, il suffirait à priori de calculer tous les termes $u_3, u_4, \ldots, u_{19}$ et u_{20}, ce qui est fastidieux. Il est donc naturel de se poser la question de savoir s'il existe une formule explicite donnant u_n en fonction de n. C'est l'objet de cet exercice.
1. Soit $q \in \mathbf{R}^*$. Démontrer que la suite géométrique $(q^n)_{n\in\mathbf{N}}$ vérifie la condition (F) si et seulement si le nombre réel vérifie l'équation algébrique $q^2 - q - 1 = 0$.
2. Trouver les deux valeurs q_1 et q_2 du paramètre $q \in \mathbf{R}$ tel que la suite géométriques $(q^n)_{n\in\mathbf{N}}$ vérifie la relation (F).
3. Touver deux constantes numériques α, β tels que la suite de Fibonacci sécrive : $u_n = \alpha q_1^n + \beta q_2^n$ pour tout $n \in \mathbf{N}$.
4. En déduire la formule suivante donnant les nombres de Fibonacci :

$$u_n = \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^{n+1} - \left(\frac{1-\sqrt{5}}{2} \right)^{n+1} \right), \forall n \geq 0. \tag{1.12}$$

Observons que par définition les nombres de Fibonacci sont des entiers !

La suite de Fibonacci est en fait une suite strictement croissante d'entiers naturels qui tend donc vers $+\infty$. Cette suite a des propriétés importantes et intervient dans plusieurs domaines des sciences.

1.8 Appendice 1 : Le critère de Cauchy

Il arrive souvent que l'on ait à étudier une suite obtenue par un procédé qui ne soit pas tout à fait explicite ou que même s'il est explicite, il ne soit pas évident de deviner la limite d'une telle suite. On a vu que si la suite est monotone, on peut décider de sa convergence. Dans le cas contraire, comment décider si une suite converge ou pas sans en connaitre a priori la limite ? La réponse à cette question sera donnée par le théorème remarquable qui va suivre.

Auparavant observons le fait simple suivant.

Proposition 1.8.1 *Si $(x_n)_{n\in\mathbf{N}}$ est une suite qui converge vers un nombre réel ℓ alors pour tout $\varepsilon > 0$, il existe un rang $N > 1$ tel que pour tous entiers $n \geq m \geq N$ on ait $|x_n - x_m \leq \varepsilon$.*

Démonstration. En effet soit $\varepsilon > 0$. Par définition de la convergence il existe un rang $N > 1$ tel que pour $n \geq N$, on ait $|x_n - \ell| \leq \varepsilon$. Alors si m et n sont deux entiers tels que $m \geq N$ et $n \geq N$ on a par l'inégalité triangulaire $|x_n - x_m| = |(x_n - \ell) + (\ell - x_m)| \leq |x_n - \ell| + |\ell - x_m| \leq 2\varepsilon$. Ce qui prouve le théorème en remplaçant ε par $\varepsilon/2$. □

Cette proposition exprime l'idée intuitive que les termes de la suite sont arbitrairement proches les uns des autres à partir d'un certain rang.

Il faut observer que cette propriété a l'immense avantage de ne faire intervenir que les termes de la suite elle-même et non sa limite qui est en général difficile à connaitre. Il est alors naturel de se demander si cette condition est suffisante pour impliquer la convergence.

Auparavant adoptons la définition suivante.

Définition 1.8.2 *On dit d'une suite $(x_n)_{n\in\mathbf{N}}$ est une suite de Cauchy si pour tout $\varepsilon > 0$, il existe une rang $N > 1$ tel que pour tout entier $p \geq 1$ et tout entier $n \geq N$ on ait $|x_{n+p} - x_n| \leq \varepsilon$.*

Il est remarquable que cette propriété suffise à démontrer la convergence d'une suite comme le montre le théorème fondamental suivant.

Théorème 1.8.3 (Critère de Cauchy) *Soit $(x_n)_{n\in\mathbf{N}}$ une suite de Cauchy de nombres réels. Alors il existe un nombre réel ℓ tel que la suite converge $(x_n)_{n\in\mathbf{N}}$ converge vers ℓ.*

Ce théorème est un théorème d'existence qui affirme l'existence d'une limite pour une suite de Cauchy de nombres réels.

La démonstration de ce théorème est constructive car elle utilise le théorème des suites adjacentes. Nous allons donc la donner.

Démonstration. Puisque $(x_n)_{n\in\mathbf{N}}$ est une suite de Cauchy, pour tout entier $n \geq 1$ fixé, en posant $\varepsilon := 2^{-n}$, il existe un rang $N > 1$ tel que pour $p \geq q \geq N$, $|x_p - x_q| \leq 2^{-n}$. Désignons par N_n le plus petit des entiers N vérifiant cette propriété. Alors la suite $(N_n)_{n\geq 1}$ est croissante. Posons pour $n \geq 1$:

$$I_n := [x_{N_n} - \frac{1}{2^{n-1}}, x_{N_n} + \frac{1}{2^{n-1}}].$$

Alors I_n est l'intervalle de centre x_{N_n} et de rayon $\frac{1}{2^{n-1}}$. Montrons que $I_{n+1} \subset I_n$ pour tout $n \geq 1$. En effet si $x \in I_{n+1}$, on $|x - x_{N_{n+1}}| \leq 2^{-n}$ et donc par application de l'inégalité triangulaire, on en déduit que

$$|x - x_{N_n}| \leq |x - x_{N_{n+1}}| + |x_{N_{n+1}} - x_{N_n}| \leq 2^{-n} + 2^{-n} = 2^{-n+1},$$

ce qui implique $x \in I_n$. Comme $|I_n| = 2^{-n+2}$ tend vers 0, le théorème des segments emboités implique qu'il existe un nombre réel $c \in \cap_{n\geq 1} I_n$. Comme par définition pour tout $n \geq 1$ et pour tout $p \geq n, x_p \in I_n$, on en déduit que

$$|x_p - c| \leq |x_p - x_{N_n}| + |x_{N_n} - c| \leq 2^{-n} + 2^{-n+1} = 3 \cdot 2^{-n}.$$

Par conséquent la suite $(x_n)_{n\in\mathbf{N}}$ converge vers c. □

Ce théorème constitue surtout un outil théorique important. Nous en donnerons des applications ci-dessous.

Il faut observer que la notion de suite de Cauchy peut se définir dans $\mathbf{Q}$ de la même façon que dans $\mathbf{R}$. Il est alors clair que dans $\mathbf{Q}$ il y a des suites de Cauchy qui n'ont pas de limites dans $\mathbf{Q}$. En effet tout nombre irrationnel est limite d'une suite de nombres rationnels, laquelle est alors une suite de Cauchy dans $\mathbf{Q}$ qui ne converge pas dans $\mathbf{Q}$.

En fait on peut voir $\mathbf{R}$ comme l'ensemble des limites des suites de Cauchy de $\mathbf{Q}$. C'est dans ce sens que l'on dit que $\mathbf{Q}$ n'est pas "complet" et que $\mathbf{R}$ est son "complété".

On peut utiliser cette idée pour donner une nouvelle construction de $\mathbf{R}$ à partir de $\mathbf{Q}$.

Comme application du critère de Cauchy nous allons énoncer le théorème du point fixe.

Théorème 1.8.4 *Soit $f : I \longrightarrow \mathbf{R}$ une fonction definie sur un intervalle fermé $I \subset \mathbf{R}$ telle que $f(I) \subset I$.*
Supposons qu'il existe un nombre réel positif $0 < k < 1$ tel que pour tout $x \in I$ et $y \in I$ on ait :

$$|f(x) - f(y)| \leq k|x - y|.$$

Alors pour tout $x_0 \in I$ la suite récurrente de premier terme x_0 définie par la relation de récurrence $x_{n+1} = f(x_n)$ pour $n \geq 0$ converge vers un nombre réel $\xi \in II$ vérifiant l'équation $f(\xi) = \xi$. De plus ξ est l'unique point fixe de de f dans I.

Démonstration. En effet, soit $n \in \mathbf{N}^*$. On a $|x_{n+1} - x_n| = |f(x_n) - f(x_{n-1})|$ et d'après l'hypothèse sur f, on en déduit que

$$|x_{n+1} - x_n| \leq k|x_n - x_{n-1}|.$$

En itérant cette inégalité, on en déduit par récurrence que pour tout $n \in \mathbf{N}^*$,

$$|x_{n+1} - x_n| \leq k^n|x_1 - x_0|.$$

Soient et $p \in \mathbf{N}^*$, en remarquant que $x_{n+p} - x_n = \sum_{j=1}^{p}(x_{n+j} - x_{n+j-1})$ et en appliquant l'inégalité triangulaire pour la valeur absolue, on en déduit que

$$\begin{aligned} |x_{n+p} - x_n| &\leq \sum_{j=1}^{p} |x_{n+j} - x_{n+j-1}| \\ &\leq \sum_{j=1}^{p} k^{n+j-1} = k^n \sum_{j=1}^{p} k^{j-1}. \end{aligned}$$

Comme $0 < k < 1$, on a $\sum_{j=1}^{p} k^{j-1} < \frac{1}{1-k}$ et donc

$$|x_{n+p} - x_n| \leq \frac{k^n}{1-k}.$$

Fixons $\varepsilon > 0$. Comme $0 < k < 1$, on a $\lim_{n\to+\infty} \frac{k^n}{1-k} = 0$ et donc il existe un rang $N \in \mathbf{N}^*$ tel que pour tout $n \geq N$, $\frac{k^n}{1-k} \leq \varepsilon$. Il en résulte alors que pour tout $n \geq N$ et tout $p \in \mathbf{N}$, on a $|x_{n+p} - x_n| \leq \varepsilon$. Ce qui prouve que la suite $(x_n)_{n\in\mathbf{N}}$ est une suite de Cauchy qui converge donc vers un nombre réel $\xi \in I$ d'après le critère de Cauchy. Comme la condition sur f implique qu'elle est continue sur I, on en déduit par la proposition 1.7.1 que $f(\xi) = \xi$. □

1.9 Appendice 2 : Une construction des nombres réels

La construction des nombres réels ne fait pas partie du programme de cette première période, mais elle est essentielle d'un point de vue conceptuel puisque toute l'Analyse mathématique est fondée sur l'existence et les propriétés du corps $\mathbf{R}$ des nombres réels.

Il nous a donc semblé utile d'essayer de donner au lecteur curieux et intéressé une idée de ce que sont les nombres réels sans pour autant l'encombrer avec des considérations trop techniques.

Il existe plusieurs constructions du corps des nombres réels. Elles sont toutes relativement délicates et par moments assez laborieuses lorsqu'il s'agit de démontrer que l'ensemble défini possède toutes les bonnes propriétés.

Nous allons présenter ici la construction de Dedekind basée sur la notion de coupures. Cette construction est importante du point de vue historique puisque c'est la première construction qui est apparu vers la fin du XIX^e siècle. En plus elle a l'avantage de permettre une définition assez simple et finalement assez intuitive de l'ensemble $\mathbf{R}$ des nombres réels tout en donnnant un accès assez direct à certaines propriétés fondamentales de l'ensemble $\mathbf{R}$ (densité de $\mathbf{Q}$ dans $\mathbf{R}$ et théorème de la borne supérieure).

L'idée de Dedekind part de l'observation simple selon laquelle tout nombre rationnel $s \in \mathbf{Q}$ découpe l'ensemble des rationnels en deux parties : la partie $\mathbf{s}_\star$ des nombres rationnels $r \in \mathbf{Q}$ tels que $r < s$ et la partie $\mathbf{s}^\star$ des nombres rationnels $r \in \mathbf{Q}$ tels que $r \geq s$. L'une des parties suffit d'ailleurs pour déterminer l'autre puisqu'elles sont complémentaires dans $\mathbf{Q}$: $\mathbf{s}^\star = \mathbf{Q} \setminus \mathbf{s}_\star$.

Suivant la même idée, on voit ainsi que pour appréhender l'éventuelle solution de l'équation $x^2 = 2$, du point de vue des nombres rationnels, on est naturellement conduit, suivant l'idée de Dedekind, à "découper" l'ensemble $\mathbf{Q}$ des nombres rationnels en deux parties : $D := \mathbf{Q}_- \cup \{r \in \mathbf{Q}_+; r^2 < 2\}$ et $E := \{r \in \mathbf{Q}_+; r^2 \geq 2\}$,où $\mathbf{Q}_-$ et $\mathbf{Q}_+$ désignent l'ensemble des nombres rationnels négatifs et positifs respectivement.

Il résulte du principe de dichotomie (voir paragraphe 1) que le couple (D, E) possède les propriétés remarquables suivantes :

(C.1) Les ensembles D et E forment une partition de $\mathbf{Q}$ i.e. ce sont des parties non vides et propres de $\mathbf{Q}$ complémentaires l'une de l'autre.

(C.2) Pour tout $a \in D, b \in E$, on a $a < b$.

(C.3) Pour tout $\varepsilon \in \mathbf{Q}_+^*$ il existe $(a, b) \in D \times E$ tel que $0 < b - a \leq \varepsilon$.

Les deux premières propriétés expriment l'idée intuitive que tous les nombres rationnels se répartissent en deux ensembles disjoints : l'ensemble D des approximants rationnels par défaut de ce "futur nombre irrationnel" positif et l'ensemble E de ses

approximants rationnels par excès.

La propriété (C.3) se traduit en disant que les deux parties D et E sont *adjacentes* et exprime qu'idéalement le "meilleur" des approximants rationnels par défaut tend à coïncider avec le "meilleur des approximants rationnels par excès et que leur valeur idéale commune est le nombre réel qui manque entre tous les rationnels dont le carré est moins que 2 et ceux dont le carré est plus que 2. Enfin un trou comblé !

On peut démontrer (voir exercice 6) que dans l'ensemble totalement ordonné des nombres rationnels il n'y a pas de plus grand approximant rationnel par défaut de $\sqrt{2}$ dans le sens où D n'a pas de plus garnd élément. De même qu'il n'existe pas de plus petit approximant rationnel par excès dans le sens où E n'a pas de plus petit élément. C'est précisément ce genre de lacune qui fait de $\mathbf{Q}$ un corps totalement ordonné "incomplet". Dans ce cas précis c'est le "nombre idéal" représenté par cette "coupure" (D, E) qui représentera dans l'ensemble des coupures la solution, notée $\sqrt{2}$ de l'équation $x^2 = 2$.

Nous allons présenter la construction de $\mathbf{R}$ basée sur la notion de "coupure" due à Dedekind en insistant sur les propriétés qui nous parraissent naturelles et en ommettant les détails techniques qui sont assez laborieux.

Par définition, une *coupure de* $\mathbf{Q}$ au sens de Dedekind est un couple $c = (D, E)$ de parties de $\mathbf{Q}$ vérifiant les trois propriétés (C.1), (C.2) et (C.3) ci-dessus. On peut démontrer grâce au principe de dichotomie que la propriété (C.3) est une conséquence des deux autres propriétés.

