UNE INVITATION AUX MATHEMATIQUES

S. De Bièvre

Novembre 2005

S. De Bièvre

Table des matières

S. De Bièvre

Chapitre 1

Arithmétique

MATHEMATIQUES – Dessèchent le coeur
Flaubert, Dictionnaire des idées reçues

1.1 Introduction

L'arithmétique est la partie des mathématiques qui se consacre à l'étude des nombres entiers. Les entiers sont sans nul doute les objets mathématiques les plus familiers aux non-mathématiciens, et aussi les plus étudiés par les mathématiciens eux-mêmes à travers les siècles. Ils sont néanmoins loin d'avoir livré tous leurs secrets, et les théoriciens des nombres s'acharnent aujourd'hui encore à essayer de les leur arracher.

Pour illustrer ces propos et dans le but de vous motiver pour l'étude de ce chapitre, je vous présente tout de suite quelques questions concernant les entiers, des plus simples aux plus compliquées. A certaines nous répondrons dans ce chapitre ou le suivant, à d'autres personne ne connaît la réponse à ce jour, à d'autres encore la réponse est connue, mais en comprendre le raisonnement nécessite des connaissances profondes en mathématiques. Nous débattrons également de l'intérêt de telles questions à la fin de l'introduction.

Question 1 : Quel est le dernier chiffre (c'est-à-dire le chiffre des unités) dans l'écriture décimale de 2^{500} ?

Il y a trois façons d'aborder cette question. La première consiste à attaquer le problème bille en tête par la force brute du calcul direct : vous calculez successivement $2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, \ldots$ et ainsi de suite. Vous pouvez facilement vous convaincre que cette méthode n'est pas très efficace : comme $2^{10} = 1024 > 10^3$ on a $2^{400} > (10^3)^{40} = 10^{120}$ et donc 2^{400} est déjà un nombre ayant au moins 120 chiffres dans son écriture décimale. Afin de le multiplier par deux pour calculer 2^{401}, on aurait besoin de beaucoup de temps et de très grandes feuilles de papier. La deuxième méthode consiste à utiliser une calculette : elle abdiquera devant la lourdeur de la tâche et vous donnera un message d'erreur. La raison est qu'une calculette n'est pas prévue pour stocker d'aussi grands nombres (dans le jargon informatique, on dit qu'elle ne calcule pas en précision arbitraire). Un ordinateur, par contre, fait le calcul en un clin d'oeil. Il y a finalement une troisième méthode, très efficace, qui consiste à commencer par réfléchir. Un minimum d'arithmétique, expliqué dans la Section 1.2, permet alors de répondre rapidement et sans peine à cette question ainsi qu'à d'autres questions semblables, comme : existe-t-il un entier positif n tel que le chiffre des unités de 3^n vaut 5 ?

Question 2 : Pourquoi un entier est-il divisible par trois si et seulement si la somme de ces chiffres (dans son écriture décimale) l'est ?

Cette règle, vous l'avez apprise à l'école primaire, avec quelques autres (les "critères de divisibilité"), et vous la croyez, parce qu'on vous a dit qu'elle fonctionne toujours. Mais en êtes-vous sûrs ? Même si vous ne mettez pas en doute la règle n'êtes-vous pas intrigué de savoir comment quelqu'un ait pu découvrir une telle chose ? Pourquoi d'ailleurs enseigne-t-on à l'école élémentaire de telles règles pour la division par $2, 3, 4, 5, 8, 9, 10$ et 11, mais pas par 6 et 7 ? Les réponses à ces questions sont simples et vous les trouverez à la fin de la section suivante.

Question 3 : Toute fraction peut être mise sous forme décimale. Ce développement décimal est soit fini, soit il se répète à l'infini de façon périodique à partir d'un certain rang. Pourquoi ?

Illustrons ces propos : $\frac{13}{20} = 0,65$ et $\frac{123}{130} = 0,9461538461538461538\ldots$. Dans le premier cas, le développement est fini : on obtient un reste nul après un nombre fini de pas. Dans le deuxième cas, les restes ne sont jamais nuls, mais ils finissent par se répéter périodiquement. Il y a au moins deux choses à comprendre ici : pourquoi les restes finissent-ils par se répéter de façon périodique et que veulent dire les trois points $\ldots$, qui rendent l'égalité entre $\frac{123}{130}$ et $0,9461538461538461538\ldots$ un peu mystérieuse pour le néophyte. Pour répondre à ces questions, nous utiliserons des résultats d'arithmétique ainsi que quelques autres arguments : nous y reviendrons dans le Chapitre 9.

Question 4 : Existe-t-il un nombre rationnel $\frac{p}{q}$ dont le carré vaut 2 ?

Ici p et q désignent des entiers positifs. Vous savez que la réponse à cette question est négative parce qu'on vous l'a dit, et vous connaissez la réponse aussi sous la forme "$\sqrt{2}$ est irrationnel." Mais pourquoi ceci est-il vrai ? Comment montrer qu'on ne peut jamais trouver des entiers p et q tel que $\frac{p^2}{q^2} = 2$? La même question se pose d'ailleurs pour $\sqrt{5}, \sqrt{10}$, etc. Nous y répondrons dans la Section 1.5. Vous verrez que les mathématiques nécessaires pour obtenir la réponse ne sont pas vraiment difficiles. La démonstration de "$\sqrt{2}$ n'est pas rationnel" n'est néanmoins pas triviale et donne une illustration illuminante d'une méthode de démonstration très performante dans bien d'autres problèmes : le raisonnement par l'absurde. La légende veut d'ailleurs que Platon, lorsqu'il apprit pour la première fois la démonstration de l'irrationalité de $\sqrt{2}$, fut tellement ébloui par sa beauté et sa puissance, qu'il décida de faire l'offrande d'un agneau aux dieux. J'espère que vous aussi, vous trouverez ici quelque chose d'irrésistible dans le contraste entre la simplicité du raisonnement et la puissance de la conclusion, qui défie tout de même un peu l'imagination. Nous reparlerons de tout cela en

détail dans les Sections 1.4 et 1.5.
Question 5 : Combien y a-t-il de nombres premiers inférieurs à un nombre positif x quelconque donné ?

Rappelons qu'un nombre premier est un entier strictement plus grand que 1 qui n'a d'autres diviseurs que 1 et lui-même :

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, \ldots$$

sont des nombres premiers. Une première question qui se présente irrésistiblement est : "Y a-t-il un nombre fini ou infini de nombres premiers ?" Pour le dire différemment : "Y a-t-il un plus grand nombre premier ?" Il s'avère que la réponse est : "Non, il n'y a pas de plus grand nombre premier, parce qu'il y en a bel et bien une infinité." Nous démontrons ce résultat dans la Section 1.5. Mais ceci suscite une autre question. Je vous ai présenté les 14 plus petits nombres premiers ci-dessus : vous pouvez facilement compléter cette liste jusqu'à 30, par exemple. Si je désigne par p_n le n-ième nombre premier, on a $p_1 = 2, p_2 = 3, p_3 = 5, p_8 = 19, p_{14} = 43$ et $p_{30} = 113$. Existe-t-il une "formule" pour p_n ? Je veux dire par cela une règle qui permet de calculer p_n rapidement, sans tester successivement tous les nombres impairs pour voir s'ils sont premiers. Pour vous donner une idée de ce à quoi je pense, si vous me demandez quel est le n-ième nombre impair, je vous dis que c'est $2n + 1$: je n'ai pas besoin de calculer explicitement les 100 premiers nombres impairs pour trouver le 101-ième. Pour les nombres premiers, la situation est toute autre : il existe bien de telles formules, mais seulement depuis quelques années, et elles sont compliquées [De]. Ceci est dû essentiellement à la répartition très irrégulière des nombres premiers parmi tous les entiers : il n'y a, par exemple, que deux nombres premiers entre 10.000.000 et 10.000.100, mais il y en a 9 entre 9.900.900 et 10.000.000 (et il y en a 25 entre 0 et 100).

Sachant qu'il y a une infinité de nombres premiers, et qu'on n'a pas de formule pour les calculer, tournons-nous vers une nouvelle question, un peu moins ambitieuse. Pouvons-nous trouver une formule qui donne *approximativement* le nombre de nombres premiers inférieurs à un nombre réel positif x quelconque donné ? Cette fois-ci la réponse est "oui." On désigne par $\pi(x)$ le nombre de nombres premiers inférieurs à x : on a par exemple $\pi(10) = 4, \pi(100) = 25, \pi(1000) = 168, \pi(1.000.000.000) = 50.847.534$. Inutile de dire que ce dernier chiffre est obtenu à l'aide d'un ordinateur, qui a calculé tous les nombres premiers jusqu'à 1.000.000.000. La formule qui donne une approximation de $\pi(x)$, connu sous le nom de "Théorème des nombres premiers", est donnée par :

$$\lim_{x\to+\infty} \frac{\pi(x)}{\frac{x}{\ln x}} = 1. \tag{1.1}$$

Ceci veut dire que le quotient de $\pi(x)$ et de $x/\ln x$ est proche de 1 si x est pris suffisamment grand : en d'autres termes, $\pi(x)$, le nombre de premiers inférieurs à x, que je ne connais pas, n'est pas trop mal approximé par $x/\ln x$, si x est grand. Par exemple, on a [DH]

x	$\pi(x)$	$\frac{\pi(x)}{x/\ln x}$
10	4	$1,0856$
100	25	$0,8686$
1.000	168	$0,8617$
10.000	1.229	$0,8834$
100.000	9.592	$0,9043$
1.000.000	78.498	$0,9221$
10.000.000.000	455.052.512	$0,9544$
10^{20}	2.220.819.602.560.918.840	$1,0272$

Ici, pour constituer la colonne $\pi(x)$ un ordinateur a été utilisé pour calculer tous les nombres premiers inférieurs à x. Cela devient très dur à faire si x est grand : aujourd'hui, on sait à l'aide de puissants ordinateurs, calculer $\pi(10^n)$ jusqu'à $n = 20$. Pour plus d'informations sur les records du monde dans ce domaine, vous pouvez consulter le site internet http ://www.loria.fr/~ zimmerma/records/primes.html, où vous trouverez entre autres le plus grand nombre premier connu explicitement à ce jour (14/10/98) : c'est $2^{3021377} - 1$. Par contre, si $x = 10^n$, on a $x/\ln x = 10^n/n \ln 10$ et $\ln 10 = 2,30258\ldots$, comme vous le dira n'importe quelle calculette. On peut donc dire qu'il y a à peu près $10^n/n \ln 10$ nombres premiers inférieurs à 10^n, où le sens précis de "à peu près" est donné par (1.1). C'est en ce sens que nous avons une formule approximative pour le nombre de nombres premiers inférieurs à 10^n, *pour tout* n.