L'ensemble D possède la propriété suivante : si $d \in D$ alors $\{x \in \mathbf{Q}; x \leq d\} \subset D$. On dira que D est une section finissante : c'est la section finissante de la coupure $c = (D, E)$. L'ensemble E possède la propriété duale suivante : si $e \in E$, $\{y \in \mathbf{Q}; y \geq e\} \subset E$. On dira que E est une section commençante : c'est la section commençante de la coupure c.

Ainsi une coupure est un couple (A, B) de parties de $\mathbf{Q}$ formant une partition de $\mathbf{Q}$ en deux *parties adjacentes* telles que A soit une section finissante, B une section commençant dans $\mathbf{Q}$.

C'est ainsi que par définition $\sqrt{2}$ est défini par la coupure (D_0, E_0), où $D_0 := \mathbf{Q}^- \cup \{r \in \mathbf{Q}^+; r^2 \leq 2\}$ et $E_0 := \{r \in \mathbf{Q}^+; r^2 \geq 2\}$.

Observer que dans cet exemple D_0 est une partie non vide et majorée de $\mathbf{Q}$ qui n'a pas de plus grand élément et que E_0 est une partie non vide et minorée de $\mathbf{Q}$ qui n'a pas de plus petit élément (voir exercice 6).

En fait une coupure $c = (A, B)$ de $\mathbf{Q}$ est entièrement déterminée par l'une de ses

deux sections A ou B puisqu'elles sont complémentaires l'une de l'autre dans $\mathbf{Q}$ i.e. $A = \overline{B}$ en notant $\overline{B}$ le compl'ementaire de B dans $\mathbf{Q}$.

Tout nombre rationnel $s \in \mathbf{Q}$ définit de façon naturelle une coupure de $\mathbf{Q}$ à savoir la coupure $\mathbf{s} := (s_\star, s^\star)$, où $s^\star := \{r \in \mathbf{Q}; r < s\}$ et $s_\star := \{r \in \mathbf{Q}; r \geq s\}$.

Observer que dans ce cas la partie $s_\star$ est une section finisante qui ne possède pas de plus grand élément alors que la partie $s^\star$ est une section commençante qui a un plus petit élément qui est précisément s.

On pourrait bien sur considérer la coupure (s', s''), où $s' := \{x \in \mathbf{Q}; x \leq s\}$ et $s'' := \{x \in \mathbf{Q}; x > s\}$. La différence essentielle avec la coupure précédente étant que $s_\star$ n'a pas de plus grand élément alors que s' en a un.

Compte tenu de cette convention, on peut donc identifier une *coupure* de $\mathbf{Q}$ au sens de Dedekind à une section finissante de $\mathbf{Q}$ qui n'admet de plus grand élément. Suivant cette identification, on pose la définition suivante.

Définition 1.9.1 *On appelle coupure ou nombre réel, une partie $\alpha \subset \mathbf{Q}$ vérifiant les propriétés suivantes :*

1. $\alpha \neq \emptyset$, $\alpha \neq \mathbf{Q}$,
2. $\forall x \in \alpha$, $\forall y \in \mathbf{Q} \setminus \alpha$, $x < y$,
3. *α n'a pas de plus grand élément.*

On peut facilement montrer l'équivalence des deux définitions. On désignera provisoirement par $\mathcal{C} \subset P(\mathbf{Q})$ l'ensemble des coupures au sens de cette définition. Une coupure $\alpha \in \mathcal{C}$ sera dite *rationnelle* s'il existe $s \in \mathbf{Q}$ tel que $\alpha = s_\star$.

Il en résulte que l'application :

$$\iota : \mathbf{Q} \longrightarrow \mathcal{C}$$

qui à un nombre rationnel $s \in \mathbf{Q}$ associe la coupure qu'il définit $\iota(s) := s_\star := \{x \in \mathbf{Q}; x < s\}$ est une application injective qui permet d'identifier $\mathbf{Q}$ à un sous ensemble $\iota(\mathbf{Q})$ de $\mathcal{C}$. Une coupure $\alpha \in \mathcal{C}$ sera dite *irrationnelle* si elle n'est pas rationnelle.

Il est facile de définir une relation d'ordre sur $\mathcal{C}$. Observons tout d'abord que si s_1, s_2 sont des nombres rationnels alors on a $s_1 \leq s_2$ si et seulement si les coupures qu'ils définissent vérifient l'inclusion $\iota(s_1) \subset \iota(s_2)$. Il est donc naturel de poser la définition suivante. Si $\alpha, \alpha' \in \mathcal{C}$, on dira que $\alpha \leq \alpha'$ si et seulement si $\alpha' \subset \alpha$. Il est évident que cette relation est une relation d'ordre sur $\mathcal{C}$ qui prolonge celle de $\mathbf{Q}$ modulo l'indentification entre les nombres rationnels et les coupures rationnelles qu'ils définissent.

On peut démontrer sans trop de difficultées que $\mathcal{C}$ muni de la relation d'ordre d'inclusion est un ensemble totalement ordonné, archimédien dans lequel toute partie non vide et majorée admet une borne supérieure. L'objectif est donc en partie atteint.

Il résulte de cette définition qu'un nombre réel x est une coupure de $\mathbf{Q}$ représentée par un ensemble formée de tous les nombres rationnels strictement plus petit que x et dont x est la borne sup'erieure.

Cette construction permet de façon naturelle de représenter géométriquement l'ensemble des nombres réels par les points d'une droite orientée sur laquelle on a choisi une origine représentant le nombre réel 0 et un sens positif représentant la relation d'ordre sur $\mathbf{R}$. La propriété (C.3) exprime alors la propriété de "continuité" de l'ensemble des nombres réels à l'image des points d'une droite.

Observons également que la propriété (C.3) exprime que tout nombre réel c peut être approché, aussi bien par défaut que par excès, par des nombres rationnels avec une erreur aussi petite que l'on veut.

La partie la plus délicate et la plus technique de cette construction est celle qui consiste à munir $\mathcal{C}$ d'une addition $+$ et d'une multiplication $\cdot$ compatibles avec la relation d'ordre ci-dessus de telle sorte que $(\mathcal{C}, +, \cdot)$ soit un corps commutatif dont $\mathbf{Q}$ est un sous-corps i.e. ι est un homomorphisqme de corps.

On peut démontrer que cela est possible, mais nous omettrons tous ces détails qui ne seront pas utiles dans la suite et nous admettrons le théorème suivant.

Théorème 1.9.2 (Théorème de Dedekind) *L'ensemble $\mathcal{C}$ des coupures de $\mathbf{Q}$ au sens de Dedekind peut être muni d'une addition $+$ et d'une multiplication $\cdot$ compatible avec sa relation d'ordre $\leq$ de telle sorte que $(\mathcal{C}, +, \cdot)$ soit un corps commutatif archimédien complet.*

Ce nouvel ensemble $\mathcal{C}$ muni de sa structure de corps commutatif, archimédien et "complet" sera noté $\mathbf{R}$ et appelé le *corps des nombres réels.*

Chapitre 2

Dénombrements

Référence pour ce chapitre : le module II.1 du L1, section 2.2.

2.1 Les bases

2.1.1 Principes de récurrence

Rappelons que l'ensemble $\mathbf{N}$ des entiers naturels est muni d'une relation d'ordre notée $\leq$ qui possède la propriété fondamentale suivante :
Toute partie non vide de $\mathbf{N}$ *admet un plus petit élément* [1].

Cette propriété est d'ailleurs équivalente à la conjonction des deux suivantes :
- L'ensemble $\mathbf{N}$ est totalement ordonné.
- Toute suite décroissante d'entiers est stationnaire. (De manière équivalente : il n'existe pas de suite infinie strictement décroissante dans $\mathbf{N}$.)

Le principe de récurrence. On en déduit de cette propriété de $\mathbf{N}$ le *principe de récurrence*. Dans la pratique, on considère ce principe comme une méthode de démonstration. Celle-ci admet au moins trois formes distinctes, que nous allons expliciter et illustrer. Notre but est de démontrer une propriété $P(n)$ pour tout $n \in \mathbf{N}$. Une telle propriété, dont la véracité dépend d'une variable, est appelée *prédicat*.

La preuve par *récurrence simple* est celle-ci :
Soit $P(n)$ *un prédicat défini sur* $\mathbf{N}$ *et vérifiant les deux hypothèses suivantes :*
- *Initialisation :* $P(0)$ *est vraie.*
- *Hérédité :* $\forall n \in \mathbf{N}\ ,\ \big(P(n) \Rightarrow P(n+1)\big)$.

[1] On dit que cette relation d'ordre fait de $\mathbf{N}$ un ensemble "bien ordonné".

Alors P est vraie sur $\mathbf{N}$ tout entier : $\forall n \in \mathbf{N}\ ,\ P(n)$.
On peut d'ailleurs aussi bien appliquer ce principe à $\mathbf{N}^*$ (qui est bien ordonné), ou à $\mathbf{N} \setminus \{0,1\} = \{2,3,4,\ldots\}$, etc. Il faut alors respectivement initialiser en vérifiant que $P(1)$ est vraie, ou que $P(2)$ est vraie, etc.

Exemple.
Montrons que, pour tout $n \in \mathbf{N}$, on a $2^n > n$. Nous notons donc, pour tout $n \in \mathbf{N}$:

$$P(n) := (2^n > n).$$

Initialisation : la propriété $P(0)$ dit que $2^0 > 0$, *i.e.* que $1 > 0$, qui est vraie.
Hérédité : supposons $P(n)$ vraie, *i.e.* $2^n > n$ (hypothèse de récurrence). Alors :

$$2^{n+1} = 2^n + 2^n \geq 2^n + 1 > (n+1) + 1.$$

La dernière inégalité utilisait l'hypothèse de récurrence. On a bien prouvé $P(n+1)$.
Du principe de récurrence (simple), on déduit que $\forall n \in \mathbf{N}\ ,\ P(n)$.

La preuve par *récurrence forte* est également conséquence du fait que $\mathbf{N}$ est bien ordonné. Elle découle du principe suivant.
Soit $P(n)$ un prédicat défini sur $\mathbf{N}$ et vérifiant l'hypothèse suivante :
Hérédité forte :

$$\forall n \in \mathbf{N}\ ,\ \Big(\big(\forall m < n\ ,\ P(m)\big) \Rightarrow P(n)\Big).$$

Alors P est vraie sur $\mathbf{N}$ tout entier : $\forall n \in \mathbf{N}\ ,\ P(n)$.
On peut d'ailleurs aussi bien appliquer ce principe à $\mathbf{N}^*$ ou à $\mathbf{N} \setminus \{0,1\}$, etc.

Exemple.
Disons qu'un entier $n \in \mathbf{N} \setminus \{0,1\}$ est *irréductible* s'il n'est pas le produit de deux entiers $p, q \in \mathbf{N} \setminus \{0,1\}$. Nous allons montrer que tout entier de $\mathbf{N} \setminus \{0,1\}$ est produit d'entiers irréductibles.
Nous notons donc, pour tout $n \in \mathbf{N} \setminus \{0,1\}$:

$$P(n) := (n \text{ est produit d'entiers irréductibles}).$$

Soit $n \in \mathbf{N} \setminus \{0,1\}$ et supposons (hypothèse de récurrence forte) que tout entier $m \in \mathbf{N} \setminus \{0,1\}$ tel que $m < n$ vérifie $P(m)$, autrement dit, qu'il est produit d'irréductibles. Il s'agit d'en déduire que n est lui-même produit d'irréductibles (hérédité forte). On distingue deux cas :

1. Si n est irréductible, il est bien entendu produit d'irréductibles !
2. Sinon, il est réductible et l'on peut écrire $n = pq$ avec $p, q \in \mathbf{N} \setminus \{0,1\}$. Comme $p, q > 1$, on a $p, q < n$. On peut donc leur appliquer l'hypothèse de récurrence forte : $P(p)$ et $P(q)$ sont vraies, *i.e.* p et q sont produits d'irréductibles, donc $n = pq$ aussi.

On a bien démontré $P(n)$, donc l'hérédité forte. Du principe de récurrence forte on tire la conclusion. (Cette démonstration remonte aux Éléments d'Euclide.)

La preuve par *récurrence double*, ou *récurrence à deux pas* [2] repose sur le principe suivant :
Soit $P(n)$ un prédicat défini sur $\mathbf{N}$ et vérifiant les deux hypothèses suivantes :
- *Initialisation : $P(0)$ et $P(1)$ sont vraies.*
- *Hérédité : $\forall n \in \mathbf{N}$, $\Big(\big(P(n)$ et $P(n+1)\big) \Rightarrow P(n+2)\Big)$.*

Alors P est vraie sur $\mathbf{N}$ tout entier : $\forall n \in \mathbf{N}$, $P(n)$.
On peut d'ailleurs aussi bien appliquer ce principe à $\mathbf{N}^*$, ou à $\mathbf{N} \setminus \{0,1\}$, etc. Il faut alors respectivement initialiser en vérifiant que $P(1)$ et $P(2)$ sont vraies, ou que $P(2)$ et $P(3)$ sont vraies, etc.

Exemple.
Nous allons démontrer que $(1+\sqrt{2})^n + (1-\sqrt{2})^n \in \mathbf{Z}$ pour tout entier $n \in \mathbf{N}$. C'est vrai pour $n = 0$ et $n = 1$ (calcul facile). De plus :

$$(1+\sqrt{2})^{n+2} + (1-\sqrt{2})^{n+2} = 2\big((1+\sqrt{2})^{n+1} + (1-\sqrt{2})^{n+1}\big) + \big((1+\sqrt{2})^n + (1-\sqrt{2})^n\big),$$

ce que l'on peut écrire $u_{n+2} = 2u_{n+1} + u_n$, en posant $u_n := (1+\sqrt{2})^n + (1-\sqrt{2})^n$. Il est alors clair que ($u_n \in \mathbf{Z}$ et $u_{n+1} \in \mathbf{Z}$) $\Rightarrow u_{n+2} \in \mathbf{Z}$, et l'on a bien l'hérédité, donc la conclusion par récurrence à deux pas.

Exercice.
Vérifier que $(1+\sqrt{2})^n + (1-\sqrt{2})^n \in \mathbf{N}$.

L'hérédité dans cette démonstration, repose sur la relation (de récurrence à deux pas !) $u_{n+2} = 2u_{n+1} + u_n$. Notons qu'en posant $v_n := (1+\sqrt{2})^n - (1-\sqrt{2})^n$ on a la relation analogue : $v_{n+2} = 2v_{n+1} + v_n$, donc la même propriété d'hérédité pour l'assertion $v_n \in \mathbf{Z}$. De plus, cette dernière est vraie pour $n = 0$, mais fausse pour $n = 1$: l'initialisation en $n = 0$ est donc insuffisante dans une récurrence à deux pas.

Constructions par récurrence. On peut *définir* des objets par récurrence. Il y a, là encore, les récurrences simple, forte et à deux (ou k) pas. Nous allons illustrer chaque cas par un exemple.

Exemple.
On peut définir une suite numérique par récurrence simple ; par exemple la suite des *factorielles* :

$$0! := 1 \text{ et } \forall n \in \mathbf{N} \ , \ (n+1)! := (n+1)\, n!.$$

[2] Il existe aussi des récurrence à trois pas, et même à k pas, où $k \in \mathbf{N}^*$.

Ainsi, $1! = 1$, $2! = 2$, $3! = 6$, $4! = 24$, etc.

Exemple.
On peut définir une suite numérique par récurrence double ; par exemple, la suite de Fibonacci :

$$F_0 = 0,\ F_1 := 1 \text{ et } \forall n \in \mathbf{N}\ ,\ F_{n+2} := F_{n+1} + F_n.$$

Exemple.
On peut définir une suite numérique par récurrence forte ; par exemple :

$$\forall n \in \mathbf{N}\ ,\ u_n := 1 + \sum_{i=0}^{n-1} u_i.$$

Par convention, pour $n = 0$, la "somme vide" $\sum_{i=0}^{n-1} u_i$ vaut 0. On a donc $u_0 = 1$, $u_1 = 2$, $u_2 = 4$ et $u_3 = 8$; et ensuite ?

Exercice.
Démontrer, par récurrence sur n, que $u_n = 2^n$.

Exercice.
On pose $v_0 := 0$, $v_1 := 1$ et $v_{n+2} := -v_{n+1} - v_n$. Calculer le terme général.

2.1.2 Comparaison de cardinaux finis.

Nous reprenons d'abord des théorèmes généraux sur les cardinaux et les appliquons ensuite de manière amusante.

Théorème 2.1.1 *Soit $f : E \to F$ une application.*
(i) Si f est injective, card $E \leq$ card F.
(ii) On suppose que card $E =$ card F. Alors f injective si, et seulement si, elle est surjective. (Naturellement, elle est alors bijective.)

□

Corollaire 2.1.2 (Principe des tiroirs de Dirichlet) *Soit $f : E \to F$ une application. Si card $E >$ card F, il existe $a \neq b \in E$ tels que $f(a) = f(b)$.*

Exemples.
Dans un groupe de 27 personnes, il y en a certainement deux dont le nom commence par la même lettre.

Le nombre de cheveux normal d'une personne est de l'ordre de 100000 à 150000. Admettons qu'il soit toujours inférieur à 200000. Il y a donc à Toulouse deux personnes qui ont le même nombre de cheveux.

Exercice.
Dans un dé "polyédrique" (nombre quelconque de faces ayant chacune un nombre quelconque de côtés), il y a deux faces qui ont le même nombre de côtés.

2.1.3 Avec l'addition

Nous prendrons comme point de départ la propriété suivante :
Si A et B sont des ensembles finis disjoints, card $(A \cup B) =$ card $A +$ card B.

Théorème 2.1.3 *Si A et B sont des ensembles finis quelconques :*

$$\textit{card}\ (A \cup B) = \textit{card}\ A + \textit{card}\ B - \textit{card}\ (A \cap B).$$

Démonstration. On a d'abord, par application de la propriété de départ à la réunion disjointe $A = (A \cap B) \cup (A \setminus B)$:

$$\text{card } A = \text{card } (A \cap B) + \text{card } (A \setminus B) \Longrightarrow \text{card } A - \text{card } (A \cap B) = \text{card } (A \setminus B).$$

On remarque ensuite que $(A \cup B)$ est l'union disjointe de B et de $(A \setminus B)$, auxquels on applique à nouveau la propriété de départ :

$$\text{card } (A \cup B) = \text{card } B + \text{card } (A \setminus B) = \text{card } A + \text{card } B - \text{card } (A \cap B).$$

□

Pour comprendre ce qui va suivre, essayons le cas de trois ensembles finis A, B, C :

$$\text{card } (A \cup B \cup C) = \text{card } \big((A \cup B) \cup C\big) = \text{card } (A \cup B) + \text{card } (C) - \text{card } \big((A \cup B) \cap C\big).$$

On calcule donc card $(A \cup B) =$ card $A +$ card $B -$ card $(A \cap B)$ et :

$$\begin{aligned} \text{card } \big((A \cup B) \cap C\big) &= \text{card } \big((A \cap C) \cup (B \cap C)\big) \\ &= \text{card } (A \cap C) + \text{card } (B \cap C) - \text{card } \big((A \cap C) \cap (B \cap C)\big) \\ &= \text{card } (A \cap C) + \text{card } (B \cap C) - \text{card } (A \cap B \cap C). \end{aligned}$$

En reportant dans la première égalité, on trouve enfin :

$$\text{card } (A \cup B \cup C) = \text{card } A + \text{card } B + \text{card } C - \text{card } (A \cap B) - \text{card } (A \cap C) - \text{card } (B \cap C) + \text{card } (A \cap B \cap C).$$

Théorème 2.1.4 (Formule d'inclusion-exclusion ou formule du crible) *Soient $A_1, \ldots, A_n$ des ensembles finis quelconques. Alors :*

$$\begin{aligned} card\ (A_1 \cup \cdots \cup A_n) &= \sum_{i=1}^{n} card\ A_i - \sum_{1\le i<j\le n} card\ (A_i \cap A_j) \\ &+ \sum_{1\le i<j<k\le n} card\ (A_i \cap A_j \cap A_k) \\ &- \sum_{1\le i<j<k<\ell\le n} card\ (A_i \cap A_j \cap A_k \cap A_\ell) + \cdots \\ &+ (-1)^{n-1} card\ (A_1 \cap \cdots \cap A_n) \\ &= \sum_{k=1}^{n} (-1)^{k-1} \sum_{1\le i_1<\cdots<i_k\le n} card\ (A_{i_1} \cap \cdots \cap A_{i_k}). \end{aligned}$$

Démonstration. Par récurrence sur n ; réservé aux courageux ! □

Exemple.
Anticipant sur le cours d'arithmétique, nous allons calculer le nombre d'entiers dans $[\![1, 900]\!]$ ayant un facteur commun avec 900. Ces entiers sont nécessairement divisibles par l'un des facteurs premiers de 900, lesquels sont 2, 3 et 5. On pose donc :

$$A := \{n \in [\![1, 900]\!] \mid 2|n\}, \quad B := \{n \in [\![1, 900]\!] \mid 3|n\} \text{ et } C := \{n \in [\![1, 900]\!] \mid 5|n\}.$$

Les éléments de A sont les $2k$ tels que $1 \le k \le 900/2$, il y en a donc 450 ; avec le même raisonnement pour B et C, on trouve :

$$\text{card } A = 450, \quad \text{card } B = 300 \text{ et card } C = 180.$$

Les éléments de $A \cap B$ sont les $6k$ tels que $1 \le k \le 900/6$, il y en a donc 150 ; avec le même raisonnement pour $A \cap C$ et $B \cap C$, on trouve :

$$\text{card } (A \cap B) = 150, \quad \text{card } (A \cap C) = 90 \text{ et card } (B \cap C) = 60.$$

Enfin, les éléments de $A \cap B \cap C$ sont les $30k$ tels que $1 \le k \le 900/30$, il y en a donc 30. Finalement, le nombre cherché est :

$$\begin{aligned} \text{card } (A \cup B \cup C) &= \text{card } A + \text{card } B + \text{card } C \\ &- \text{card } (A \cap B) - \text{card } (A \cap C) - \text{card } (B \cap C) \\ &+ \text{card } (A \cap B \cap C) \\ &= 450 + 300 + 180 - 150 - 90 - 60 + 30 = 660. \end{aligned}$$

Exercice.
Combien d'entiers de $[\![100, 999]\!]$ ont au moins un chiffre 7 en écriture décimale ?

2.1.4 Avec la multiplication

Nous prendrons comme point de départ la propriété suivante :
Si A et B sont des ensembles finis quelconques, card $(A \times B) =$ card $A \times$ card B.

Théorème 2.1.5 (Principe des bergers) *Soit $f : E \to F$ une application. On suppose que toutes les images réciproques $f^{-1}(\{y\})$, $y \in F$, ont le même nombre d'éléments q. Alors card $E = q$ card F.*

Démonstration. Fixons un ensemble G à q éléments (par exemple $[\![1, q]\!]$). Pour tout $y \in F$, soit ϕ_y une bijection de G sur $f^{-1}(\{y\})$. L'application $(y, i) \mapsto \phi_y(i)$ est alors une bijection de $F \times G$ sur E. □

Exemple.
Pour compter des moutons, il suffit de compter les pattes et de diviser par 4. (Des applications plus significatives suivront !)

Puissances. Fixons $a \in \mathbf{N}$. On définit a^n par récurrence sur n : $a^0 = 1$ et, pour tout $n \in \mathbf{N}$, $a^{n+1} := a.a^n$. On démontre (par récurrence !) les formules classiques : $a^{m+n} = a^m.a^n$, $(ab)^m = a^m b^m$ et $(a^m)^n = a^{mn}$.

Exercice.
Interpréter ces trois formules à l'aide de bijections.

Théorème 2.1.6 *Soit E un ensemble fini. On a : card $\mathcal{P}(E) = 2^{\text{card } E}$.*

Démonstration. Elle se fait par récurrence sur $n :=$ card E. Pour $n = 0$, on a card $\mathcal{P}(\emptyset) =$ card $\{\emptyset\} = 1 = 2^0$, comme escompté.
Supposons la propriété vérifiée pour un ensemble à n éléments et considérons E tel que card $E = n + 1$. Soient $x \in E$ et $E' := E \setminus \{x\}$, d'où card $E' = n$. par hypothèse de récurrence, card $\mathcal{P}(E') = 2^n$. Considérons maintenant l'application $F \mapsto F \cap E'$ de $\mathcal{P}(E)$ dans $\mathcal{P}(E')$. Pour tout $F' \in \mathcal{P}(E')$, l'image réciproque de F' dans $\mathcal{P}(E)$ a exactement 2 éléments : F' et $F' \cup \{x\}$. D'après le principe des bergers, card $\mathcal{P}(E) = 2$ card $\mathcal{P}(E') = 2.2^n = 2^{n+1}$ (c'est la définition des puissances), ce qui achève la récurrence. □

Rappelons que $\mathcal{F}(E, F)$ désigne l'ensemble des applications de E dans F. On le note également F^E, ce qui se peut se justifier par la formule card $\mathcal{F}(E, F) = (\text{card } F)^{\text{card } E}$, que nous allons maintenant démontrer.

Théorème 2.1.7 *Soient E et F des ensembles finis. On a : card $\mathcal{F}(E, F) = (\text{card } F)^{\text{card } E}$.*

Démonstration. Elle se fait par récurrence sur $n := \text{card } E$. Nous noterons $q := \text{card } F$. Pour $n = 0$, il faut admettre que card $\mathcal{F}(\emptyset, F) = 1$. Si l'on trouve cette affirmation trop étrange (elle est pourtant rigoureusement exacte), on n'a qu'à l'admettre comme une pure convention et entamer la récurrence avec $n = 1$. Dans ce cas, E est un singleton : $E = \{x\}$ et on vérifie sans peine que l'application $f \mapsto f(x)$ de $\mathcal{F}(\{x\}, F)$ sur F est une bijection.
Supposons l'affirmation vraie pour card $E = n$ et prouvons la pour card $E = n + 1$. On écrit $E = E' \cup \{x\}$, où card $E' = n$ et où $x \notin E'$. L'hypothèse de récurrence nous dit que card $\mathcal{F}(E', F) = q^n$. Nous allons prouver, que card $\mathcal{F}(E, F) = q \,\text{card}\, \mathcal{F}(E', F)$. Considérons en effet l'application de restriction $f \mapsto f_{|F'}$ de $\mathcal{F}(E, F)$ dans $\mathcal{F}(E', F)$. L'image réciproque de $g \in \mathcal{F}(E', F)$ est formée des $f \in \mathcal{F}(E, F)$ qui prennent sur F' les mêmes valeurs que g et qui prennent en x une valeur arbitraire dans F. Il y a donc q telles applications f et le principe des bergers nous donne la conclusion. On a donc : card $\mathcal{F}(E, F) = q.q^n = q^{n+1}$, vue la définition par récurrence des puissances, ce qui achève la démonstration. □

Fonctions caractéristiques. Les ensembles $\mathcal{F}(E, \{0, 1\})$ et $\mathcal{P}(E)$ ont tous deux $2^{\text{card } E}$ éléments. On va construire une bijection explicite de l'un sur l'autre. On fixe un ensemble E. À tout sous-ensemble $F \subset E$, on associe sa *fonction caractéristique* χ_F : c'est l'application de E dans $\{0, 1\}$ définie par :

$$\forall x \in E \ , \ \chi_F(x) := \begin{cases} 1 \text{ si } x \in F, \\ 0 \text{ si } x \notin F. \end{cases}$$

Théorème 2.1.8 *L'application $F \mapsto \chi_F$ est une bijection de $\mathcal{P}(E)$ sur $\mathcal{F}(E, \{0, 1\})$.*

Démonstration. Soit $\phi : E \to \{0, 1\}$ une application quelconque. On définit son *support* $\text{Supp}(\phi) := \phi^{-1}(1) = \{x \in E \mid x = 1\}$, qui est une partie de E. On a l'équivalence :

$$\phi = \chi_F \Longleftrightarrow F = \text{Supp}(\phi).$$

Les applications $F \mapsto \chi_F$ et $\phi \mapsto \text{Supp}(\phi)$ sont donc réciproques l'une de l'autre. □

Exercice.
Combien vaut 0^n ?

Exercice.
Soit $E \subset \mathbf{C}^*$ un ensemble à n éléments et soit $p \in \mathbf{N}^*$. Combien y a-t'il de complexes tels que $z^p \in E$?