Le théorème des nombres premiers a été deviné par Gauss (il avait 15 ans, c'était aux environs de 1792) et démontré en 1896 par de la Vallée-Poussin et Hadamard. Il faut remarquer que la convergence de $\pi(x)$ sur $\frac{x}{\ln x}$ vers 1 n'est pas très rapide, puisque même pour $x = 10^{10}$, le quotient diffère de 5% de 1 et pour $x = 10^{20}$, l'erreur est encore de presque 3%. Des amélioriations considérables au théorème des nombres premiers ont été obtenues dans les cent dernières années.

Je me contenterai ici de ces quelques questions, mais il y en a beaucoup d'autres qui viennent naturellement à l'esprit quand on se met à réfléchir aux nombres premiers et la plupart n'ont pas trouvé de réponse à ce jour.

Ces questions sont-elles intéressantes ? Plus précisément, devraient-elles vous intéresser au point de vous inciter à continuer l'étude de ces pages ? La réponse à cette question-là dépend évidemment de vos goûts. La Question 1 relève du puzzle : si vous aimez les puzzles, vous trouverez sans doute cette question intriguante et elle peut suffire pour vous motiver à étudier un peu d'arithmétique. Il y a bien des façons d'aimer les mathématiques et c'en est une de les aborder par le biais de l'aspect jeu ou puzzle qui leur est propre. Au delà de cet aspect, je ne vois personnellement pas beaucoup d'intérêt à cette première question. Je ne vais en particulier pas prétendre qu'elle a un intérêt pratique. Par exemple, comme 2^{500} est plus grand que 10^{150}, une erreur dans le dernier chiffre décimal de ce nombre ne représente qu'une imprécision d'une part dans 10^{150}, ce qui est ridiculement petit. La seconde question a un petit côté pratique, ainsi qu'un aspect plus intellectuel. En effet, si l'on doit faire une division par trois (par exemple pour tester si un nombre est premier !) on peut savoir d'avance, et sans faire la division, par un petit calcul si on doit trouver un reste non nul ou non. C'est bien pratique et rassurant. Par ailleurs, se demander pourquoi la règle est vraie est déjà une préoccupation plus intellectuelle.

Les Questions 3, 4 et surtout 5 sont nettement plus profondes que les deux premières. Je prétends par exemple qu'il est impossible de comprendre les rudiments de l'analyse, sans avoir compris les réponses aux Questions 3 et 4. J'y reviendrai d'ailleurs dans le Chapitre 9. Enfin, la Question 5, elle, est très proche des préoccupations des mathématiciens professionnels qui s'intéressent aujourd'hui-même à la théorie des nombres. Même la démonstration du théorème des nombres premiers – pourtant vieille déjà d'un siècle – dépasse déjà nettement le cadre d'un cours de mathématiques de première année.

La plupart des mathématiciens professionnels seraient d'accord pour dire que les problèmes évoqués dans les Questions 4 et 5 sont de beaux problèmes de mathématiques. En général, ils aiment les mathématiques parce qu'ils y trouvent un plaisir esthétique et aussi parce que les strictes exigences de rigueur imposées aux raisonnements mathématiques donnent aux résultats obtenus une fiabilité et une sûreté inégalées et selon certains même un caractère de vérité absolue, universelle et éternelle. (Oui, oui, rien que ça !) Les preuves de l'irrationalité de $\sqrt{2}$ et de l'existence d'un nombre infini de premiers sont considérées comme de bons exemples de tels résultats [D][DH][H][P2]. Il y a par ailleurs beaucoup de gens qui aiment les mathématiques parce qu'elles leur fournissent un language et un outil de pensée permettant d'attaquer les problèmes non-mathématiques de leur intérêt, que ce soit dans les sciences fondamentales, l'économie, l'analyse numérique, le monde financier ou autre. J'en donnerai un premier exemple dans la Section 1.6, où j'expliquerai comment on utilise aujourd'hui des résultats sur les nombres premiers pour développer des codes secrets.

J'en termine là avec cette courte présentation de quelques raisons pour étudier l'arithmétique. Si vous constatez qu'aucune des questions évoquées ne vous intrigue, ni stimule votre curiosité, il y a de fortes chances pour que vous n'aimiez pas l'arithmétique, ni peut-être même les mathématiques. En supposant que ce n'est pas le cas, je vous invite à démarrer votre exploration du paysage mathématique.

Pour en savoir plus

Pour une analyse à la fois pertinente, pleine d'humour et non-technique du monde des mathématiques et des mathématiciens je vous recommande vivement de lire [DH]. Pour avoir une idée de la perception que les mathématiciens eux-mêmes ont de leur art, rien ne vaut la lecture de ce qu'ils en disent : [P2], [H] et [D]. Vous constaterez que les opinions divergent...

Les mathématiques développées dans la suite de ce chapitre sont traitées également dans le Chapitre 9 de [LM] et, avec moins de soin et de détails, dans le Chapitre 6 de [AA]. Vous trouverez aussi dans ces livres des exercices complémentaires, dont certains résolus. Un troisième livre très intéressant, du même niveau de ce cours, mais qui va plus loin dans la théorie des nombres est [DKM], dont les trois premiers chapitres couvrent exactement le programme du présent chapitre et qui contient également beaucoup d'exercices.

Finalement, un excellent livre "grand public" sur l'arithmétique, son histoire et ses applications est le récent livre de P.Delahaye [De] sur les nombres premiers.

Je vous encourage à consulter ces livres ainsi que d'autres que vous découvrirez en fouillant les rayons de la bibliothèque universitaire. Ils vous offrent un autre point de vue que le mien sur la matière, ce qui peut vous servir de deux façons. En effet, d'une part, si ma présentation ne vous convient pas, une autre vous conviendra peut-être mieux. Par contre, si ma présentation vous convient parfaitement, et si vous êtes sûrs d'avoir compris la matière, la lecture d'un autre texte sur le même sujet devrait être facile et constitue donc un excellent test du niveau de vos connaissances.

1.2 Divisibilité et congruence

1.2.1 Divisibilité

Pour fixer les notations et la terminologie, je vous rappelle qu'on désigne par $\mathbb{Z}$ l'ensemble de tous les entiers (qu'on appelle aussi les entiers relatifs) :

$$\mathbb{Z} = \{\cdots - 9, -8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, \ldots\}.$$

L'ensemble des entiers naturels est $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$, et par un entier positif on entend un entier naturel différent de 0. On désigne l'ensemble des entiers positifs par $\mathbb{N}^*$. De même, $\mathbb{Z}^*$ est l'ensemble des entiers relatifs différents de 0. Voici alors la première définition de ce chapitre :

Définition 1.1. *Soient a et b des entiers quelconques. On dit que a divise b si et seulement si il existe un entier k tel que l'on a*

$$b = ka. \tag{1.2}$$

Dans ce cas on dit aussi que b est un multiple de a, ou que a est un diviseur de b, ou encore que b est divisible par a. On écrit a/b lorsque a divise b.

Une définition est un énoncé qui définit des objets ou des notions mathématiques de façon précise. Ici, la notion en question est particulièrement simple. Ce ne sera pas toujours le cas... Illustrons rapidement comment on utilise cette définition pour montrer que 6 est un multiple de 2. On procède ainsi : $b = 6$ est un multiple de $a = 2$ parce qu'il existe un entier k, à savoir $k = 3$, tel que $b = ka$. De même, $a = 5$ divise $b = 125$ parce qu'il existe un entier k, à savoir $k = 25$ tel que $b = ka$. Finalement, 5 n'est pas multiple de 2 : ne dites jamais le contraire, en prenant $k = \frac{5}{2}$, parce que ce n'est pas un entier ! Bien sûr, tout ceci peut vous paraître d'une pédanterie excessive, mais je donne ces deux exemples pour vous faire remarquer que la valeur de k qui intervient dans (1.2) dépend de a et de b. On reverra ce phénomène de façon un peu moins triviale dans la démonstration du lemme suivant, qui rassemble quelques propriétés de base de la divisibilité.

Lemme 1.2. *Soient a, b, c et d des entiers. On a*

(i) Si a divise b et si b divise c, alors a divise c.

(ii) Si a divise b et si b divise a, alors $a = b$ ou $a = -b$.

(iii) Si $b \neq 0$ et si a divise b, alors $|a| \leq |b|$.

Avant d'en donner la démonstration, faisons une petite remarque : un lemme est un énoncé mathématique qui rassemble une ou plusieurs propriétés vraies des objets mathématiques préalablement définis. La même définition s'applique à une proposition ou à un théorème. La distinction entre les trois est donc purement qualitative. En général, on réserve le terme "théorème" pour des propriétés très importantes et/ou difficiles à établir : le théorème de Bézout (Section 1.4), le théorème des valeurs intermédiaires (Chapitre 8)), le théorème des accroissements finis (Chapitre 7), ... Les lemmes de ce livre rassemblent souvent des propriétés simples, voire presqu'évidentes, mais utiles pour la suite et donc tout de même importantes. Souvent les résultats des lemmes sont utilisés dans les démonstrations des théorèmes ; de cette façon, l'utilisation de lemmes permet de couper les démonstrations des théorèmes en petits morceaux, plus faciles à assimiler. Les propositions ont un statut intermédiaire entre celui des lemmes et celui des théorèmes.