2.2 Analyse combinatoire

2.2.1 Arrangements, permutations

Arrangements. Soient E et F deux ensembles finis ayant respectivement m et n éléments. Nous noterons $I(E,F)$ l'ensemble des applications injectives de E dans F. Si $m > n$, il n'y en a aucune et $I(E,F) = \emptyset$. Nous allons calculer card $I(E,F)$ lorsque $m \leq n$. Remarquons d'abord que, si card E = card E' et card F = card F', alors card $I(E,F)$ = card $I(E',F')$. (Argument : une bijection entre E et E' et une bijection entre F et F' donnent lieu à une bijection entre $I(E,F)$ et $I(E',F')$.) Le nombre recherché ne dépend donc que de m et de n. On le note A_n^m. (Donc $A_n^m = 0$ lorsque $m > n$.) Pour la même raison, on peut aussi bien supposer que $E = [\![1,m]\!]$. Dans ce cas, se donner une application injective f de E dans F revient à se donner une suite $(y_1,\ldots,y_m)$ de m éléments distincts de F : on pose $y_i := f(i)$. Une telle suite est appellée *arrangement de m objets pris parmi n.*

Lemme 2.2.1 *Si $0 \leq m \leq n-1$, on a : $A_n^{m+1} = (n-m)A_n^m$.*

Démonstration. À toute suite $(y_1,\ldots,y_{m+1})$ de $(m+1)$ éléments distincts de F, associons la suite $(y_1,\ldots,y_m)$ de m éléments distincts de F. On obtient ainsi une application ϕ de $I([\![1,m+1]\!],F)$ dans $I([\![1,m]\!],F)$. L'image réciproque de $(y_1,\ldots,y_m)$ par ϕ est formée de toutes les suites $(y_1,\ldots,y_m,y)$ telles que $y \in F \setminus \{y_1,\ldots,y_m\}$: cette image réciproque a donc $(n-m)$ éléments. D'après le principe des bergers, card $I([\![1,m+1]\!],F) = (n-m)$ card $I([\![1,m]\!],F)$. □

Théorème 2.2.2 *Si $m \leq n$, on a $A_n^m = \dfrac{n!}{(n-m)!} = \prod_{i=0}^{m-1}(n-i)$.*

Démonstration. Elle se fait par récurrence sur m. Pour $m = 0$, l'unique application de $\emptyset$ dans F est injective et l'on trouve $A_n^0 = 1 = \dfrac{n!}{n!}$, ce qui est correct. Si l'on trouve l'argument trop bizarre, on admet cette valeur comme une convention et l'on initialise la récurrence à $m := 1$. Dans ce cas, E est un singleton et les n applications de E dans F sont injectives : on a bien $A_n^1 = \dfrac{n!}{(n-1)!} = n$. On peut également dire que les arrangements de 1 objet pris parmi n sont ici les n suites (y) de 1 élément de F.
Supposons maintenant que $A_n^m = \dfrac{n!}{(n-m)!}\cdot$ pour un certain $m \in [\![0,n-1]\!]$. En combinant le lemme et l'hypothèse de récurrence, on trouve :

$$A_n^{m+1} = (n-m)A_n^m = (n-m)\frac{n!}{(n-m)!} = \frac{n!}{\big(n-(m+1)\big)!},$$

d'où la première égalité. L'égalité $\dfrac{n!}{(n-m)!} = \prod_{i=0}^{m-1}(n-i)$ est immédiate. □

Permutations. Lorsque $m = n$, toute application injective de E dans F est bijective. Le nombre A_n^n de ces bijections est égal au nombre des suites finies $(y_1, \ldots, y_n)$ formées des n éléments de F, chacun étant (bien entendu) présent une fois et une seule. Une telle suite est appelée *permutation* de F. Une définition essentiellement équivalente est celle-ci : une permutation de F est une bijection de F dans lui-même.

Théorème 2.2.3 *Le nombre de permutations d'un ensemble à n éléments est $n!$.*

Démonstration. C'est $A_n^n = \dfrac{n!}{(n-n)!} = \dfrac{n!}{0!} = n!$. □

Un peu de dérangements. Soit $f : F \to F$ une application bijective (donc une permutation). On dit que c'est un *dérangement* si : $\forall y \in F\ ,\ f(y) \neq y$. De manière équivalente, la suite $(y_1, \ldots, y_n)$ de n éléments distincts de $\{1, \ldots, n\}$ est un dérangement si $\forall i \in [\![1, n]\!]\ ,\ y_i \neq i$. Nous allons calculer le nombre d_n de dérangements de F. Pour cela, nous prendrons $F := \{1, \ldots, n\}$. Nous noterons S_n l'ensemble de toutes les permutations de F et D_n l'ensemble de tous les dérangements de F. Pour tout $i \in F$, nous noterons $\mathcal{F}_i$ l'ensemble des bijections $f : F \to F$ telles que $f(i) = i$. L'ensemble des dérangements est donc égal à : $D_n = S_n \setminus \bigcup_{i=1}^n \mathcal{F}_i$, de sorte que : $d_n = n! - \text{card } \bigcup_{i=1}^n \mathcal{F}_i$. On applique la formule du crible :

$$\text{card } \bigcup_{i=1}^{n} \mathcal{F}_i = \sum_{k=1}^{n} (-1)^{k-1} \sum_{1 \leq i_1 < \cdots < i_k \leq n} \text{card } (\mathcal{F}_{i_1} \cap \cdots \cap \mathcal{F}_{i_k}).$$

Mais $\mathcal{F}_{i_1} \cap \cdots \cap \mathcal{F}_{i_k}$ est formé des permutations telles que $f(i_1) = i_1, \ldots, f(i_k) = i_k$. Leur nombre est celui des permutations de $F \setminus \{i_1, \ldots, i_k\}$, c'est-à-dire $(n-k)!$. Par ailleurs, le nombre des k-uplets $(i_1, \ldots, i_k)$ tels que $1 \leq i_1 < \cdots < i_k \leq n$ est noté $\binom{n}{k}$. Nous montrerons plus loin que $\binom{n}{k} = \dfrac{n!}{k!(n-k)!}$. Il en découle :

$$\text{card } \bigcup_{i=1}^{n} \mathcal{F}_i = \sum_{k=1}^{n} (-1)^{k-1} \binom{n}{k} (n-k)! = \sum_{k=1}^{n} (-1)^{k-1} \frac{n!}{k!}.$$

Finalement :

$$d_n = n! - \sum_{k=1}^{n} (-1)^{k-1} \frac{n!}{k!} = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}.$$

On verra en cours d'analyse (une autre année !) que $\lim_{n \to +\infty} \sum_{k=0}^{n} \dfrac{(-1)^k}{k!} = \dfrac{1}{e}$. Donc $d_n \sim \dfrac{n!}{e}$.

Exercice.
Décrire tous les arrangements de 1, 2, 3 objets pris parmi les 4 éléments $\{1, 2, 3, 4\}$.

Exercice.
Décrire toutes les permutations de $F := \{1, 2, 3\}$ de deux manières (suites d'éléments de F ou bijections de F dans lui-même).

2.2.2 Combinaisons

Soit E un ensemble à n éléments. Lorsque $0 \leq m \leq n$, on appelle *combinaison de m objets pris parmi les n éléments de E* un sous-ensemble $\{y_1, \ldots, y_m\}$ formé de m éléments distincts de E : ce n'est donc rien d'autre qu'un sous-ensemble à m éléments de n. La différence entre une combinaison et un arrangement, c'est que l'ordre importe dans un arrangement mais pas dans une combinaison. Le nombre de ces combinaisons ne dépend évidemment que de m et de n. On le note traditionnellement C_n^m et, de manière plus moderne (influencée par l'univers anglo-saxon !) $\binom{n}{m}$, ce qui se lit : "choix de m parmi n". Les $C_n^m = \binom{n}{m}$ sont appelés *coefficients binomiaux* pour des raisons qui apparaitront à la section 2.2.4. On convient que $\binom{n}{m} = 0$ lorsque $m > n$. (Pourquoi ?)

Théorème 2.2.4 *Lorsque $0 \leq m \leq n$, le nombre de combinaisons de m objets pris parmi n est donné par la formule :*

$$C_n^m = \binom{n}{m} = \frac{n!}{m!\,(n-m)!}\cdot$$

Démonstration. À chaque arrangement $(y_1, \ldots, y_m)$ dans E, associons l'ensemble $\{y_1, \ldots, y_m\}$ sous-jacent, obtenu en oubliant l'ordre. Les arrangements ayant pour image une combinaison $\{y_1, \ldots, y_m\}$ donnée sont les $m!$ permutations de $(y_1, \ldots, y_m)$. D'après le principe des bergers, on a donc $A_n^m = m!\,C_n^m$, d'où la conclusion. □

Corollaire 2.2.5 *Le nombre d'applications strictement croissantes de $[\![1, m]\!]$ dans $[\![1, n]\!]$ est $\binom{n}{m}$.*

Démonstration. Une application strictement croissante f de $[\![1, m]\!]$ dans $[\![1, n]\!]$ est totalement déterminée par son image $\{y_1, \ldots, y_m\} \subset [\![1, n]\!]$: le plus petit élément est $f(1)$, le suivant est $f(2)$, etc.

Corollaire 2.2.6 *Pour $0 \leq m \leq n$, on a les formules :*

$$\binom{n}{m} = \binom{n}{n-m} \text{ et } \sum_{m=0}^{n} \binom{n}{m} = 2^n.$$

Démonstration. La première formule est immédiate par calcul sur l'expression $\binom{n}{m} = \frac{n!}{m!\,(n-m)!}\cdot$ On peut également la justifier en remarquant que, si card $E = n$, l'application $F \mapsto \complement_E F$ (passage au complémentaire) est une bijection de l'ensemble des parties à m éléments sur l'ensemble des parties à $(n-m)$ éléments.
La deuxième formule vient de ce que E a au total 2^n parties, dont $\binom{n}{0}$ à 0 éléments, $\binom{n}{1}$ à 1 élément, $\binom{n}{2}$ à 2 éléments, etc. □

Exemple.
Donnons une démonstration combinatoire de la formule :

$$\sum_{p=0}^{q} \binom{m}{p}\binom{n}{q-p} = \binom{m+n}{q}.$$

Soient E et F deux ensembles disjoints ayant respectivement m et n éléments. L'ensemble $E \cup F$ a $(m+n)$ éléments, donc $\binom{m+n}{q}$ sous-ensembles à q éléments. Chacun de ces sous-ensemble est de la forme $E' \cup F'$, où $E' \subset E$ a p éléments (pour un p tel que $0 \leq p \leq q$) et où $F' \subset F$ a $(q-p)$ éléments. Pour chaque p, il y a $\binom{m}{p}\binom{n}{q-p}$ tels ensembles $E' \cup F'$, et leur nombre total est bien $\sum_{p=0}^{q} \binom{m}{p}\binom{n}{q-p}$. Une autre preuve, de nature algébrique, sera proposée en exercice à la section 2.2.4.

Un peu de surjections. Notons $n := \text{card } E$ et $p := \text{card } F$. Nous allons compter le nombre $S(n,p)$ d'applications surjectives de E dans F. Naturellement, on peut tout aussi bien supposer que $F = [\![1,p]\!]$, ce que nous ferons. Pour tout $i \in F$, soit $\mathcal{F}_i := \{f \in \mathcal{F}(E,F) \mid i \notin \text{Im}f\}$. Par définition, l'ensemble des surjections est égal à $\mathcal{F}(E,F) \setminus \bigcup_{i\in F} \mathcal{F}_i$, de sorte que $S(n,p) = p^n - \text{card} \bigcup_{i\in F} \mathcal{F}_i$. Nous allons calculer le cardinal de $\bigcup_{i\in F} \mathcal{F}_i$ à l'aide de la formule du crible :

$$\text{card} \bigcup_{i\in F} \mathcal{F}_i = \text{card} \bigcup_{i=1}^{p} \mathcal{F}_i = \sum_{k=1}^{p} (-1)^{k-1} \sum_{1\leq i_1<\cdots<i_k\leq p} \text{card}\,(\mathcal{F}_{i_1} \cap \cdots \cap \mathcal{F}_{i_k}).$$

L'ensemble $\mathcal{F}_{i_1} \cap \cdots \cap \mathcal{F}_{i_k}$ est formé des applications $f : E \to F$ telles que $i_1, \ldots, i_k \notin \text{Im}f$, autrement dit, des applications de E dans $F \setminus \{i_1, \ldots, i_k\}$. Comme ce dernier ensemble a $p-k$ éléments, on déduit du théorème : $\text{card}\,(\mathcal{F}_{i_1} \cap \cdots \cap \mathcal{F}_{i_k}) = (p-k)^n$. Anticipant sur la section 2.2 et notant $\binom{p}{k}$ le nombre de parties à k éléments $\{i_1, \ldots, i_k\} \subset F$:

$$S(n,p) = p^n - \sum_{k=1}^{p} (-1)^{k-1} \binom{p}{k} (p-k)^n = \sum_{k=0}^{p} (-1)^k \binom{p}{k} (p-k)^n.$$

Exercice.
Décrire toutes les combinaisons de 1, 2, 3 objets pris parmi les 4 éléments $\{1,2,3,4\}$.

Exercice.
Combien de poignées de main échangent n personnes qui se rencontrent ?

Exercice.
Calculer le nombre d'applications croissantes de $[\![1,m]\!]$ dans $[\![1,n]\!]$. (Remarquer que $k \mapsto f(k)$ est croissante si, et seulement si, $k \mapsto f(k)+k-1$ est strictement croissante.) En déduire le nombre de solutions entières de l'équation : $x_1 + \cdots + x_n = p$. Vérifier la formule obtenue pour $p = 1, 2, 3$. (Remarquer que, pour toute solution $(x_1, \ldots, x_p)$, l'application $k \mapsto \sum_{i=1}^{k} x_i$ est croissante de $[\![1,p]\!]$ dans $[\![1,n]\!]$.)

2.2.3 Étude des coefficients binomiaux

Théorème 2.2.7 (Formule de Pascal) *Pour tous $m, n \in \mathbf{N}$ on a :*

$$\binom{n+1}{m+1} = \binom{n}{m+1} + \binom{n}{m}.$$

Démonstration. Si $m > n$, les deux membres de l'égalité sont nuls. Si $m = n$, $\binom{n+1}{m+1} = \binom{n}{m} = 1$ et $\binom{n}{m+1} = 0$, et les deux membres de l'égalité sont égaux à 1. On peut donc supposer que $0 \leq m < n$. Nous disposons dans ce cas de deux preuves tout à fait différentes. La preuve calculatoire vient immédiatement à l'esprit :

$$\begin{aligned}
\binom{n}{m+1} + \binom{n}{m} &= \frac{n!}{(m+1)!\,\big(n-(m+1)\big)!} + \frac{n!}{m!\,(n-m)!} \\
&= (n-m)\frac{n!}{(m+1)!\,(n-m)!} + (m+1)\frac{n!}{(m+1)!\,(n-m)!} \\
&= (n+1)\frac{n!}{(m+1)!\,(n-m)!} \\
&= \frac{(n+1)!}{(m+1)!\,(n-m)!} \\
&= \binom{n+1}{m+1}.
\end{aligned}$$

La preuve combinatoire revient à montrer que les deux nombres comptent la même chose. Considérons un ensemble E à n éléments soit $E' := E \cup \{x\}$ avec $x \notin E$. Donc E' a $(n+1)$ éléments. L'entier $\binom{n+1}{m+1}$ est le nombre de parties de E' qui ont $(m+1)$ éléments. Il y en a de deux types :

1. Les parties à $(m+1)$ éléments de E : il y en a $\binom{n}{m+1}$.
2. Les $F \cup \{x\}$, où F est une partie à m éléments de E : il y en a $\binom{n}{m}$.

Au total, on a bien $\left(\binom{n}{m+1} + \binom{n}{m}\right)$ parties à $(m+1)$ éléments de E'. □

On peut calculer les coefficients binomiaux à l'aide du *triangle de Pascal* :

```
                    1
                1       1
            1       2       1
        1       3       3       1
    1       4       6       4       1
1       5       10      10      5       1
```

La règle de formation est la suivante : les côtés du triangle sont formés de 1 ; chaque coefficient du tableau est la somme de ceux qui lui sont supérieurs juste à gauche et juste à droite. Sur la n^{e} ligne on trouve alors de gauche à droite les $\binom{n}{m}$ pour $m = 0, 1, \ldots, n$.

La formule de Pascal permet également un calcul "récursif" des coefficients binomiaux par l'algorithme suivant :

```
Pasc(n,p)
si p = 0 alors rendre 1 sinon si n = 0 alors rendre 0
sinon rendre Pasc(n-1,p) + Pasc(n-1,p-1) ;;
```

Le lecteur intéressé pourra rechercher la "complexité" de cet algorithme ; par exemple, combien d'additions requiert-il ? Et dans quel mesure les calculs sont-ils redondants ?

Une application de la formule de Pascal On écrit la formule de Pascal sous la forme $\binom{k+1}{m+1} - \binom{k}{m+1} = \binom{k}{m}$ et l'on additionne ces égalités pour $k = 0, \ldots, n$. Par élescopages (simplifications des soustractions), on trouve :

$$\binom{m}{m} + \cdots + \binom{n}{m} = \sum_{k=m}^{n} \binom{k}{m} = \binom{n+1}{m+1}.$$

Par exemple, pour $m = 1$, cela donne : $1 + \cdots + n = \binom{n+1}{2} = \dfrac{n(n+1)}{2}$. Pour $m = 2$:

$$\sum_{k=2}^{n} \frac{k(k-1)}{2} = \frac{(n-1)n(n+1)}{6}.$$

Comme le terme $\dfrac{k(k-1)}{2}$ est nul pour $k = 1$, en combinant avec le calcul précédent :

$$\sum_{k=1}^{n} k^2 = 2\sum_{k=1}^{n} \frac{k(k-1)}{2} + \sum_{k=1}^{n} k = \frac{(n-1)n(n+1)}{3} + \frac{n(n+1)}{2} = \frac{n(n+1)(2n+1)}{6}.$$

Variations des coefficients binomiaux. Soient m, n tels que $0 \leq m \leq n-1$. De la formule :

$$\frac{\binom{n}{m+1}}{\binom{n}{m}} = \frac{n-m}{m+1},$$

on déduit que $\binom{n}{m+1} > \binom{n}{m}$ si, et seulement si, $2m \leq n$. On en tire les variations de la suite des $\binom{n}{m}$ à n fixé : si n est pair, cette suite croit strictement de 0 à $n/2$ (où elle prend sa valeur maximum) puis décroit strictement de $n/2$ à n ; si n est impair, cette suite croit strictement de 0 à $(n-1)/2$, prend la même valeur (son maximum) en $(n-1)/2$ et $(n+1)/2$, puis décroit strictement de $(n+1)/2$ à n.

Exercice.
Démontrer par récurrence la formule : $\sum_{n=p}^{q} \binom{n}{p} = \binom{q+1}{p+1}$, puis l'expliciter pour $p = 0, 1, 2$.

Exercice.
Calculer $\sum_{n=1}^{q} n^3$.

2.2.4 La formule du binôme de Newton

Théorème 2.2.8 (Formule du binôme de Newton) *Soient a et b deux nombres complexes. On a alors, pour tout $n \in \mathbf{N}$:*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

Démonstration. Elle se fait par récurrence sur n. Pour $n = 0$, il s'agit de vérifier que $(a+b)^0 = \sum_{k=0}^{0} \binom{0}{k} a^k b^{0-k}$, autrement dit, que $1 = \binom{0}{0} a^0 b^0$, ce qui est bien vrai. Supposons la formule vraie au rang n. On calcule alors :

$$\begin{aligned}
(a+b)^{n+1} &= (a+b)(a+b)^n \\
&= (a+b) \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} \\
&= \sum_{k=0}^{n} \binom{n}{k} a^{k+1} b^{n-k} + \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k+1} \\
&= \sum_{j=1}^{n+1} \binom{n}{j-1} a^j b^{n-j+1} + \sum_{k=0}^{n+1} \binom{n}{k} a^k b^{n-k+1} \\
&= \sum_{j=1}^{n+1} \left(\binom{n}{j-1} + \binom{n}{j} \right) a^j b^{n-j+1} + b^{n+1} \\
&= \sum_{j=1}^{n+1} \binom{n+1}{j} a^j b^{n-j+1} + \binom{n}{0} a^0 b^{n-0+1} \\
&= \sum_{j=0}^{n+1} \binom{n+1}{j} a^j b^{n+1-j}.
\end{aligned}$$

□

Un peu d'algèbre combinatoire. Si l'on développe $(a+b)^n = (a+b)\cdots(a+b)$ (n facteurs), on voit apparaitre des termes de la forme $a^k b^{n-k}$. Chacun de ces termes apparait autant de fois qu'il y a de choix des k facteurs $(a+b)$ dans lesquels on prend a plutôt que b, donc, au total $\binom{n}{k}$ fois : c'est une autre preuve de la formule de Newton. Notons que les seules propriétés utilisées sont la commutativité et l'associativité de l'addition et de la multiplication, ainsi que la distributivité.

Exercice.
Calculer le terme en x^q dans $(1+x)^m(1+x)^n = (1+x)^{m+n}$, et en déduire l'égalité :

$$\sum_{p=0}^{q} \binom{m}{p} \binom{n}{q-p} = \binom{m+n}{q}.$$

Appendice : petit lexique de théorie des ensembles

Les lettres minuscules $x, y, z, \ldots$ désignent des "éléments". Les lettres majuscules $E, F, G, \ldots$ désignent des ensembles. Les lettres minuscules $f, g, h, \ldots$ désignent des applications.

$x \in E$ signifie : l'élément x *appartient* à l'ensemble E.
$x \notin E$ signifie : l'élément x *n'appartient pas* à l'ensemble E.
$F \subset E$ signifie : l'ensemble F *est* inclus dans l'ensemble E ; on dit alors que c'est une *partie* de E, ou un *sous-ensemble* de E :

$$\Big(F \subset E\Big) \Longleftrightarrow \Big(\forall x \ , \ (x \in F) \Rightarrow (x \in E)\Big).$$

$\emptyset$ désigne *l'ensemble vide*, qui n'a aucun élément.
$E \cup F$ désigne la *réunion* de E et F :

$$x \in E \cup F \Longleftrightarrow x \in E \text{ ou } x \in F.$$

$E \cap F$ désigne l'*intersection* de E et F :

$$x \in E \cap F \Longleftrightarrow x \in E \text{ et } x \in F.$$

$E \setminus F$ désigne la *différence* de E et F :

$$x \in E \cup F \Longleftrightarrow x \in E \text{ et } x \notin F.$$

$E \times F$ désigne le *produit cartésien* de E et F, *i.e.* l'ensemble des *couples* (x, y) tels que $x \in E$ et $y \in F$.
$\mathcal{P}(E)$ désigne l'*ensemble des parties* de E :

$$F \in \mathcal{P}(E) \Longleftrightarrow F \subset E.$$

Une *application* $f : E \to F$ associe à tout $x \in E$ un élément (unique) $y = f(x) \in F$. On dit que y est *l'image* de x (par f) et que x est *un antécédent* de y (par f).
f est *injective* si tout $y \in F$ admet au plus un antécédent :

$$\forall x, x' \in E \ , \ f(x) = f(x') \Rightarrow x = x'.$$

f est *surjective* si tout $y \in F$ admet au moins un antécédent :

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

f est *bijective* si elle est injective et surjective, autrement dit, si tout $y \in F$ admet exactement un antécédent :

$$\forall y \in F \ , \ \exists! x \in E \ : \ y = f(x).$$

L'*image* par $f : E \to F$ de $E' \subset E$ est :

$$f(E') := \{f(x) \mid x \in E'\} \subset F.$$

L'*image réciproque* par $f : E \to F$ de $F' \subset F$ est :

$$f^{-1}(F') := \{x \in E \mid f(x) \in F'\} \subset E.$$

Chapitre 3

Arithmétique

3.1 Arithmétique dans N

3.1.1 Ensemble des entiers naturels

On peut construire l'ensemble $\mathbf{N}$ des entiers naturels dans le cadre de la théorie des ensembles. Nous ne le ferons pas ici, et procéderons de manière axiomatique. Nous admettrons qu'il existe un ensemble infini $\mathbf{N} := \{0, 1, 2, ...\}$, dont les éléments sont appelés *entiers naturels*, et doté des structures et des propriétés suivantes.

1. L'ensemble $\mathbf{N}$ est muni d'une relation d'ordre total, notée $\leq$, telle que toute partie non vide de $\mathbf{N}$ admet un plus petit élément : on dit que $\mathbf{N}$ est bien ordonné. On en déduit en particulier le principe de récurrence, énoncé au début du chapitre 2.
2. L'ensemble $\mathbf{N}$ est muni de deux lois de composition $+$ (addition) et $\times$ (multiplication). Ces lois sont associatives et commutatives, et la multiplication est distributive par rapport à l'addition. (Revoir le vocabulaire concernant ces propriétés dans la partie du chapitre 1 consacrée aux nombres réels.) Chacune admet un élément neutre (respectivement 0 et 1).
3. Bien que $\mathbf{N}$ ne soit ni un groupe, ni, *a fortiori*, un corps, on a les propriétés de *régularité* suivantes : $\forall a, b, c \in \mathbf{N}$, $a + b = a + c \Longrightarrow b = c$; $\forall a \in \mathbf{N}^*, \forall b, c \in \mathbf{N}$, $ab = ac \Longrightarrow b = c$; et $\forall a, b \in \mathbf{N}$, $ab = 0 \Longrightarrow (a = 0$ ou $b = 0)$.
4. La relation d'ordre est compatible avec l'addition et la multiplication. De plus, on a l'équivalence suivante : $\forall a, b \in \mathbf{N}$, $a \leq b \Longleftrightarrow (\exists c \in \mathbf{N} \ : \ b = a + c)$. D'après la première propriété de régularité, un tel c est alors unique ; par définition, $c = b - a$.
5. Propriété d'Archimède : soient a et b deux entiers naturels avec $b \neq 0$; il existe alors un entier naturel N tel que $a < Nb$.

Exercice.
Démontrer à l'aide de ces propriétés que toute partie non vide majorée de $\mathbf{N}$ possède un plus grand élément. L'ensemble $\mathbf{N}$ admet-il un plus grand élément ?

3.1.2 Algorithmes fondamentaux

Division euclidienne dans N

Théorème 3.1.1 *Soient a, b deux entiers naturels avec $b \neq 0$. Alors il existe un unique couple d'entiers naturels (q, r) vérifiant $a = bq + r$ et $r < b$.*

Démonstration. Existence. Soit $E := \{k \in \mathbf{N} \mid a < bk\}$. On déduit de la propriété d'Archimède que E est non vide. Soit $m := \min(E)$. Alors $m \geq 1$ et l'on pose $q := m-1$, $r := a - qb$. Unicité. Supposons $a = bq + r = bq_1 + r_1$ avec, par exemple, $r \leq r_1 < b$. Alors $0 \leq r_1 - r < b$ et $r_1 - r = b(q - q_1)$ (pourquoi cette soustraction est-elle possible ?), ce qui entraine $q = q_1$ et $r = r_1$. □

Définition 3.1.2 *Dans l'énoncé du théorème, les entiers q et r sont respectivement appelés* quotient *et* reste *de la division (euclidienne) de a par b. On peut respectivement les noter $a \div b$ et a mod b.*

Exercice.
Quel résultat donne la division euclidienne de b^n par $b - 1$? de 10^{100} par 9 ?

Approche algorithmique de la division euclidienne

La preuve qui précède n'est pas « constructive ». Notons ici $q(a, b)$ et $r(a, b)$ le quotient et le reste de la division de a par b. On vérifie que $(q(a, b), r(a, b))$ vaut $(0, a)$ si $a < b$ et $(1 + q(a - b, b), r(a - b, b))$ si $a \geq b$. Cela suggère l'algorithme fonctionnel récursif suivant (en style CAML) :

```
let rec diveucl (a,b) =
  if a < b then (0,a)
  else let (q1,r1) = diveucl(a-b,b) in (1 + q1,r1);;
```

En style impératif-itératif, on procédera plutôt comme suit. On retranche b à a tant que c'est possible ; le nombre de telles soustractions est le quotient q, la valeur finale de a est le reste r. Pour réaliser cela, on déclare deux variables q et r. La première vaut 0 au départ (initialisation) et augmente de 1 à chaque étape (mises à jour). La deuxième vaut a au départ et diminue de b à chaque étape. Voici l'algorithme :

```
(* Division euclidienne de a par b *)
q := 0; r := a;
tant que r >= b faire (q := q + 1; r := r - b);
rendre(q,r);;
```

Nous allons *démontrer* que cet algorithme est correct. Il faut bien entendu supposer pour cela que les données sont valides, autrement dit que $a, b \in \mathbf{N}$ et que $b \neq 0$.

Tout d'abord, on prouve la *terminaison*, autrement dit, que le processus s'arrête un jour ! Comme presque toutes les preuves de terminaison d'algorithmes ou de programmes, celle-ci repose sur l'argument suivant : il y a un certain entier naturel (parfois appelé "compteur") qui diminue strictement à chaque étape. Comme $\mathbf{N}$ est bien ordonné, il ne peut donc y avoir une infinité d'étapes. Ici, le rôle du compteur est tenu par r. Comme on lui retranche $b \geq 1$ à chaque étape, il diminue en effet strictement.