La démonstration du Lemme 1.2 est très simple et ne nécessite rien d'autre qu'un appel à la définition de "divise." Elle vous fournit un premier exemple de rédaction d'un raisonnement complet.

Démonstration : (i) Il faut montrer que a divise c ou que c est un multiple de a, c'est à dire qu'il existe un entier k tel que $c = ka$. Selon l'hypothèse, a divise b et b divise c : il existe donc deux entiers k_1 et k_2 tels que $b = k_1 a$ et $c = k_2 b$. On conclut que $c = k_2 b = k_2 k_1 a$. Il existe donc bien un entier k tel que $c = ka$, à savoir $k = k_1 k_2$. Ceci termine la démonstration du point (i).

(ii) Il faut montrer que $|a| = |b|$, où $|\cdot|$ désigne la valeur absolue. Si a divise b, il existe un entier k tel que $b = ka$. Si b divise a, il existe un entier k' tel que $a = k'b$. Par conséquent

$$b = kk'b, \text{ ou encore } b(1 - kk') = 0.$$

Il y a alors deux possibilités. Soit $b = 0$; dans ce cas $a = k'b$ implique que $a = 0$ et donc que $a = b$. Soit $b \neq 0$, mais alors forcément $kk' = 1$ et donc $|k||k'| = 1$ (où $|\cdot|$ désigne la valeur absolue). Par conséquent, aucun des deux entiers naturels $|k|$ ou $|k'|$ n'est nul.

Je peux maintenant terminer la démonstration ainsi : comme il est clair que le produit de deux entiers positifs est égal à 1 si et seulement si chacun des deux entiers vaut 1, on a $|k| = |k'| = 1$. Par conséquent $|a| = |k'||b| = |b|$, ce qu'il fallait montrer.

(iii) Il existe k tel que $b = ka$ et donc $|b| = |k||a|$. Comme $b \neq 0$, on sait que $k \neq 0$. Donc $|k| \geq 1$, ce qui entraîne $|k||a| \geq |a|$ et par conséquent $|b| \geq |a|$. □

Avant de continuer, je vous fais encore remarquer que, dans la démonstration du point (i), j'ai appliqué trois fois la Définition 1.1, mais avec d'autres symboles : d'abord a, b et k_1, puis b, c et k_2, puis a, c et $k = k_1 k_2$. Ceci est à rapprocher de la remarque faite juste avant la démonstration.

1.2.2 Congruence

Le concept qui nous permettra de donner une réponse rapide aux Questions 1 et 2 de l'introduction est celui de congruence :

Définition 1.3. *Soit m un entier positif et soient a et b deux entiers. On dit que a est congru à b modulo m si et seulement si m divise $b - a$. On écrit alors*

$$a \equiv b \ [m]$$

A titre d'exemple, vous vérifierez facilement que $1 \equiv 7 \ [6]$, $3 \equiv 7 \equiv 11 \equiv -1 \ [4]$. Remarquez aussi que, d'un côté, on ne peut pas comprendre la définition de "congru" si on ne comprend pas celle de "divise," et que de l'autre, une fois qu'on a bien compris "divise," "congru" n'apporte rien de fondamentalement nouveau : il s'agit juste d'un peu de vocabulaire, qui permet de dire "a est congru à b modulo m," plutôt que "m divise $b - a$." On peut d'ailleurs s'étonner de me voir prétendre que c'est ce concept ultra-simple qui nous permettra de craquer le mystère du chiffre des unités de 2^{500} et de comprendre les "caractères de divisibilité." La clé des réponses réside dans la partie (iv) du Lemme 1.5 ci-dessous. D'abord, nous listons quelques propriétés élémentaires de la congruence, qui sont indispensables dans les calculs ultérieurs :

Lemme 1.4. *Soit m un entier positif. Soient a, b et c des entiers. On a*
(i) $a \equiv a \ [m]$.
(ii) Si $a \equiv b \ [m]$, alors $b \equiv a \ [m]$.
(iii) Si $a \equiv b \ [m]$ et $b \equiv c \ [m]$, alors $a \equiv c \ [m]$.

Je vous laisse la démonstration en exercice : elle est plus simple encore que celle du lemme précédent, ne nécessitant qu'un appel direct à la définition de "congru." Dans le jargon des mathématiciens, le lemme nous dit que la relation "congru" définit une "relation d'équivalence" : on en reparlera ultérieurement.

Lemme 1.5. *Soit m un entier positif. Soient a, b, c, d des entiers. On a*
(i) Si $a \equiv b \ [m]$, alors $a + c \equiv b + c \ [m]$.
(ii) Si $a \equiv b \ [m]$, alors $ac \equiv bc \ [m]$.
(iii) Si $a \equiv b \ [m]$ et $c \equiv d \ [m]$, alors $a + c \equiv b + d \ [m]$.
(iv) Si $a \equiv b \ [m]$ et $c \equiv d \ [m]$, alors $ac \equiv bd \ [m]$.
(v) Pour tout entier naturel n, on a la propriété suivante :

$$\text{Si } a \equiv b \ [m], \text{ alors } a^n \equiv b^n \ [m].$$

Ces deux lemmes montrent que la notion de "congru" se comporte un peu comme la notion "égale" et en particulier qu'on peut ajouter et multiplier "membre à membre". Faites néanmoins attention, tout n'est pas si rose, comme l'exercice suivant le montre.

Exercice 1.6. *L'affirmation suivante est-elle vraie ou fausse ? "Soit $m \in \mathbb{N}_*$, soient a et b des entiers. Alors $a \equiv b$ $[m]$ implique $a \equiv 0$ $[m]$ ou $b \equiv$ $[m]$."*

Solution : Eh bien, c'est faux ! En effet, il suffit de prendre $m = 6$, $a = 2$ et $b = 3$ pour s'en convaincre. Faites donc attention, tandis que, si le produit de deux entiers est *égal* à zéro, un des deux facteurs doit l'être, ce n'est pas parce que le produit de deux entiers est *congru* à zéro, qu'un des deux facteurs l'est. Nous verrons dans la Section 1.4.3 que ceci est dû au fait que 6 n'est pas un nombre premier.

Les démonstrations de (i)–(iv) sont à nouveau très simples, celle de (v) l'est déjà moins. Ceci est lié à l'observation suivante : le point (v) affirme qu'une certaine propriété est valable pour tout entier naturel, et donc le (v) contient une infinité d'affirmations, pour chaque choix de a, b et m. La démonstration du (v) fera appel au Principe de Récurrence, qui constitue un des arguments de preuve mathématique typiques et que nous rencontrons ici pour la première fois. Mais avant de vous présenter la démonstration de ce lemme, je vous montre comment le (v) permet de trouver la réponse aux Questions 1 et 2.

Exercice 1.7. *Trouver la réponse à la Question 1.*

Solution : On commence par remarquer que $34576 \equiv 6$ $[10], 57 \equiv 7$ $[10]$, et plus généralement que tout entier positif est congru modulo 10 au chiffre des unités dans son écriture décimale. Il s'agit donc pour nous de trouver l'entier entre 0 et 9 auquel 2^{500} est congru modulo 10 : ce sera forcément le chiffre recherché. Essayons :

$$2^1 \equiv 2 \ [10],\ 2^2 \equiv 4 \ [10],\ 2^3 \equiv 8, [10],$$

$$2^4 \equiv 6 \ [10],\ 2^5 \equiv 2 \ [10],\ 2^6 \equiv 4 \ [10],\ 2^7 \equiv 8 \ldots.$$

Ici, je n'ai pas encore utilisé le Lemme 1.5, mais j'ai obtenu ce résultat en inspectant le chiffre des unités des puissances successives de 2 : $2, 4, 8, 16, 32, 64, 128$ et ainsi de suite. Or, comme je l'ai expliqué dans l'introduction, je ne peux pas continuer ainsi, puisque les puissances de 2 devriendront rapidement trop longues à écrire. Le moment est alors venu de faire la remarque qui sauve : comme $2^5 \equiv 2[10]$, on peut appliquer le Lemme 1.5 (v) avec $a = 2^5, b = 2, n = 100$ pour obtenir $2^{500} \equiv (2^5)^{100} \equiv 2^{100}$ $[10]$. Le chiffre des unités de 2^{500} est donc le même que celui de 2^{100} et c'est un pas dans la bonne direction puisque 100 est nettement plus petit que 500, donc la puissance centième est moins difficile à calculer. Ce n'est néanmoins pas ce que je vais faire. Je préfère répéter l'argument pour obtenir :

$$2^{500} \equiv 2^{100} \equiv (2^5)^{20} \equiv 2^{20} \equiv (2^5)^4 \equiv 2^4 \equiv 6 \ [10].$$

Je peux maintenant conclure : comme 2^{500} est congru à 6 modulo 10, le chiffre des unités de 2^{500} est 6. Je vous fais remarquer une dernière fois que, pour obtenir ce résultat, je n'ai pas dû calculer 2^{500}. $\square$

Question : Le Lemme 1.4 a-t-il été utilisé quelque part ?

Je vous laisse cela en exercice et je passe maintenant à la démonstration du Lemme 1.5 :

Démonstration du Lemme 1.5 : Je ne fais pas la démonstration de (i)–(iv), que je vous laisse en exercice.

Pour le (v), il sera d'abord commode d'introduire la notation P_n pour l'affirmation

$$\text{“Si } a \equiv b\ [m], \text{ alors } a^n \equiv b^n\ [m]\text{”;} \tag{1.3}$$

Il faut donc montrer que, pour tout entier n, P_n est vrai. On le fera en trois étapes. La première consiste à remarquer que, clairement, P_1 est vrai. Dans la deuxième étape, on montre que, pour tout entier naturel k, la propriété suivante est vraie :

$$\text{“Si } a \equiv b\ [m] \text{ implique } a^k \equiv b^k\ [m], \text{ alors } a \equiv b\ [m] \text{ implique } a^{k+1} \equiv b^{k+1}\ [m]\text{”,} \tag{1.4}$$

c'est à dire que P_k implique P_{k+1}. On appelle ceci parfois la “propriété d'hérédité.” Je démontrerai (1.4) ci-dessous, mais je vais d'abord montrer comment on finit la démonstration de (1.3) pour tout n, sachant que (1.4) est vrai pour tout k. C'est la troisième et dernière étape du raisonnement par récurrence, celle précisément qu'on appelle le “Principe de Récurrence.” Soit n un entier quelconque. On sait que P_1 est vrai. On applique alors successivement (1.4) avec $k = 1$, puis $k = 2$, ...jusqu'à $k = n - 1$. On obtient ainsi successivement que P_1 implique P_2, puis que P_2 implique P_3, ..., puis que P_{n-1} implique P_n, ce qui finit la démonstration puisque P_1 est vrai.

Il nous reste donc à démontrer (1.4) pour tout k. Soit $k \in \mathbb{N}$. Supposons donc que $a \equiv b\ [m]$ implique $a^k \equiv b^k\ [m]$. Il faut montrer que $a \equiv b\ [m]$ implique $a^{k+1} \equiv b^{k+1}\ [m]$. Mais si $a \equiv b\ [m]$ et si $a^k \equiv b^k\ [m]$, alors le (iii) du Lemme implique tout de suite que $a^{k+1} \equiv b^{k+1}\ [m]$. □

Le mécanisme de cette démonstration est connu sous le nom de “raisonnement par récurrence.” Pour bien le comprendre, il est crucial de clairement voir la différence entre (1.3) et (1.4). La seconde de ces affirmations dit que, si la propriété recherchée est valable à un rang donné, elle l'est aussi au rang suivant : c'est la propriété d'hérédité. Ce n'est pas la même chose que de dire que la propriété est vraie pour tout n. C'est la troisième étape de cette démonstration qui est connue sous le nom de “Principe de Récurrence”. Comme le raisonnement par récurrence est utile dans beaucoup de situations différentes, il est important d'apprendre à le manier. Nous y reviendrons donc dans la Section 2.9, où je vous en présenterai d'autres applications.

Le lecteur s'entraîne :

1. Quel est le chiffre des unités de 3^{700} ?

2. Trouver tous les entiers naturels n tels que 7^n ait 5 comme chiffre des unités.

3. Trouver tous les entiers naturels n tels que 7^n ait 3 comme chiffre des unités.

4. Montrer que 13 divise

$$12^{3^{12^{3^{12}}}} + 3^{12^{3^{12^3}}}.$$

5. Trouver le plus petit diviseur de $3333^{4444} + 4444^{3333}$ qui est strictement plus grand que 1.

6.* Calculer la somme des chiffres de la somme des chiffres de la somme des chiffres de 7^{500}.

1.3 Le PGCD et la division euclidienne

1.3.1 Le Plus Grand Commun Diviseur

Je vais maintenant avancer un peu dans l'arithmétique, dans le but de répondre, dans la Section 1.5 aux Questions 2, 4 et (une partie de la) Question 5 de l'introduction, ainsi qu'à quelques autres en passant.

Définition 1.8. *Soient a et b des entiers non tous deux nuls. Le Plus Grand Commun Diviseur de a et b* (PGCD (a, b) *ou* $a \wedge b$) *est le plus grand entier positif qui divise à la fois a et b.*

Le PGCD (a, b) est donc le plus grand parmi tous les diviseurs positifs communs à a et à b. Quand un nouvel objet mathématique vous est proposé dans une définition, il faut toujours vous poser la question : existe-t-il ? Ici, il s'agit de comprendre si le PGCD existe toujours. C'est en effet le cas : tout d'abord 1 est toujours un diviseur commun à a et b, donc il y a des diviseurs communs. Puis, grâce au Lemme 1.2 (iii), nous savons que les diviseurs positifs communs à a et b sont tous inférieurs à $|a|$ si $a \neq 0$ et à $|b|$ si $|b| \neq 0$. Il y en a donc un nombre fini, et parmi un nombre fini d'entiers, il y en a un qui est le plus grand.

Question : Pourquoi avoir exclu, dans la définition ci-dessus, le cas $a = 0 = b$?

Pour tester si vous avez compris la définition, je vous invite à faire l'exercice suivant. Les démonstrations demandées ne font appel à rien d'autre qu'à la définition du PGCD et aux quelques propriétés simples de “divise” de la section précédente.

Exercice 1.9. *Montrer les affirmations suivantes :*

(i) Si $a \neq 0$, alors PGCD $(a, 0) = |a|$ *;*

(ii) Si a et b sont des entiers non tous deux nuls, alors PGCD $(a, b) =$ PGCD $(|a|, |b|)$ *;*

(iii) Si a divise b, alors PGCD $(a, b) = |a|$.

Quel est par exemple le PGCD $(18, -24)$? Pour le trouver, on pourrait d'abord faire la liste exhaustive de tous les diviseurs positifs de 18 : $1, 2, 3, 6, 9, 18$. Puis, celle de -24 : $1, 2, 3, 4, 6, 8, 12, 24$. On voit alors, par inspection, que PGCD $(18, -24) = 6$. Cette méthode n'a rien d'efficace : pour vous en convaincre, je vous invite à chercher ainsi le PGCD $(9724, 544)$. C'est encore un exemple où un peu de réflexion permet d'obtenir une réponse plus rapidement et plus facilement. Il existe en effet un algorithme de calcul de PGCD, l'algorithme d'Euclide, que j'expliquerai à la fin de cette section. D'abord, montrons la propriété suivante, qui est souvent utile et découle directement de la définition du PGCD.

Lemme 1.10. *Soient a et b des entiers non tous deux nuls. Soient a', respectivement b', les quotients de la division de a, respectivement de b, par le* PGCD (a, b). *Alors* PGCD $(a', b') = 1$.

Démonstration : C'est un bon exercice, qui vous permettra de tester si vous avez bien compris la définition de PGCD. Il faut montrer que PGCD $(a', b') = 1$, c'est à dire que 1 est le seul diviseur positif commun à a' et b'. Soit donc d un quelconque diviseur commun à a' et b' : on se propose de montrer qu'il vaut 1. Il existe des entiers k et ℓ tels que $a' = dk$ et $b' = d\ell$. Puisque par ailleurs $a = a'\text{PGCD }(a, b), b = b'\text{PGCD }(a, b)$, on en conclut que $a = kd\text{PGCD }(a, b), b = \ell d\text{PGCD }(a, b)$. Par conséquent, $d\text{PGCD }(a, b)$ est un diviseur positif commun à a et b. Il doit donc être plus petit que le PGCD (a, b) lui-même, ce qui entraîne que $d = 1$. □

1.3.2 La division euclidienne

Pour expliquer l'algorithme d'Euclide pour le calcul du PGCD, nous avons besoin du résultat suivant :

Proposition 1.11. (La division euclidienne) *Soient a un entier et b un entier positif. Alors il existe un unique entier q et un unique entier r tels que*

$$a = bq + r, \qquad 0 \leq r < b. \tag{1.5}$$

Démonstration : Comme $b \neq 0$, on peut considérer les multiples de b :

$$\cdots - 3b < -2b < -b < 0 < b < 2b, \ldots \ .$$

Il est alors clair que a se trouve entre deux multiples successifs de b : c'est à dire qu'il existe un unique entier q tel que $qb \leq a < (q+1)b$. Par conséquent $0 \leq (a - bq) < b$. En posant $r = a - bq$, on a donc

$$a = bq + (a - bq) = bq + r.$$

□

On appelle q le quotient et r le reste de la division euclidienne de a par b. Avant de présenter l'algorithme d'Euclide pour le calcul du PGCD, et en guise d'application de la division euclidienne et de la notion de "congru" , répondons à la Question 2.

Exercice 1.12. *Trouver la réponse à la Question 2.*

Solution : Rappelons d'abord que, quand nous écrivons 3756, nous pensons à

$$3756 = 3 \times 10^3 + 7 \times 10^2 + 5 \times 10^1 + 6 \times 10^0.$$

Plus généralement, en utilisant la division euclidienne, vous montrez facilement que tout entier $n > 0$ peut être écrit en forme décimale, c'est à dire qu'il existe un entier N et des entiers $0 \leq a_i \leq 9$ avec $a_N \neq 0$ tels que

$$n = a_N \times 10^N + a_{N-1} \times 10^{N-1} + \cdots + a_2 \times 10^2 + a_1 \times 10 + a_0.$$

On appelle les a_i les chiffres de (l'écriture décimale de) n ; a_0 est le chiffre des unités, a_1 le chiffre des dizaines, a_2 des centaines, etc.. Cette écriture est unique.

Par ailleurs, dire qu'un entier n est divisible par 3, c'est dire qu'il est congru à zéro modulo 3. De plus, pour tout k, $10^k \equiv 1[3]$. On en conclut que

$$n \equiv a_N + a_{N-1} + \cdots + a_3 + a_2 + a_1 + a_0 \ [3].$$

On voit donc que n est divisible par 3 si et seulement si la somme de ses chiffres est divisible par 3.

Le même type de raisonnement produit les caractères de divisibilité par $2, 4, 5, 8, 9$ et 11. En particulier, pour 11, il faut remarquer que $10^k \equiv (-1)^k \ [11]$. Pour 6, il faut réfléchir un peu...