Nous allons ensuite montrer qu'à la fin de l'exécution de l'algorithme, les valeurs rendues q et r vérifient bien les propriétés qui caractérisent le quotient et le reste. La technique repose sur la notion d'*invariant de boucle*, qui s'apparente au principe de récurrence. Notre invariant de boucle est l'affirmation suivante : *À tout moment de l'exécution de l'algorithme, q et r sont des entiers naturels tels que $a = qb + r$.*
Comme pour une démonstration par récurrence, il y a une *initialisation*, qui consiste à vérifier l'invariant de boucle au départ. Ici, l'initialisation des variables q et r est `q := 0; r := a;`, et l'on a bien, au départ :

$$qb + r = 0.b + a = a.$$

Il y a ensuite une vérification d'*hérédité*, qui consiste à prouver que, si l'invariant de boucle est satisfait avant une itération, alors il est satisfait après. On voit bien ici que les "variables" des programmeurs ne sont pas comme les variables des mathématicien, elles changent de valeur au cours du temps ! On va exprimer cela en notant q, r les valeurs contenues dans les variables `q,r` avant une itération (ou boucle), et q', r' les valeurs contenues dans les variables `q,r` après. Par définition des affectations qui constituent la boucle : `(q := q + 1; r := r - b)`, on a les relations $q' = q + 1$ et $r' = r - b$. On a donc : $q'b + r' = (q + 1)b + (r - b) = qb + r$. Ainsi :

$$a = qb + r \Longrightarrow a = q'b + r'.$$

Si l'invariant de boucle est vérifié avant, il l'est encore après ; et il l'est au départ. Donc il l'est toujours, donc encore à la fin. Les valeurs q,r rendues sont donc telles que $a = qb + r$, et nous avons *presque* fini ...

Il reste à montrer que l'on a bien (à la fin) $r < b$. Cela repose sur la condition `r >= b` de la *structure de contrôle* `tant que`. Pour que l'itération s'arrête, il faut que cette condition soit fausse (sinon, par définition de cette structure de contrôle, l'itération continuerait). À la fin de l'exécution de l'algorithme, on a donc bien $r < b$.

Exercice.
Nous n'avons pas prouvé que q,r restaient des entiers naturels. Combler cette lacune.

Numération en base b

Proposition 3.1.3 *Soit $b > 1$ un entier. Tout entier $n \in \mathbf{N}^*$ peut s'écrire de manière unique sous la forme :*

$$n = c_k b^k + c_{k-1} b^{k-1} + \cdots + c_1 b + c_0,$$

où $k \in \mathbf{N}$ et où $c_0, ..., c_k \in \{0, 1, ..., b-1\}$ et $c_k \neq 0$: les c_i sont donc des chiffres. *On dit alors que $n = c_k c_{k-1} \cdots c_1 c_0$ est* l'écriture de n en base b. *Si la base b doit être précisée, on écrit $x = (c_k c_{k-1} \cdots c_1 c_0)_b$.*

Démonstration. Unicité. Elle provient de l'unicité dans la division euclidienne, en remarquant que $n = bq_0 + c_0$, $q_0 = bq_1 + c_1, \ldots$, $q_{k-2} = bq_{k-1} + c_{k-1}$, $q_{k-1} = c_k$.
Existence. La preuve de l'unicité fournit une idée de preuve de l'existence, en remarquant que $n > q_0 > q_1 > \cdots > q_{k-2} \geq b > q_{k-1} = c_k$. □

La numération en base b permet d'effectuer de manière efficace les opérations sur les entiers : les algorithmes appris à l'école pour le calcul en base 10 se transposent sans peine. On consultera à ce sujet l'ouvrage L1 habituel (chapitre sur l'algorithmique).

Exercice.
Ecrire 13 en base 2, en base 3, et en base 7.

Exercice.
Avec les hypothèses et notations du théorème, montrer que k est l'unique entier tel que $b^k \leq n < b^{k+1}$. En déduire la « taille » de la représentation de n en base b, c'est-à-dire le nombre de chiffres nécessaires à l'écriture de n en base b.

Approche algorithmique de l'écriture en base b

On suppose connus les entiers n et b sous une forme qui permet les calculs nécessaires. Par exemple, ces entiers peuvent être codés en base 10 et les calculs effectués par un humain pour une conversion en base $b = 2$; ou au contraire, ils peuvent être codés en base 2 dans et les calculs effectués par des circuits logiques pour une conversion en base $b = 10$. Dans tous les cas, le calcul fondamental est la division euclidienne par b, que l'on représentera par une fonction auxiliaire `diveucl(a,b)` dont le résultat est le couple `(q,r)` formé du quotient et du reste. Voici une version fonctionnelle récursive :

```
let rec conversion n b = match n with
  | 0 -> []
  | - -> let (q,r) = diveucl(n,b) in r :: (conversion q b);;
```

Attention ! Cette fonction rend la liste des chiffres à l'envers, *i.e.* avec le chiffre des unités en premier ! On peut la rendre à l'endroit, mais il faut ruser : cherchez ...

Voici une version impérative itérative, qui écrit les chiffres :

```
(* conversion de n en base b *)
a := n;
tant que a > 0 faire ((q,r) := diveucl(a,b); ecrire r; a := q);;
```

Questions : dans quel ordre sortent les chiffres ? Comment justifier cet algorithme ?

Exponentiation rapide

Soient n un entier naturel et a un nombre (entier, réel ou complexe). Le calcul de a^n de manière évidente (par la définition) nécessite $n-1$ multiplication $a^{k+1} = a^k \times a$, $k = 1, \ldots, n-1$. Par « calculer rapidement », nous entendons que le nombre de multiplications utilisées ne doit pas croître linéairement avec n, comme dans l'algorithme évident ci-dessus, mais seulement avec $\log n$ (i.e. la taille de n).

Une méthode d'exponentiation plus rapide, appelée parfois exponentiation chinoise ou indienne ou babylonienne ou dichotomique, est connue depuis fort longtemps. Elle repose sur le principe « diviser pour régner » :

$$a^n := \begin{cases} a^{\frac{n}{2}} \times a^{\frac{n}{2}} & \text{si } n \text{ est pair,} \\ a \times a^{\frac{n-1}{2}} \times a^{\frac{n-1}{2}} & \text{si } n \text{ est impair.} \end{cases}$$

On a ramené le problème (calculer a^n) à deux sous-problèmes (calculer $a^{\frac{n}{2}}$) plus simples, principe qui améliore parfois les performances d'un l'algorithme.

Exemples.
1) $a^{16} = (a^8)^2 = ((a^4)^2)^2 = (((a^2)^2)^2)^2$. On effectue alors 4 multiplications au lieu de 15 : $a^2 = a \times a$, $a^4 = a^2 \times a^2$, $a^8 = a^4 \times a^4$, et $a^{16} = a^8 \times a^8$.
2) $a^{15} = a(a^7)^2 = a(a(a^3)^2)^2 = a(a(aa^2)^2)^2$. On effectue 6 multiplications au lieu de 14 : $a^3 = a \times a \times a$, $a^7 = a \times a^3 \times a^3$, $a^{15} = a \times a^7 \times a^7$.

Avec l'écriture en base 2 de $n = (c_k c_{k-1} \cdots c_0)_2 = c_0 + c_1 \cdot 2 + \cdots + c_k \cdot 2^k$, où $c_i \in \{0, 1\}$, on voit que $a^n = a^{c_0}(a^2)^{c_1}(a^{2^2})^{c_2} \cdots (a^{2^k})^{c_k}$. On a besoin au plus de k multiplications pour calculer tous les a^{2^i} $(1 \leq i \leq k)$, puis k multiplications pour former le produit des $(a^{2^i})^{c_i}$ $(1 \leq i \leq k)$. Le nombre total de multiplications est $2k = 2\lfloor \log_2 n \rfloor = O(\log n)$. Voici un algorithme basé sur cette idée :

```
(* Calcul de a puissance n *)
r := 1; x := a; p := n;
tant que p >0 faire (si p impair alors r := x * r; p := p div 2; x := x * r);
rendre r;;
```

Exercice.
Vérifier la terminaison, la correction de l'algorithme.

3.1.3 Divisibilité dans N

Définition 3.1.4 *Soient a, b deux entiers naturels. On dit que a* divise *b, ou que a est un* diviseur *de b, ou encore que b est un* multiple *de a, et l'on note $a|b$, s'il existe un entier naturel c tel que $b = ac$.*

Si a divise b, il divise tous les multiples de b. Si a divise b et c, il divise $b + c$; si de plus $b \leq c$, alors il divise $c - b$.

Exercice.
Quels entiers divisent 0 ? 1 ? 2 ? Quels entiers divise 0 ? 1 ? 2 ?

Exercice.
Montrer que la relation "a divise b" sur $\mathbf{N}$ est une relation d'ordre non total.

Nombres premiers

Définition 3.1.5 *On dit qu'un entier naturel p est* premier*, ou encore que c'est* un nombre premier*, si $p \geq 2$ et si les seuls diviseurs de p sont 1 et p.*

Pour qu'un entier $p > 1$ soit premier, il faut et il suffit qu'il ne soit pas produit de deux entiers strictement plus grands que 1. De manière équivalente : si $p = ab$, avec $a, b \in \mathbf{N}$, alors $a = 1$ ou $b = 1$. Autre caractérisation : n n'est pas premier si $n = 1$, ou si l'on peut écrire $n = ab$ avec $a, b < n$. Les premiers nombres premiers sont $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, \ldots$ et le lecteur est invité à les chercher tous jusqu'à 100.

Théorème 3.1.6 *Tout entier naturel est produit de nombres premiers.*

Démonstration. Pour $n = 1$, on convient que c'est le "produit de 0 nombres premiers" (ce point de vue est expliqué dans le chapitre 2). Au delà, on raisonne par récurrence forte. Si $n \geq 2$ est premier, il est produit d'un nombre premier ; sinon, on peut écrire $n = ab$ avec $a, b \in \mathbf{N}$ et $a, b < n$. Par hypothèse de récurrence forte, a et b sont produits de nombres premiers, donc $n = ab$ aussi. □

Corollaire 3.1.7 *Il y a une infinité de nombres premiers.*

Démonstration. Sinon, notons $p_1, \ldots, p_k$ tous les nombres premiers et soit $n := p_1 \cdots p_k + 1$. Puisque $n \geq 2$, il est divisible par un nombre premier, donc par l'un des p_i. Ce p_i divise $n = p_1 \cdots p_k + 1$ et, bien entendu, $p_1 \cdots p_k \leq n$; il divise donc $n - p_1 \cdots p_k = 1$, ce qui ne se peut. □

Exercice.
Notons $p_1, \ldots, p_k, \ldots$ les nombres premiers rangés par ordre croissant. Démontrer que $p_{k+1} \leq p_1 \cdots p_k + 1$. En déduire par récurrence que $p_k \leq 2^{2^k - 1}$.

3.2 Arithmétique dans Z

Nous allons démontrer le "Théorème fondamental de l'arithmétique" : l'écriture d'un entier naturel $n \geq 2$ en produit de facteurs premiers est unique, à l'ordre des facteurs près. Mais, pour arriver à ce résultat, il est plus commode de faire un détour par l'arithmétique des entiers relatifs.

3.2.1 L'ensemble des entiers relatifs

Nous ne traitons pas ici la construction axiomatique de l'ensemble $\mathbf{Z}$ des *entiers relatifs*, qui contient $\mathbf{N}$, et qui est muni d'une relation d'ordre notée $\leq$ qui prolonge celle de $\mathbf{N}$, et de deux opérations $+$ et $\times$ prolongeant également celles de $\mathbf{N}$. Nous supposons connues les propriétés suivantes.

1. La relation d'ordre est totale. Tout entier relatif est donc soit positif ou nul (et c'est alors un entier naturel), soit strictement négatif (et c'est alors l'opposé d'un entier naturel non nul). Avec la notation (et la définition) ci-dessous de l'opposé, on peut donc écrire l'ensemble $\mathbf{Z}$ comme une réunion disjointe :
$$\mathbf{Z} = -\mathbf{N}^* \sqcup \{0\} \sqcup \mathbf{N}^*.$$

2. Outre les propriétés énoncées sur $\mathbf{N}$, les opérations possèdent la suivante : tout élément $a \in \mathbf{Z}$ admet un unique *opposé* $-a$ tel que $a + (-a) = (-a) + a = 0$. On résume l'ensemble des ces propriétés en disant que $(\mathbf{Z}, +, \times)$ est un "anneau commutatif unitaire intègre" (voir la terminologie en **??**). L'intégrité signifie que $ab = 0$ si, et seulement si, $a = 0$ ou $b = 0$.

3. La relation d'ordre et la structure de groupe sur $(\mathbf{Z}, +)$ sont liées par la règle suivante :
$$a \leq b \Longleftrightarrow b - a \in \mathbf{N}.$$

4. La relation $\leq$ est compatible avec $+$ et $\times$ au sens suivant :
$$\begin{aligned} \forall a, b, c, d \in \mathbf{Z}\ ,\ (a \leq b \text{ et } c \leq d) &\Longrightarrow (a + c \leq b + d), \\ \forall a, b \in \mathbf{Z}\ ,\ (a \leq b) &\Longleftrightarrow (-b \leq -a), \\ \forall a, b \in \mathbf{Z}, \forall c \in \mathbf{N}^*\ ,\ (a \leq b) &\Longleftrightarrow (a \times c \leq b \times c). \end{aligned}$$

5. Toute partie non vide et majorée de $\mathbf{Z}$ admet un plus grand élément. Toute partie non vide et minorée de $\mathbf{Z}$ admet un plus petit élément.

Exercice.
Quels sont les "éléments inversibles" de $\mathbf{Z}$, *i.e.* les $a \in \mathbf{Z}$ tels qu'il existe $b \in \mathbf{Z}$ tel que $ab = 1$?

Valeur absolue

Soit $a \in \mathbf{Z}$. Si $a > 0$, alors $a > -a$. Si $a < 0$, alors $a < -a$. Si $a = 0$, alors $a = -a$. Le plus grand des entiers a et $-a$ est donc dans tous les cas un entier naturel, appelé *valeur absolue* de a et noté $|a|$:

$$|a| := \max(a, -a) = \begin{cases} a \text{ si } a \geq 0, \\ -a \text{ si } a \leq 0. \end{cases}$$

On retrouve les propriétés de la valeur absolue sur $\mathbf{R}$:

$$\begin{aligned} |a| = 0 &\iff a = 0, \\ |-a| &= |a|\,, \\ |a+b| &\leq |a| + |b|\,, \\ |ab| &= |a|\ |b|\,. \end{aligned}$$

Exercice.
Reconnaitre $\dfrac{a+b+|a-b|}{2}$.

Divisibilité

Définition 3.2.1 *Soient a, b deux entiers relatifs. On dit que a* divise *b, ou que a est un* diviseur *de b, ou que b est un* multiple *de a, ce que l'on note $a|b$, s'il existe un entier relatif c tel que $b = ac$.*

C'est presque une relation d'ordre. Elle est réflexive : $\forall a \in \mathbf{Z}\ ,\ a|a$; et elle est transitive : $\forall a, b, c \in \mathbf{Z}\ ,\ (a|b \text{ et } b|c) \implies a|c$. Mais elle n'est pas antisymétrique : $\forall a, b \in \mathbf{Z}\ ,\ (a|b \text{ et } b|a) \not\implies a = b$. Voyez-vous pourquoi ?