Le lemme suivant, qui a l'air bien anodin, sera utile à plusieurs reprises dans la suite, et en particulier dans la deuxième version de la démonstration du Théorème 1.28.

Lemme 1.13. *Soient a un entier et b un entier positif. Le reste de la division euclidienne de a par b est nul si et seulement si b divise a.*

Démonstration : Si le reste est nul, (1.5) implique immédiatement que b divise a. Il reste à montrer que :

Si b divise a, alors le reste dans (1.5) est nul.

Si b divise a, alors il existe k tel que $a = bk$ ou encore $a = bk + 0$. Comparant à (1.5), et utilisant l'unicité de q et r, on conclut que $q = k$ et $r = 0$. □

1.3.3 L'algorithme d'Euclide

La clé de l'algorithme d'Euclide pour le calcul du PGCD réside dans le lemme suivant :

Lemme 1.14. *Soient a un entier et b un entier positif. Si r est le reste de la division euclidienne de a par b, alors* PGCD $(a, b) =$ PGCD (b, r).

Démonstration : La démonstration est très simple. Le PGCD (a, b) divise a et b, donc il divise $r = a - bq$. Le PGCD (a, b) est donc un diviseur à la fois de

b et de r, et il est donc forcément plus petit que le plus grand commun diviseur de b et de r :

$$\text{PGCD }(a,b) \leq \text{PGCD }(b,r).$$

Par ailleurs, le PGCD (b,r) divise b et r, et donc il divise aussi $a = bq + r$. Le PGCD (b,r) est donc un diviseur positif à la fois de b et de a, et il est donc forcément plus petit que le plus grand commun diviseur de b et de a :

$$\text{PGCD }(b,r) \leq \text{PGCD }(a,b).$$

De ces deux inégalités, le résultat s'ensuit. □

Algorithme d'Euclide : Soit a un entier et b un entier positif. Une méthode efficace pour déterminer le PGCD (a,b) est la suivante. D'abord, si b divise a, alors PGCD $(a,b) = b$ et on a fini. Si b ne divise pas a, la division euclidienne de a par b donne

$$a = bq_1 + r_1, \qquad 0 < r_1 < b.$$

On a, grâce au Lemme 1.14, PGCD $(a,b) =$ PGCD (b,r_1). Si r_1 divise b, on obtient ainsi PGCD $(a,b) = r_1$. Si non, on fait la division euclidienne de b par r_1 pour obtenir

$$b = r_1 q_2 + r_2, \qquad 0 < r_2 < r_1$$

et, grâce au Lemme 1.14 encore une fois

$$\text{PGCD }(a,b) = \text{PGCD }(b,r_1) = \text{PGCD }(r_1,r_2).$$

On continue cette opération, divisant à chaque fois le reste précédent par le nouveau reste, jusqu'à ce qu'un reste nul soit obtenu :

$$\begin{aligned}
r_1 &= r_2 q_3 + r_3, \qquad 0 < r_3 < r_2, && (1.6)\\
r_2 &= r_3 q_4 + r_4, \qquad 0 < r_4 < r_3, && (1.7)\\
\vdots &\ \vdots\ \vdots && (1.8)\\
r_{N-2} &= r_{N-1} q_N + r_N, \qquad 0 < r_N < r_{N-1} && (1.9)\\
r_{N-1} &= r_N q_{N+1}. && (1.10)
\end{aligned}$$

Comme les restes diminuent à chaque pas $(0 < r_N < r_{N-1} < \cdots < r_4 < r_3 < r_2 < r_1 < b)$, un reste nul est forcément obtenu après un nombre fini de divisions, que j'ai appelé $N+1$ ci-dessus. On a, utilisant le Lemme 1.14 de façon répétée

$$\begin{aligned}
\text{PGCD }(a,b) &= \text{PGCD }(b,r_1) = \text{PGCD }(r_1,r_2)\\
&= \ldots\\
&= \text{PGCD }(r_{N-1},r_N) = r_N.
\end{aligned}$$

J'ai utilisé ici, pour établir la dernière égalité, le résultat de l'Exercice 1.9. On obtient ainsi le PGCD (a,b) comme le dernier reste non-nul dans l'algorithme d'Euclide ci-dessus. Pour illustrer mes propos, je vous montre comment rapidement trouver le PGCD de 9724 et de 544. On a

$$\begin{aligned}
9724 &= 544 \times 17 + 476, \qquad \text{c'est à dire } a = 9724, b = 544, r_1 = 476;\\
544 &= 476 \times 1 + 68, \qquad \text{c'est à dire } b = 544, r_1 = 476, r_2 = 68;\\
476 &= 68 \times 7 + 0, \qquad \text{c'est à dire } r_1 = 476, r_2 = 68, r_3 = 0.
\end{aligned}$$

Vous remarquerez que les restes ont diminués très rapidement, de façon à ce que trois opérations ont suffi ($N = 2$) pour obtenir un reste 0. Le dernier reste non-nul est 68, qui est donc le PGCD $(9724, 544)$. C'est évidemment bien plus rapide que la recherche fastidieuse de tous les diviseurs de 9724, de tous ceux de 544, et la recherche parmi ceux-là du plus grand qu'ils ont en commun.

1.3.4 Efficacité de l'algorithme d'Euclide*

Peut-on prédire de combien de pas au plus on aura besoin dans l'algorithme d'Euclide avant de trouver le PGCD(a, b) $(a > b > 0)$? Dans les notations ci-dessus, la réponse est que

$$N + 1 \leq 2(\frac{\ln b}{\ln 2} + 1). \tag{1.11}$$

Cela veut dire que, si b est un nombre à 3 chiffres décimales, c'est à dire si b est au plus 999, au plus 22 pas seront nécessaires, et si b est au plus 999999, au plus 42 pas suffiront. Il est clair que c'est donc en effet une procédure très efficace puisque le nombre de pas ne croît pas très vite avec b. En effet, on constate que le nombre de pas est proportionnel au nombre de chiffres de b et pas à b lui-même ! Pour montrer (1.11), on remarquera d'abord que

$$r_2 \leq \frac{1}{2} b,$$

puis on montrera par récurrence que, pour tout n tel que $2n \leq N$, on a

$$r_{2n} \leq \left(\frac{1}{2}\right)^n b.$$

Si $N = 2K$ est pair, on en conclut

$$1 \leq r_{2K} \leq \left(\frac{1}{2}\right)^K b,$$

d'où $K \leq \frac{\ln b}{\ln 2}$ et donc (1.11). Lorsque $N = 2K + 1$ est impair, on a

$$1 \leq r_{N-1} = r_{2K} \leq \left(\frac{1}{2}\right)^K b,$$

et donc $N + 1 = 2(K + 1)$ avec la même conclusion.

Le lecteur s'entraîne.

1. Calculer PGCD$(5544, 1890)$ et PGCD$(3987, 324)$ en utilisant l'algorithme d'Euclide.

2. Montrer que, pour tout $n \in \mathbb{N}$, on a

$$\text{PGCD}(n, n+1) = 1 \text{ et } \text{PGCD}((n+1)^2, n+2) = 1.$$

1.4 Les théorèmes de Bézout et de Gauss

1.4.1 Le théorème de Bézout

Définition 1.15. *Soient a et b des entiers, non tous deux nuls. On dit qu'ils sont premiers entre eux si et seulement si* PGCD $(a, b) = 1$.

Il faut remarquer que cette définition n'introduit pas un nouveau concept, mais juste un peu de terminologie. Les mathématiques utilisent un vocabulaire riche et varié, parfois ésotérique, et il faudra que vous l'assimiliez au fur et à mesure que nous progressons. Une partie de l'apprentissage des mathématiques consiste donc bel et bien à apprendre un vocabulaire, exactement comme dans l'apprentissage d'une langue étrangère.

Nous en sommes arrivés maintenant au premier vrai théorème de ce cours, qui constitue la clé de voûte de ce chapitre.

Théorème 1.16. (Théorème de Bézout) *Soient a et b des entiers, non tous deux nuls. On a :*

(i) Il existe des entiers u et v tels que

$$au + bv = \text{PGCD } (a, b).$$

(ii) a et b sont premiers entre eux si et seulement si il existe des entiers u et v tels que

$$au + bv = 1.$$

(iii) Il existe des entiers u et v tels que

$$au + bv = c$$

si et seulement si le PGCD (a, b) *divise c.*

A moins que vous soyez particulièrement doués pour les mathématiques, la vérité des énoncés de ce théorème n'a rien d'immédiatement évident, contrairement à ce qui se passe pour la plupart des petites propriétés énoncées dans les lemmes précédents. C'est bien pour cela qu'il s'agit ici d'un théorème !

Afin de nous familiariser avec ce théorème, et avant de le démontrer, regardons un peu ce qu'il dit pour des valeurs particulières de a et de b. La partie (i) implique par exemple qu'il existe u et v tel que

$$4u + 10v = 2.$$

Ceci est en effet vrai puisque $u = -2, v = 1$ fait l'affaire. Remarquez qu'il y a d'autres possibilités : par exemple $u = 3, v = -1$ en est une autre. Plus généralement, dans les trois parties de ce théorème, l'existence *d'au moins un* couple d'entiers satisfaisant une certaine équation est affirmée mais rien n'empêche l'existence de plusieurs tels couples. Une autre façon de formuler le (i), par exemple, est de dire qu'il existe (au moins) une solution à l'équation $ax + by =$ PGCD (a, b) avec comme inconnus les entiers x et y. Le (iii) implique par ailleurs qu'il ne peut y avoir de u et v tels que $4u + 10v = 25$, tout simplement parce que 25 n'est pas un multiple du PGCD $(4, 10) = 2$.

Il y a beaucoup de théorèmes "d'existence" de ce style en mathématiques, et nous en rencontrerons encore un certain nombre dans ce cours. Une façon de démontrer un tel résultat est bien évidemment de calculer explicitement la solution, comme dans le cas $a = 4, b = 10$ ci-dessus. C'est rarement facile à faire. Dans le cas $ax + by =$ PGCD (a, b), un algorithme de calcul existe, et je vous le présenterai tout à l'heure. Mais d'abord, vous allez voir dans la démonstration du théorème 1.16 un premier exemple où l'on démontre l'existence de la solution, sans la calculer explicitement, c'est à dire sans proposer un algorithme de calcul. C'est assez étonnant, je pense, qu'une telle chose soit possible.

Démonstration : Soient a et b deux entiers non tous deux nuls. Introduisons le sous-ensemble de $\mathbb{Z}$, défini par

$$E_{a,b} = \{ax + by | x, y \in \mathbb{Z}\} = \{q \in \mathbb{Z} | \exists x, y \in \mathbb{Z}\,, q = ax + by\}.$$

Le symbole $\exists$ se lit "il existe". $E_{a,b}$ est donc constitué de tous les entiers de la forme $ax + by$, où x et y parcourent l'ensemble des entiers. Si vous n'êtes pas familier avec ces notations, je vous conseille de jeter d'abord un rapide coup d'œil sur la Section 2.10. De même, et bien que ce ne soit pas strictement nécessaire pour la compréhension du reste de la démonstration, il n'est pas inutile de se familiariser avec les ensembles $E_{a,b}$ en faisant l'exercice suivant :

Exercice 1.17. *(i) Déterminer* $E_{14,-6}$ *; montrer que les éléments de* $E_{14,-6}$ *sont précisément tous les nombres pairs.(ii) Soient* a *et* b *des entiers quelconques. Montrer que tous les multiples de* a *et de* b *appartiennent à* $E_{a,b}$*. Montrer que, si* c *appartient à* $E_{a,b}$*, alors tous les multiples de* c *appartiennent à* $E_{a,b}$*. Montrer que* $0, a, b, -a, -b$ *appartiennent tous à* $E_{a,b}$*.*

Retournons à la démonstration. Puisque $a, b, -a$ et $-b$ appartiennent tous à $E_{a,b}$ (Exercice 1.17), cet ensemble contient au moins un entier positif. Par conséquent, il contient un plus petit élément positif, que je désignerai par d (On a donc $d \geq 1$). Comme d appartient à $E_{a,b}$, la définition même de cet ensemble implique l'existence de deux entiers u et v tels que $d = ua + vb$.

Je vais d'abord montrer que $d =$ PGCD (a, b), ce qui implique (i). Dans ce but, faisons la division euclidienne de a et de b par d :

$$a = dq + r \quad 0 \leq r < d, b = dq' + r' \quad 0 \leq r' < d. \tag{1.12}$$

On en conclut que

$$r = a - dq = (1 - uq)a + (-vq)b, \text{ et } r' = (-uq')a + (1 - q'v)b,$$

ce qui montre que r et r' appartiennent à $E_{a,b}$. Mais r et r' sont des entiers naturels strictement plus petit que d (voir (1.12)), donc par la définition de d, ils sont forcément nuls ! On conclut alors de (1.12) que d est un diviseur commun à a et b. Se rappelant que d est positif, la définition même du PGCD entraîne

$$d \leq \text{PGCD } (a, b).$$

Par ailleurs, comme $d = ua + vb$, on voit facilement que le PGCD (a, b) divise d, donc (en utilisant le Lemme 1.2(iii)) que

$$\text{PGCD } (a, b) \leq d,$$

d'où l'on conclut en effet que $d = \text{PGCD } (a, b)$, ce qui termine la démonstration du (i).

J'enchaîne tout de suite sur le (ii). L'implication directe est une conséquence du (i) et de la définition de "premiers entre eux". L'implication réciproque dit que l'existence de u et v tels que $au + vb = 1$ implique que PGCD $(a, b) = 1$. Pour la montrer, il suffit de remarquer que l'hypothèse implique que 1 appartient à $E_{a,b}$ et donc que d, qui est le plus petit élément de $E_{a,b}$, vaut 1 : comme par ailleurs $d = \text{PGCD } (a, b)$, on en conclut que PGCD $(a, b) = 1$.

Finalement, pour le (iii), il suffit de remarquer deux choses. D'abord, si une solution existe, alors tous les diviseurs communs à a et b divisent c. Donc en particulier, PGCD (a, b) divise c. Par ailleurs, si c est un multiple du PGCD (a, b), alors il existe k tel que $c = k\text{PGCD } (a, b)$. Comme la partie (i) du théorème assure l'existence de deux entiers u' et v' tels que $au' + bv' = \text{PGCD } (a, b)$, on a $au + bv = c$ avec $u = ku'$ et $v = kv'$. □

Voici une première application du théorème de Bézout, qui sera importante dans le chapitre sur les polynômes :

Lemme 1.18. *(Caractérisation du PGCD) Soient a et b deux entiers, non tous deux nuls. Soit c un entier positif. Alors c est le plus grand commun diviseur de a et de b si et seulement si (i) c divise a et b et (ii) tout diviseur commun à a et b divise c.*

Exercice 1.19. *Montrer le lemme ci-dessus.*

1.4.2 Le théorème de Gauss

Le théorème de Bézout entraîne d'autres résultats importants, dont le premier est le théorème de Gauss.

Théorème 1.20. (Théorème de Gauss) *Soient a, b et c des entiers. Si a et b sont premiers entre eux et si a divise bc, alors a divise c.*

A nouveau, avant de passer à la démonstration, il est bon de tester l'énoncé avec des nombres concrets. Soient $a = 6, b = 5$ et $c = 42$, alors en effet a divise $bc = 210$, a et b sont premiers entre eux, et a divise c. Peut-on affaiblir les hypothèses ? Par exemple, si a divise bc et si a ne divise pas b, est-ce qu'alors

forcément a divise c ? Non ! Pour le voir, il suffit de trouver des valeurs de a, b et c pour lesquelles les hypothèses sont satisfaites, mais les conclusions sont fausses ; c'est ce qu'on appelle un *contre-exemple*. En l'occurence : $a = 6, b = 10, c = 21$. Remarquer que ce contre-exemple montre évidemment aussi que, si a divise bc, a ne divise pas forcément soit b, soit c, erreur très répandue parmi les débutants.
Démonstration : Comme a et b sont premiers entre eux, le théorème de Bézout implique l'existence de deux entiers u et v tels que $au + bv = 1$. Donc, en multipliant cette relation par c, on obtient $acu + bcv = c$. Par ailleurs, comme a divise bc, il existe un entier k tel que $ak = bc$. En insérant la dernière égalité dans la précédente, on obtient

$$a(cu + kv) = c.$$

Comme $cu + kv$ est un entier, ceci montre que c est un multiple de a, ce qui termine la démonstration. □

Vous voyez que la démonstration du théorème de Gauss n'est pas difficile, une fois qu'on dispose du théorème de Bézout. Nous utiliserons le théorème de Gauss dans la section suivante pour répondre aux Questions 4 et 5 de l'introduction.

1.4.3 Le lemme d'Euclide

Voici encore une variante du théorème de Gauss, connue comme le lemme d'Euclide, et souvent utile dans les applications :

Lemme 1.21. *(Lemme d'Euclide) Soit p un nombre premier et a, b des entiers. Si p divise ab, alors p divise a ou p divise b.*

Si vous ne vous souvenez pas de ce qu'est un nombre premier, consultez la Définition 1.27.

Exercice 1.22. *(i) Démontrer le lemme d'Euclide.* **Indication :** *Il faut remarquer que* $\mathrm{PGCD}(p, a) = 1$ *ou* $\mathrm{PGCD}(p, a) = p$*, puisque p est un nombre premier, puis utiliser le théorème de Gauss.*

(ii) Voici un autre résultat bien utile du même type que je vous invite à montrer : Soient k un entier positif, p un nombre premier et a un entier. Si p divise a^k, alors p divise a.

(iii) Montrer aussi cette variante du même résultat : Soit p un nombre premier et a, b, c des entiers. Si p divise abc, alors p divise a ou p divise b ou p divise c.

A partir de ce qui précède, il est clair qu'on peut généraliser le lemme d'Euclide de la façon suivante :

Si un nombre premier divise un produit d'entiers, alors il divise un des facteurs.

Cette formulation englobe à la fois le Lemme 1.21 et le (ii) et le (iii) de l'exercice. En effet, le produit peut contenir un nombre arbitraire de facteurs !

1.4.4 Le Plus Petit Commun Multiple

Le reste de cette section est consacrée à l'étude de quelques propriétés simples du Plus Petit Commun Multiple de deux entiers non nuls a et b. Cette notion ne jouera pas de rôle dans la suite de ce chapitre, et si vous êtes pressés de comprendre les réponses aux Questions 4 et 5, vous pouvez pour le moment laisser le reste de cette section pour y revenir plus tard.

Définition 1.23. *Soient a et b deux entiers non nuls. Le Plus Petit Commun Multiple de a et b (on écrit* PPCM*(a,b) ou $a \vee b$) est le plus petit entier positif qui est à la fois multiple de a et de b.*

On vérifie facilement que $\mathrm{PPCM}(18, 24) = 72$.

Question : Le $\mathrm{PPCM}(a, b)$ existe-t-il toujours quand a et b sont non nuls ? Pourquoi avoir exclu le cas où l'un des deux est nul ?