Enfin, on a la propriété algébrique suivante :

$$\forall a, b, c \in \mathbf{Z}\ ,\ (a|b \text{ et } a|c) \implies a|b \pm c.$$

Nous noterons $D(x)$ l'ensemble des diviseurs de $x \in \mathbf{Z}$. Par exemple, $D(0) = \mathbf{Z}$, $D(1) = \{+1, -1\}$ et $D(6) = \{+1, +2, +3, +6, -1, -2, -3, -6\}$. De manière générale, si $a \neq 0$, l'ensemble $D(a)$ est fini, car tout diviseur x de a vérifie $|x| \leq |a|$. (L'ensemble $D(a)$ admet donc au plus $2\,|a| + 1$ éléments.)

Il est clair que $D(a) = D(-a)$, donc que $D(a) = D(|a|)$. Réciproquement, pour que $D(a) = D(b)$, il faut, et il suffit, que $b = \pm a$ (car a divise b et b divise a).

Exercice.
Quels sont les diviseurs, les multiples, de 0, de 1, de -1 dans $\mathbf{Z}$? Quels entiers relatifs sont diviseurs de tous les entiers relatifs ? Quels entiers relatifs sont multiples de tous les entiers relatifs ?

3.2.2 Algorithmes fondamentaux

Division euclidienne

Théorème 3.2.2 *Soient a, b deux entiers relatifs avec $b > 0$. Il existe alors un unique couple d'entiers relatifs (q, r) tel que $a = bq + r$ et $0 \leq r < b$. Les entiers q et r sont respectivement appelés* quotient *et* reste *de la division (euclidienne) de a par b. On peut respectivement les noter $a \div b$ et $a \bmod b$.*

Démonstration. Les entiers relatifs a, b, q étant donnés, avec $b > 0$, l'existence de r tel que $a = bq + r$ et $0 \leq r < b$ équivaut à l'encadrement $0 \leq a - bq < b$, donc à :

$$bq \leq a < b(q + 1).$$

On doit choisir pour q le plus grand élément de l'ensemble E des entiers relatifs x tels que $bx \leq a$. Il faut, pour cela, vérifier que E est non vide et majoré. Nous le prouverons en supposant $a < 0$ (sinon, on est ramené à la division euclidienne dans $\mathbf{N}$). La première assertion découle de la propriété d'Archimède : choisir N tel que $Nb > |a|$, et vérifier que $-N \in E$. La deuxième assertion est triviale, E étant majoré par 0. □

Exercice.
Adapter l'algorithme de division euclidienne au cas où $a < 0$.

Algorithme d'Euclide et pgcd

Le but de l'algorithme d'Euclide est de déterminer l'ensemble des *diviseurs communs* à deux entiers relatifs a, b. Cet ensemble sera noté :

$$CD(a, b) := D(a) \cap D(b).$$

Comme $D(a) = D(|a|)$ et $D(b) = D(|b|)$, on a $CD(a, b) = CD(|a|, |b|)$, et l'on peut donc se ramener au cas de deux entiers naturels. L'algorithme repose sur les idées suivantes :

Lemme 3.2.3 *Soient a, b deux entiers naturels. Si $b = 0$, alors $CD(a, b) = D(a)$. Si $b > 0$, soit r le reste de la division euclidienne de a par b ; alors : $CD(a, b) = CD(b, r)$.*

Démonstration. Puisque $D(0) = \mathbf{Z}$, la première assertion est évidente. Supposons donc $b > 0$ et soit q le reste de la division euclidienne de a par b, de sorte que $a = qb + r$. Si $x \in CD(a, b)$, alors x divise $qb + r$ et b, donc $qb + r$ et qb,, donc leur différence r, donc $x \in CD(b, r)$. Si réciproquement $x \in CD(b, r)$, alors x divise b et r, donc qb et r, donc $qb + r = a$, donc $x \in CD(a, b)$. □

Algorithme : forme mathématique. Soient $(a, b) \in \mathbf{N} \times \mathbf{N}^*$. On veut calculer $CD(a, b)$. On pose $r_0 := a$, $r_1 := b$. On effectue des divisions euclidiennes successives :

$$\begin{aligned} r_0 &= q_0 r_1 + r_2 \\ r_1 &= q_1 r_2 + r_3 \text{ si } r_2 \neq 0 \\ r_2 &= q_2 r_3 + r_4 \text{ si } r_3 \neq 0 \\ &\cdots \\ r_k &= q_k r_{k+1} + r_{k+2} \text{ si } r_{k+1} \neq 0 \\ &\cdots \end{aligned}$$

Comme $b = r_1 > r_2 > \cdots \geq 0$, il existe $N \geq 2$ tel que $r_{N-1} \neq 0$ et $r_N = 0$. D'après le lemme, on a :

$$CD(a, b) = CD(r_0, r_1) = CD(r_1, r_2) = \cdots = CD(r_{N-1}, r_N) = CD(r_{N-1}, 0) = D(r_{N-1}),$$

où r_{N-1} est le dernier reste non nul.

Proposition 3.2.4 *Soient a, b deux entiers relatifs. Il existe un unique entier naturel d tel que $CD(a, b) = D(d)$.*

Démonstration. Si $a = b = 0$, alors $CD(a, b) = \mathbf{Z}$ et $d := 0$ est la seule solution possible.
Le problème étant symétrique en a et b, on va donc supposer que $b \neq 0$. Quitte à remplacer a et b par leurs valeurs absolues respectives, ce qui ne change pas $CD(a, b)$, on peut supposer que $a \in \mathbf{N}$ et que $b \in \mathbf{N}^*$. On prend alors $d := r_{N-1}$ avec les notations de l'algorithme, ce qui établit l'existence de d.
Enfin, si $CD(a, b) = D(d) = D(d')$, on a $d' = \pm d$ et seul l'un des deux est naturel. □

Définition 3.2.5 *L'unique entier naturel d tel que $CD(a, b) = D(d)$ est appelé* plus grand commun diviseur *de a et b, et noté $pgcd(a, b)$.*

Remarque.
Il faut prendre garde que $pgcd(a, b)$ n'est pas seulement le plus grand parmi les diviseurs communs aux entiers a et b : c'est en fait un multiple de tous ces diviseurs communs. Par exemple, les diviseurs communs à 12 et 18 sont $\pm 1, \pm 2, \pm 3, \pm 6$. Leur pgcd est donc 6, qui non seulement est le plus grand parmi ces diviseurs, mais qui en est multiple commun.

Algorithme : forme algorithmique. Voici d'abord une version fonctionnelle récursive :

```
let rec pgcd a b = match b with
  | 0 -> a
  | - -> let (q,r) = diveucl(n,b) in (pgcd b r);;
```

Voici maintenant une version impérative itérative. Comme d'habitude, le principe est de déclarer des variables globales qui prendront successivement les valeurs r_i.

```
(* calcul du pgcd de a et b *)
x := a; y := b;
tant que y > 0 faire ((q,r) := diveucl(x,y); x := y; y := r);;
rendre x;;
```

Exercice.
Calculer $pgcd(9000, 1575)$ et $pgcd(1480, 324)$.

Exercice.
Soient $(a, b) \in \mathbf{Z} \times \mathbf{Z} \setminus \{(0, 0)\}$.
1) Soit $d = pgcd(a, b)$. Montrer que $pgcd(\frac{a}{d}, \frac{b}{d}) = 1$.
2) Montrer que pour tout entier $n \geq 1$, on a $pgcd(na, nb) = npgcd(a, b)$.

Exercice.
Soit $r \in \mathbb{Q}_+$. Montrer qu'il existe un unique couple $(u, v) \in \mathbf{N} \times \mathbf{N}^*$ tel que $r = \frac{u}{v}$ et $pgcd(u, v) = 1$ ("forme réduite" ou "irréductible" du rationnel r).

Exercice.
Préciser les hypothèses de bon fonctionnement de l'algorithme algorithmique et le justifier. En écrire une version récursive.

Algorithme d'Euclide étendu et coefficients de Bézout

Reprenons l'algorithme d'Euclide sous sa forme mathématique. On peut calculer les r_i en fonction de a et b et des quotients q_i comme suit ; $r_0 = a$, $r_1 = b$, puis :

$$\begin{aligned} r_2 &= r_0 - q_0 r_1 = a - q_0 b \\ r_3 &= r_1 - q_1 r_2 = -q_1 a + (1 + q_1 q_0) b \\ r_4 &= r_2 - q_2 r_3 = (1 + q_1 q_2) a - (q_0 + q_2 + q_1 q_0 q_2) b \\ &\dots \end{aligned}$$

et chaque r_i s'obtient comme "combinaison linéaire à coefficients entiers" de a et b.

Exemple.
Le pgcd de $a = 215$ et $b = 150$ s'obtient par les divisions euclidiennes suivantes :

$$215 = 1.150 + 65,\ 150 = 2.65 + 20,\ 65 = 3.20 + 5,\ 20 = 4.5 + 0.$$

On a donc $pgcd(215, 150) = 5$. On peut "remonter" ces égalités :

$5 = 65 - 3.20 = 65 - 3.(150 - 2.65) = 7.65 - 3.150 = 7.(215 - 1.150) - 3.150 = 7.215 - 10.150.$

Théorème 3.2.6 (Théorème de Bézout) *Soient a et b deux entiers relatifs. Il existe alors deux entiers $u, v \in \mathbf{Z}$ vérifiant la* relation de Bézout *:*

$$au + bv = pgcd(a, b).$$

Démonstration. Avec les notations ci-dessus, posons $u_0 := 1$, $v_0 := 0$, $u_1 := 0$, $v_1 := 1$, puis les relations de récurrence :

$$\begin{cases} u_{k+2} := u_k - q_k u_{k+1}, \\ v_{k+2} := v_k - q_k v_{k+1}. \end{cases}$$

On voit alors par récurrence sur k que $r_k = au_k + bv_k$. Il suffit donc de prendre $u := u_{N-1}$ et $v := v_{N-1}$. □

Définition 3.2.7 *Soient a, b deux entiers. On dit que a et b sont* premiers entre eux *si $pgcd(a, b) = 1$.*

Corollaire 3.2.8 *Soient $(a, b) \in \mathbf{Z} \times \mathbf{Z} \setminus \{(0, 0)\}$. Alors a et b sont premiers entre eux si, et seulement s'il existe $u, v \in \mathbf{Z}$ tels que $au + bv = 1$.*

Algorithme : forme algorithmique. Outre les variables `x` et `y` de l'algorithme d'Euclide "simple", nous entretenons quatre nouvelles variables destinées à exprimer les valeurs successives de `x` et `y` en fonction de a et b.

```
(* calcul du pgcd de a et b et des coefficients de B\'ezout u et v *)
x := a; y := b; u := 1; v := 0; s := 0; t := 1;
tant que y > 0 faire
    ((q,r) := diveucl(x,y);
     x := y;
     y := r
     (u,s) := (s,u - q s);            (* affectations simultanees *)
     (v,t) := (t,v - q t));;
rendre (x,u,v);;
```

Exercice.
Soient $a, b, c \in \mathbf{Z}$. Démontrer l'équivalence logique :

$$(\exists x, y \in \mathbf{Z} \ : \ ax + by = c) \iff pgcd(a, b) | c.$$

Exercice.
Justifier l'algorithme étendu (terminaison, correction). (Utiliser l'invariant de boucle : $x = ua + vb$ et $y = sa + tb$.)

3.2.3 Divisibilité dans Z

Rappelons que $a, b \in \mathbf{Z}$ sont dits premiers entre eux si leurs seuls diviseurs communs sont $+1$ et -1 ; et que cette relation équivaut à l'existence de $u, v \in \mathbf{Z}$ tels que $ua+vb = 1$ (relation de Bézout).

Proposition 3.2.9 (Lemme de Gauss) *Soient $a, b, c \in \mathbf{Z}$. Si a divise bc et si a et b sont premiers entre eux, alors a divise c.*

Démonstration. L'hypothèse que a divise bc s'écrit $bc = ax$, avec $x \in \mathbf{Z}$. L'hypothèse que a et b sont premiers entre eux s'écrit $ua + vb = 1$ avec $u, v \in \mathbf{Z}$. On a alors :

$$c = (ua + vb)c = uac + vbc = uac + vax = ay,$$

avec $y := uc + vx \in \mathbf{Z}$, de sorte que a divise c. □

Lemme 3.2.10 *Soient p un nombre premier et n un entier. Alors ou bien p divise n, ou bien p et n sont premiers entre eux.*

Démonstration. Les seuls diviseurs de p sont ± 1 et $\pm p$. Si p et n ne sont pas premiers entre eux, ils admettent d'autres diviseurs communs que $+1$ et -1, donc p ou $-p$ divise n, donc, dans tous les cas, p divise n. □

Proposition 3.2.11 (Lemme d'Euclide) *Soient p un nombre premier et $b, c \in \mathbf{Z}$. Si p divise bc, alors p divise b ou p divise c. Plus généralement, si p divise un produit $b_1 \cdots b_k$, alors il divise l'un des b_i.*

Démonstration. La première assertion vient immédiatement en combinant le lemme ci-dessus avec le lemme de Gauss. La deuxième se prouve par application réitérée de la première. □

Corollaire 3.2.12 *Les diviseurs premiers de $n!$ sont les nombres premiers $\leq n$.*

Démonstration. Tout diviseur premier de $n! = \prod_{k=1}^{n} k$ est diviseur de l'un des $k \in \{1, \ldots, n\}$ donc est $\leq n$. Réciproquement, tout nombre premier $\leq n$ figure parmi les $k \in \{1, \ldots, n\}$, donc divise $n!$. □

Corollaire 3.2.13 *Soient p un nombre premier et k un entier tel que $1 \leq k \leq p-1$. Alors p divise $C_p^k = \binom{p}{k}$.*

Démonstration. Soient $x := \binom{p}{k} \in \mathbf{Z}$. Alors p ne divise ni $k!$ ni $(p-k)!$ (d'après le corollaire précédent) ni donc leur produit $y := k!\,(p-k)!$ (d'après le lemme d'Euclide). Comme p divise $p! = xy$, il divise donc x (toujours d'après le lemme d'Euclide). □

Théorème 3.2.14 (Théorème fondamental de l'arithmétique) *Tout entier naturel $n \geq 2$ peut s'écrire comme un produit de nombres premiers, et cette factorisation est unique à l'ordre près.*

Démonstration. L'existence d'une telle factorisation a déjà été démontrée au paragraphe 3.1.3. L'unicité se prouve ainsi. Supposons que l'on ait :

$$n = p_1 \dots p_r = q_1 \dots q_s,$$

où les p_i et les q_j sont premiers. Alors, par application du lemme d'Euclide, on voit que p_r divise l'un des q_j ; ce dernier étant premier, on a donc $p_r = q_j$. Quitte à modifier la numérotation, on peut supposer que $j = s$. Le facteur premier $p := p_r = q_s$ est donc présent dans les deux factorisations, et l'on en déduit en le simplifiant les deux factorisations $p_1 \dots p_{r-1} = q_1 \dots q_{s-1}$ de n/p. On peut alors renouveler l'argument. □

Tout entier est donc produit de ses *facteurs premiers*, éventuellement comptés plusieurs fois (autrement dits, munis d'exposants). On conviendra de faire figurer *tous les nombres premiers* dans une telle factorisation (ou *décomposition*), tout simplement en affectant d'un exposant nul ceux qui ne divisent pas l'entier concerné ! Notant $p_1, p_2, \dots$ la suite de tous les nombres premiers, rangés par ordre croissant, on voit donc que tout entier naturel non nul s'écrit de manière unique :

$$n = \prod_{i \geq 1} p_i^{e_i},$$

les entiers e_i étant presque tous nuls. Par exemple, dans l'écriture de $n = 1$, tous les e_i sont nuls ; dans l'écriture d'un nombre premier $n = p_{i_0}$, l'exposant e_{i_0} vaut 1 et tous les autres sont nuls ; etc. Si l'on note $a = \prod_{i \geq 1} p_i^{e_i}$ et $b = \prod_{i \geq 1} p_i^{f_i}$, il est clair que $ab = \prod_{i \geq 1} p_i^{e_i + f_i}$, et l'on en déduit facilement les règles suivantes :

$$\big(a|b \iff \forall i \geq 1\ ,\ e_i \leq f_i\big),\ \text{et}\ pgcd(a,b) = \prod_{i \geq 1} p_i^{\min(e_i, f_i)}.$$

Exercice.
(i) Avec les notations ci-dessus, montrer que les multiples communs a et b sont les multiples de leur "plus grand commun diviseur" $pgcd(a,b) = \prod_{i \geq 1} p_i^{\max(e_i, f_i)}$.
(ii) Démontrer que $\text{ppcm}(a,b)pgcd(a,b) = ab$.