Lemme 1.24. *Soient a et b des entiers non nuls. Alors*

$$|ab| = \mathrm{PGCD}(a, b)\mathrm{PPCM}(a, b)$$

Démonstration : Comme $\mathrm{PGCD}(a, b) = \mathrm{PGCD}(|a|, |b|)$ et $\mathrm{PPCM}(a, b) = \mathrm{PPCM}(|a|, |b|)$, il suffira de montrer le résultat avec a et b positifs. Puisque $\mathrm{PGCD}(a, b)$ divise a et b, il divise ab : désignons par m le quotient de la division euclidienne de ab par $\mathrm{PGCD}(a, b)$:

$$ab = m\mathrm{PGCD}(a, b). \tag{1.13}$$

Il faut montrer que $m = \mathrm{PPCM}(a, b)$. Avec les notations du Lemme 1.10, nous avons $a = a'\mathrm{PGCD}(a, b)$ et $b = b'\mathrm{PGCD}(a, b)$, avec $\mathrm{PGCD}(a', b') = 1$. Donc,

$$m\mathrm{PGCD}(a, b) = ab = a'b'\mathrm{PGCD}(a, b)^2,$$

c'est à dire

$$m = a'b'\mathrm{PGCD}(a, b) = a'b = ab'.$$

On en conclut que m, défini par (1.13), est en effet un multiple positif commun à a et b. Il reste à montrer que c'est le plus petit. Soit m' un quelconque multiple positif commun à a et b. Alors, il existe des entiers k et ℓ tels que $ka = m' = \ell b$, d'où l'on tire $ka' = \ell b'$. Or, comme $\mathrm{PGCD}(a', b') = 1$, on en conclut, en utilisant le théorème de Gauss, que b' divise k et que a' divise ℓ. Par conséquent, on a $b' \leq k$ et donc $m' = ka \geq b'a = m$, ce qui termine la démonstration. □

On a aussi

Lemme 1.25. *(Caractérisation du* PPCM*) Soient a, b, c des entiers non nuls. Alors c est égal au* $\mathrm{PPCM}(a, b)$ *si et seulement si*
(i) c est un multiple commun à a et b,
et
(ii) tous les multiples communs de a et de b sont aussi des multiples de c.

Ceci est à comparer au Lemme 1.18.

Exercice 1.26. *Montrer le lemme.*

Le lecteur s'entraîne

1. (i) Calculer PGCD(18,385) par l'algorithme d'Euclide, et en déduire un couple $(u_0, v_0) \in \mathbb{Z}^2$ solution de l'équation $18u + 385v = 1$, avec$(u, v) \in \mathbb{Z}^2$. Fournir enfin l'ensemble des solutions entières de $18u + 385v = 1$.
(ii) Déterminer l'ensemble des solutions entières de $18u + 385v = 3$.
(iii) Déterminer l'ensemble des solutions entières de $54u + 1155v = 3$.
(iv) Déterminer l'ensemble des solutions entières de $54u + 1155v = 5$.

2. Résoudre, si possible, les équations suivantes : (i) $34x \equiv 7\ [4]$; (ii) $22x \equiv 33\ [5]$ mod 5.

3. Résoudre dans $\mathbb{Z}$ le système suivant :

$$\begin{cases} x \equiv 4 & [6] \\ x \equiv 7 & [9] \end{cases}$$

(On pourra commencer par chercher une solution particulière.)

4. Déterminer l'ensemble des entiers n tels que 17 divise $n^2 - 5n - 11$.

5. Redémontrer le Lemme 1.10 en utilisant le théorème de Bézout.

Dans les exercices 6 et 7 a et b désignent deux entiers non tous deux nuls.

6. Montrer que, si $n \in \mathbb{N}^*$, alors $\mathrm{PGCD}(na, nb) = n\mathrm{PGCD}(a, b)$.

7. (i) Montrer que, si $\mathrm{PGCD}(a, b) = 1$, alors

$$\mathrm{PGCD}(a, b^2) = 1 = \mathrm{PGCD}(a^2, b) = \mathrm{PGCD}(a^2, b^2).$$

(ii) En conclure que $\mathrm{PGCD}(a + b, a^2) = 1$.
(iii) Montrer que $\mathrm{PGCD}(a^2, b^2) = (\mathrm{PGCD}(a, b))^2$. (Même si $\mathrm{PGCD}(a, b) \neq 1$!)

8. Trouver des entiers naturels a et b entiers tels que
(i) $a + b = 2070$ et $\mathrm{PPCM}(a, b) = 9180$. **Indication :** On pourra utiliser le résultat de l'exercice 7(ii) ;
(ii) $a^2+b^2 = 5409$ et $\mathrm{PPCM}(a, b) = 360$. **Indication :** On pourra commencer par montrer que $\mathrm{PGCD}(a, b)$ divise PGCD(5409,360) et considérer ensuite différents cas.

9. Soient $a, b, c \in \mathbb{Z}$, tous non nuls.
(i) Soit $d_1 = a \wedge (b \wedge c)$. Montrer que d_1 divise $a \wedge b$ et c.
(ii) Soit $d_2 = (a \wedge b) \wedge c$. Montrer que d_2 divise $b \wedge c$ et a.
(iii) Montrer que $a \wedge (b \wedge c) = (a \wedge b) \wedge c$.
(iv) Montrer que $a \wedge (b \wedge c) = (a \wedge b) \wedge c$ est le plus grand des diviseurs commun à a, b et c.

10. Les affirmations suivantes, sont-elles vraies ou fausses ?
(i) "Soient $a, b, c \in \mathbb{Z}$; ab divise c si et seulement si a divise c et b divise c."
(ii) "Soient a, b des nombres premiers distincts et soit $c \in \mathbb{Z}$; ab divise c si et seulement si a divise c et b divise c."
(iii) "Soient a, b des nombres premiers et soit $c \in \mathbb{Z}$; ab divise c si et seulement si a divise c et b divise c."

1.5 Les nombres premiers

1.5.1 Combien y a-t-il de nombres premiers ?

Nous voilà prêts pour aborder les Questions 4 et 5 de l'introduction. Rappelons d'abord la définition de nombre premier.

Définition 1.27. *Un nombre premier est un entier strictement plus grand que* 1 *dont les seuls diviseurs positifs sont* 1 *et l'entier lui-même.*

Voici donc la première parcelle de réponse à la Question 5.

Théorème 1.28. *Il existe une infinité de nombres premiers.*

Je vais vous offrir trois démonstrations de ce résultat. Elles ne sont que des variantes l'une de l'autre, mais comme elles utilisent le déroutant raisonnement par l'absurde, il m'a paru utile de vous en présenter plus qu'une. Comme vous verrez, dans le raisonnement par l'absurde, on fait l'hypothèse que la propriété qu'on veut montrer est fausse, et on en déduit une affirmation (comme $1 = 0$, par exemple) qui contredit une propriété déjà connue (à savoir que $1 \neq 0$). On en conclut alors que l'hypothèse faite est fausse, c'est à dire que la propriété que l'on voulait démontrer est bien vérifiée. Je reviendrai en un peu plus de détail sur l'utilisation du raisonnement par l'absurde dans la Section 2.7, que vous pourriez éventuellement lire dès maintenant.

J'aurai, dans la démonstration, besoin du lemme suivant :

Lemme 1.29. *Tout entier plus grand que* 2 *a au moins un diviseur premier.*

Attention, pour éviter toute confusion, je vous signale que par "a est plus grand que b," j'entends $a \geq b$ et par "a est strictement plus grand que b," j'entends $a > b$. Le lemme affirme que, quelque soit $n \geq 2$, il existe un nombre premier qui divise n. C'est donc encore un résultat "d'existence". Etant donné un entier n, où trouver ce diviseur premier ? En prenant quelques exemples d'entiers, vous pouvez facilement constater que le plus petit diviseur positif plus grand que 2 de chacun d'entre eux est premier : pour 50, c'est 2, pour 63 c'est 3, pour 35, c'est 5 et ainsi de suite. L'idée de la démonstration sera précisément d'établir que le plus petit diviseur positif et plus grand que 2 de n'importe quel entier positif est toujours un nombre premier.

Démonstration : Soit n un entier plus grand que 2. Il a des diviseurs plus grand que 2, puisqu'il se divise lui-même. Considérons donc le plus petit diviseur positif de n qui est plus grand que 2, que je désignerai par d. On va montrer que d est un nombre premier. Soit d' un diviseur positif de d, différent de d ($d' \neq d$) ; il faut montrer que $d' = 1$. Comme d' divise d, il est alors strictement plus petit que d ($d' < d$) (Lemme 1.2(iii)) et il divise n. Mais un diviseur positif de n qui est strictement plus petit que d est forcément égal à 1, par la définition même de d.□

Démonstration du Théorème 1.28 :

Première version : Supposons qu'il n'y a qu'un nombre fini N de nombres premiers que je désignerai par $p_1, p_2, p_3, \dots p_N$. Considérons alors l'entier M défini par

$$M = p_1 p_2 p_3 \dots p_N + 1. \tag{1.14}$$

Comme $M \geq 2$, le lemme précédent garantit l'existence d'au moins un nombre premier p qui divise M. Par ailleurs, comme p est forcément égal à un des nombres premiers p_i, $(1 \leq i \leq N)$, on conclut que p divise $M - 1$. Par conséquent, p divise $1 = (1 - M) + M$. Nous avons donc établi l'implication suivante :

"S'il n'existe qu'un nombre fini de nombres premiers, alors il existe
alors il existe un entier plus grand que 2 qui divise 1."

Or, il n'existe pas de tel entier, donc il existe un nombre infini de nombres entiers.

Deuxième version : Je reprends la première version jusqu'à (1.14) et j'enchaîne de la façon suivante. Comme le reste de la division euclidienne de M par chacun des p_i est 1, aucun d'eux ne divise M (Lemme 1.13). Nous avons donc établi l'implication suivante :

"S'il n'existe qu'un nombre fini de nombres premiers, alors il existe
un entier plus grand que 2 qui n'a pas de diviseurs premiers."

Or ceci est en contradiction avec le Lemme 1.29.

Troisième version : Je reprends la première version jusqu'à "...d'au moins un nombre premier p qui divise M" et j'enchaîne de la façon suivante. Soit r le reste de la division euclidienne de M par p. Comme p divise M, $r = 0$. Par ailleurs, comme p est égal à un des p_i, on conclut de (1.14) que $r = 1$. On a donc montré que $0 = 1$. Ceci étant faux, on conclut qu'il existe un nombre infini de nombres premiers.