Exercice.
(i) Énumérer les facteurs premiers de 15!. Pour chacun d'entre eux, préciser son exposant dans la décomposition de 15! en produits de facteurs premiers.
(ii) Écrire la décomposition de 15! en produits de facteurs premiers.
(iii) Déterminer le nombre de diviseurs de 15!.

3.2.4 Congruences

Définition 3.2.15 *Soient $n \in \mathbf{N}^*$ et $a, b \in \mathbf{Z}$. On dit que a* est congru à *b* modulo *n si n divise $a - b$. On écrit alors $a \equiv b \pmod{n}$.*

Proposition 3.2.16 *(i) La relation de congruence est une relation d'équivalence. Plus précisément :*

$$\begin{aligned}
\forall a \in \mathbf{Z}\ ,\ & a \equiv a \pmod{n},\\
\forall a, b \in \mathbf{Z}\ ,\ & (a \equiv b \pmod{n}) \Longrightarrow (b \equiv a \pmod{n}),\\
\forall a, b, c \in \mathbf{Z}\ ,\ & (a \equiv b \pmod{n} \text{ et } b \equiv c \pmod{n}) \Longrightarrow (a \equiv c \pmod{n}).
\end{aligned}$$

Ces propriétés sont respectivement appelées réflexivité, symétrie *et* transitivité *de la relation.*
(ii) Cette relation d'équivalence est compatible avec l'addition et la multiplication. Plus précisément :

$$\begin{aligned}
&\forall a, b, a', b' \in \mathbf{Z}\ ,\ (a \equiv a' \pmod{n} \text{ et } b \equiv b' \pmod{n}) \Longrightarrow a + a' \equiv b + b' \pmod{n},\\
&\forall a, b, a', b' \in \mathbf{Z}\ ,\ (a \equiv a' \pmod{n} \text{ et } b \equiv b' \pmod{n}) \Longrightarrow aa' \equiv bb' \pmod{n}.
\end{aligned}$$

Toutes ces propriétés sont très faciles à démontrer, on en laisse le plaisir au lecteur. Il ne faut cependant pas les sous-estimer, car elles sont fondamentales et interviennent en permanence implicitement dans les raisonnements.

Proposition 3.2.17 *Soient a un entier relatif quelconque et n un entier naturel non nul. Il existe alors un unique "représentant" $r \in \{0, \ldots, n-1\}$ tel que $a \equiv r \pmod{n}$.*

Démonstration. Écrivons $a = qn + r$ (division euclidienne de a par n), de sorte que $a \equiv r \pmod{n}$ et que $r \in \{0, \ldots, n-1\}$: cela prouve l'existence du représentant r de la "classe de congruence" de a.
Pour établir l'unicité de ce représentant dans $\{0, \ldots, n-1\}$, on suppose que l'on a trouvé $r, r' \in \{0, \ldots, n-1\}$ tels que $a \equiv r \pmod{n}$ et $a \equiv r' \pmod{n}$. Puisque la relation de congruence est symétrique et transitive, on a $r \equiv r' \pmod{n}$. Comme $|r - r'| < n$, cela implique que $r = r'$. □

Cette proposition permet de démontrer beaucoup de propriétés générales des entiers relatifs par examen d'un nombre fini de cas.

Exemple.
Pour tout $a \in \mathbf{Z}$, l'entier $a^3 - a$ est divisible par 6. Pour le voir, on raisonne ainsi : si $a \equiv r \pmod{6}$, alors $a^3 - a \equiv r^3 - r \pmod{6}$ (cela vient du fait que l'on a une relation d'équivalence compatible avec l'addition et la multiplication). Il suffit donc de vérifier que $r^3 - r \pmod{6}$ lorsque $r \in \{0, \ldots, 5\}$: on laisse au lecteur le plaisir de contrôler ces six cas.

Des exemples de congruences

1. Tout carré est congru modulo 8 à 0, 1 ou 4. Il suffit de le vérifier pour les carrés de $0, 1, \ldots, 7$. (À faire **maintenant !)**
2. Puisque 8 est multiple de 4, on en déduit que tout carré est congru modulo 4 à 0 ou 1 ; et donc que toute somme de deux carrés est congrue modulo 4 à 0, 1 ou 2. L'égalité $a^2 + b^2 = 4n - 1$ est donc impossible en nombres entiers.
3. De même, en vertu du premier item, l'égalité $a^2 + b^2 + c^2 = 8n + 7$ est impossible en nombres entiers.

Deux critères de divisibilité par $b \pm 1$

Soit b un entier ≥ 2. Notons $a := b - 1$ et $c := b + 1$. De la proposition 3.2.16, on déduit les congruences :

$$\begin{aligned} b \equiv 1 \pmod{a} &\implies \forall k \in \mathbf{N}\,, \quad b^k \equiv 1 \pmod{a}, \\ b \equiv -1 \pmod{c} &\implies \forall k \in \mathbf{N}\,, \quad b^k \equiv (-1)^k \pmod{c}. \end{aligned}$$

Soit maintenant x un entier naturel écrit en base b :

$$x = (c_k c_{k-1} \cdots c_1 c_0)_b = \sum_{i=0}^{k} c_i b^i.$$

Toujours de la proposition 3.2.16, on déduit les congruences :

$$x \equiv \sum_{i=0}^{k} c_i \pmod{a} \text{ et } x \equiv \sum_{i=0}^{k} (-1)^i c_i \pmod{c}.$$

En particulier :

1. Pour que l'entier x soit divisible par $b - 1$, il faut, et il suffit, que la somme $c_0 + \cdots + c_k$ de ses chiffres soit soit divisible par $b - 1$.
2. Pour que l'entier x soit divisible par $b + 1$, il faut, et il suffit, que la somme "alternée" $c_0 - c_1 + c_2 + \cdots + (-1)^k c_k$ de ses chiffres soit soit divisible par $b + 1$.

En base dix, on reconnait les critères classiques de divisibilité par neuf et par onze [1].

Exercice.
Voici deux nouvelles preuves de l'exemple qui suit la proposition 3.2.17.
(i) Le produit de trois entiers consécutifs est divisible par par 2 et par 3, donc par 6. Appliquer à l'exemple.
(ii) Lorsque $a \in \mathbf{N}$, déduire l'exemple du fait que $\binom{a}{3}$ est entier. Comment passer au cas $a \in \mathbf{Z}$?

[1] L'un des rédacteurs de ce poly a appris cette application avec sa démonstration complète en 1964, en classe de *cinquième*, dans le lycée d'une petite ville de province.

3.3 Deux théorèmes classiques

3.3.1 Un théorème grec en rapport avec Fermat

Voici un problème *antique* : quels triangles rectangles ont trois côtés entiers ? D'après le théorème de Pythagore, on est ramené résoudre l'équation "diophantienne" :

$$a^2 + b^2 = c^2, a, b, c \in \mathbf{N}. \tag{3.1}$$

L'adjectif (qui fait référence au mathématicien grec Diophante) signifie que l'on cherche des solutions *entières*. Il y a bien entendu les solutions "triviales", telles que $a = 0$ et $b = c$, ou $b = 0$ et $a = c$. Les premiers exemples non triviaux sont bien connus : $3^2 + 4^2 = 5^2$ et $12^2 + 5^2 = 13^2$. On vérifie aussi que, si $(a, b, c) \in \mathbf{N}^3$ est solution de (3.1), alors, pour tout $d \in \mathbf{N}$, le triplet (da, db, dc) est également solution de (3.1). Pour aller plus loin, nous aurons besoin d'un lemme.

Lemme 3.3.1 *(i) Si $x, y \in \mathbf{N}$ sont tels que x^2 divise y^2, alors x divise y.*
(ii) Si $x, y \in \mathbf{N}$ ont pour pgcd d et sont tels que le produit xy est un carré (d'entier naturel), alors $x = du^2$ et $y = dv^2$, où $u, v \in \mathbf{N}$.

Démonstration. (i) On écrit les décompositions en facteurs premiers $x = \prod_{i\geq 1} p_i^{e_i}$ et $y = \prod_{i\geq 1} p_i^{f_i}$, et l'on remarque que $2e_i \leq 2f_i \Rightarrow e_i \leq f_i$.
(ii) Commençons par le cas où $d = 1$, *i.e.* x, y sont premiers entre eux. On écrit les décompositions en facteurs premiers $x = \prod_{i\geq 1} p_i^{e_i}$ et $y = \prod_{i\geq 1} p_i^{f_i}$. Dire que x, y sont premiers entre eux revient à dire que, pour tout i, l'un des exposants e_i, f_i au moins est nul. Dire que xy est un carré revient à dire que, pour tout i, l'exposant $e_i + f_i$ est pair. Il en découle que tous les e_i et tous les f_i sont pairs, donc que x et y sont des carrés. Dans le cas général, on pose $x = dx'$ et $y = dy'$. Puisque $d^2x'y'$ est un carré, on déduit facilement de l'assertion (i) que $x'y'$ est un carré, et l'on est ramené au premier cas. □

Proposition 3.3.2 *Toute solution de (3.1) est de la forme (da, db, dc), où $(a, b, c) \in \mathbf{N}^3$ est solution de (3.1) et où a, b, c sont premiers entre eux deux à deux.*

Démonstration. Soit $(a', b', c') \in \mathbf{N}^3$ une solution de (3.1) et soit d le pgcd de a' et b'. On a donc $a' = da$ et $b' = db$, et $a, b \in \mathbf{N}$ sont premiers entre eux. On a alors $c'^2 = d^2(a^2 + b^2)$, et, d'après l'assertion (i) du lemme ci-dessus, d divise c'. On écrit $c' = dc$ et l'on a évidemment $a^2 + b^2 = c^2$ et $(a', b', c') = (da, db, dc)$.
Reste à voir que a, b, c sont premiers entre eux deux à deux. C'est vrai par construction pour a et b. On va le prouver pour b et c (le cas de a et c est similaire). S'ils n'étaient pas premiers entre eux, ils admettraient un facteur premier commun p, lequel diviserait b^2 et c^2, donc $a^2 = c^2 - b^2$, donc a (lemme d'Euclide), contredisant le fait que a et b sont premiers entre eux. □

Une solution $(a, b, c) \in \mathbf{N}^3$ de (3.1) telle que a, b, c sont premiers entre eux deux à deux sera dite *primitive*. Il suffit de les déterminer toutes ; le résultat suivant apparaît déjà dans les *Éléments d'Euclide*.

Théorème 3.3.3 *Toute solution primitive de (3.1) est (quitte à permuter a et b) de la forme $(2uv, u^2 - v^2, u^2 + v^2)$, où $u, v \in \mathbf{N}$ sont premiers entre eux et $v \leq u$.*

Démonstration. Seul l'un des entiers a, b, c est pair (sinon, la solution ne serait pas primitive). Si a et b étaient impairs, on aurait $a^2, b^2 \equiv 1 \pmod 4$, donc $c^2 = a^2 + b^2 \equiv 2 \pmod 4$, ce qui ne se peut. Ainsi, c est impair ainsi que a ou b, mettons b ; et a est pair. On tire de (3.1) l'égalité $a^2 = (c - b)(c + b)$, dans laquelle $c - b$ et $c + b$ sont naturels et ont pour pgcd 2 : en effet, ils sont pairs, et, si le nombre premier p les divise tous les deux, il divise leur somme $2c$ et leur différence $2b$ dont le pgcd est 2 (puisque b et c sont premiers entre eux). D'après l'assertion (ii) du lemme ci-dessus, $c + b = 2u^2$ et $c - b = 2v^2$, où $u, v \in \mathbf{N}$. La fin de la démonstration est alors facile ... et laissée au lecteur ! □

Exercice.
Vérifier que, si $u, v \in \mathbf{N}$ et $v \leq u$, alors $(2uv, u^2 - v^2, u^2 + v^2)$ est bien solution de (3.1). À quelle condition cette solution est-elle primitive ?

Exercice.
Quel est le rapport avec Fermat ?

3.3.2 Un théorème dû à Fermat

Théorème 3.3.4 (Petit théorème de Fermat) *Soient p un nombre premier et a un entier. On a $a^p \equiv a \pmod p$.*

Démonstration. Posons $f(a) = a^p - a$. On a donc :

$$f(a+1) - f(a) = \big((a+1)^p - (a+1)\big) - (a^p - a) = (a+1)^p - a - 1 = \sum_{k=1}^{p-1} \binom{p}{k} a^k,$$

qui est un multiple de p, en vertu du corollaire 3.2.13. On en déduit la congruence :

$$\forall a \in \mathbf{Z}\ ,\ f(a+1) \equiv f(a) \pmod p.$$

Comme $f(0) = 0$, la propriété est allors immédiate pour $a \in \mathbf{N}$, par récurrence sur a ; puis, pour $-a \in \mathbf{N}$, par récurrence sur $-a$. □

Exercice.
Démontrer, pour tout $a \in \mathbf{Z}$, la congruence : $a^{561} \equiv a \pmod{561}$. L'entier 561 est-il premier ?