□

Il existe plusieurs autres variantes, dont une dans [AA] et une autre dans l'exercice suivant.

Exercice 1.30. *Montrer le Théorème 1.28 en montrant par récurrence que, pour tout entier positif n, on a*

P_n *: Il existe au moins n nombres premiers.*

Comme expliqué dans l'introduction, nous n'irons pas plus loin dans l'analyse de la Question 5. Pour avancer dans cette direction, vous pouvez consulter [DKM].

1.5.2 Le Crible d'Eratosthène

Avant de tourner mon attention vers la Question 4 de l'introduction, je vous donne un autre résultat utilisant le Lemme 1.29. Sa démonstration me donnera l'occasion de vous présenter, après les raisonnements par récurrence et par l'absurde, une troisième méthode de démonstration très utile et omniprésente : la démonstration par contraposition. Vous trouverez un peu plus de détails sur ces méthodes dans le Chapitre 2, que je vous recommande vivement de lire dès maintenant.

Lemme 1.31. *Soit n un entier plus grand que 2 $(n \geq 2)$: n n'a pas de diviseurs premiers plus petit que $\sqrt{n}$, si et seulement si n est un nombre premier.*

Démonstration : L'implication réciproque est évidente : si n est un nombre premier, son seul diviseur premier est n lui-même. Je vais montrer l'implication directe en démontrant sa contraposée, à savoir : "Si n n'est pas un nombre premier, alors n a au moins un diviseur premier plus petit que $\sqrt{n}$." Soit donc n un entier plus grand que 2 qui n'est pas un nombre premier. Soit d_1 le plus petit diviseur positif de n qui est plus grand que 2. La démonstration du Lemme 1.29 garantit que d_1 est premier et comme n n'est pas premier, on a $1 < d_1 < n$. On en conclut qu'il existe d_2 tel que $1 < d_1 \leq d_2 < n$ et $n = d_1 d_2$. Par conséquent $d_1^2 \leq d_1 d_2 = n$, d'où l'on conclut que d_1 est plus petit que $\sqrt{n}$. □

Le lemme est à la base d'un très ancien algorithme pour déterminer tous les nombres premiers inférieurs à un entier positif donné, "le crible d'Eratosthène". Supposons que nous voulions déterminer tous les nombres premiers inférieurs à 10^4. Procédons ainsi : nous écrivons d'abord la liste de tous les nombres impairs inférieurs à 10^4. Puis, nous rayons de la liste successivement tous les multiples de 3 sauf 3, puis tous les multiples de 5 sauf 5, puis tous les multiples de 7 sauf 7, et ainsi de suite jusqu'aux multiples de 97, dernier nombre premier inférieur à 100. Les nombres non-rayés sont tous des nombres premiers, selon le lemme précédent : en effet, ils n'ont pas de diviseur premier inférieur à $100 = \sqrt{10.000}$. Remarquez que, à chaque étape de l'algorithme, le premier nombre non-rayé est un nombre premier !

Le lemme nous fournit également, et par la même méthode, ce qu'on appelle un "test de primalité" : il permet de décider si un entier naturel donné est un nombre premier ou pas. Si l'entier en question est très grand, le test en question n'est pas très commode, parce qu'il demande trop de calculs, même pour un ordinateur.

Pour en savoir plus sur les différentes techniques permettant de tester la primalité d'un nombre ou de calculer des nombres premiers très grands, je vous renvoie à [De]. L'importance de ces deux problèmes deviendra plus clair lorsque je parlerai de cryptographie à clés publiques dans la Section 1.6.

1.5.3 Quels entiers ont une racine carrée rationnelle ?

Tournons maintenant notre attention vers la Question 4.

Théorème 1.32. *Soit p un nombre premier. Il n'existe pas de nombre rationnel dont le carré vaut p.*

Avant de démontrer ce résultat, je vais tenter de vous convaincre qu'il est vraiment très surprenant, et extrêmement difficile à croire. Ça vous motivera peut-être pour étudier très attentivement la démonstration : moins un résultat est évident, plus nous avons besoin d'une démonstration pour nous convaincre qu'il est vrai. La surprise provient du conflit entre l'assertion faite dans le théorème et notre intuition concernant les nombres rationnels. Si vous placez sur un intervalle de longueur 1 successivement les nombres rationnels

$$0, 1, 1/2, 1/3, 2/3, 1/4, 3/4, 1/5, 2/5, 3/5, 4/5, \ldots$$

et ainsi de suite, vous aurez l'impression de remplir complètement l'intervalle. Il est très difficile de s'imaginer qu'il y aurait des longueurs entre 0 et 1 que vous n'obtiendriez pas, pourvu que vous placiez des nombres rationnels avec des dénominateurs suffisamment grands. Or, selon le théorème ci-dessus c'est exactement ce qui se passe. En effet, il implique que $1/\sqrt{2}$ n'est pas rationnel et est donc une grandeur que vous n'obtiendriez pas. C'est pour cette raison-là qu'on est obligé d'élargir le concept de nombre au delà de celui de nombre rationnel, et d'introduire les nombres réels, dont nous reparlerons en détail dans les chapitres suivants.
Démonstration du Théorème 1.32 : Soit un nombre rationnel de la forme $\frac{a}{b}$, avec a un entier relatif et b un entier non-nul. Alors, avec les notations du Lemme 1.10, on a $\frac{a}{b} = \frac{a'}{b'}$, PGCD $(a', b') = 1$. Je ferai une démonstration par l'absurde. Supposons qu'il existe des entiers a' et b' tels que $(\frac{a'}{b'})^2 = p$, avec PGCD $(a', b') = 1$. Alors ${a'}^2 = p{b'}^2$ et donc p divise ${a'}^2$. Il en résulte, grâce au lemme d'Euclide (voir Exercice 1.22), que p divise a', c'est à dire qu'il existe un entier k tel que $kp = a'$. Par conséquent, $k^2p^2 = p{b'}^2$, et donc p divise ${b'}^2$. Une seconde application du lemme d'Euclide entraîne alors la conclusion que p divise b'. Or, le PGCD (a', b') étant 1, on en conclut que $p = 1$, ce qui contredit l'hypothèse que p est premier. □

Cette démonstration doit vous paraître bien courte, étant donnée l'importance que je semble attacher au résultat. Mais elle n'est pas courte : elle repose sur le lemme précédent qui, lui, utilise le théorème de Gauss, lui-même une conséquence du théorème de Bézout.

Voici un autre résultat intéressant, qui se démontre de façon assez analogue.

Exercice 1.33. *Montrer que, si $n \in \mathbb{N}$ est le carré d'un nombre rationnel, alors n est le carré d'un entier.*

Solution : Je ne donnerai qu'une esquisse de démonstration, à vous de fournir les détails. Si $n = \frac{a^2}{b^2}$ avec $\mathrm{PGCD}(a, b) = 1$, alors b^2 divise a^2 et donc $\mathrm{PGCD}(a^2, b^2) = b^2$. Il en résulte que $b = 1$.

1.5.4 La décomposition en nombres premiers

Un résultat important est le suivant :

Théorème 1.34. *Tout entier plus grand que 2 peut être écrit comme le produit de nombres premiers. A part l'ordre dans lequel les nombres premiers apparaissent dans le produit, cette écriture est unique.*

On a ainsi $26 = 2 \times 13 = 13 \times 2$ et $50 = 2 \times 5 \times 5 = 5 \times 2 \times 5$.
Démonstration : Je démontrerai d'abord l'existence d'une telle décomposition, utilisant un raisonnement par récurrence.

Je vais montrer, pour tout $n \in \mathbb{N}$, la propriété P_n suivante :

> Tout entier $2 \leq m \leq n$ peut être écrit comme le produit de nombres premiers.

Clairement, P_2 est vraie. Soit $k \in \mathbb{N}$ et supposons que la propriété P_k soit vérifiée. Considérons alors $k+1$. Nous savons que $k+1$ a un diviseur premier, donc $k+1 = p\ell$, avec p un nombre premier et $\ell \in \mathbb{N}$. Si $k+1$ est lui-même premier, on a $\ell = 1$ et la propriété P_{k+1} est vérifiée. Si $k+1$ n'est pas premier, alors $p < (k+1)$ et $2 \leq \ell \leq k$. L'hypothèse de récurrence P_k garantit alors que ℓ peut être écrit comme un produit de nombres premiers. On en conclut que $k+1 = p\ell$ est également un produit de nombres premiers, ce qui montre la propriété d'hérédité et finit la démonstration.

Démontrons maintenant l'unicité de la décomposition en nombre premiers d'un entier n. C'est (conceptuellement) un peu plus difficile. Soit p un nombre premier quelconque. Il existe clairement une plus grande puissance de p qui divise n. Notons-la p^k. Remarquez que k peut valoir 0 : c'est le cas lorsque p ne divise pas n. Par exemple, si $n = 60$ et $p = 5$, $k = 1$. Mais si $n = 60$ et $p = 2$, on trouve $k = 2$, et si $p = 7$, on a $k = 0$.

Supposons d'abord que $k = 0$. Cela signifie que p ne divise pas n. Il est clair qu'alors le facteur p ne peut intervenir dans aucune décomposition de n en nombres premiers. Supposons ensuite qu'au contraire, $k \geq 1$: p divise donc n. Mais alors le Lemme d'Euclide implique que p divise un des facteurs dans n'importe quelle décomposition en nombres premiers de n : p apparaît donc dans une telle décomposition avec une certaine puissance ℓ :

$$n = p^\ell q', \quad p \wedge q' = 1.$$

Clairement, on a $\ell \leq k$, puisque p^k est la plus grande puissance de p qui divise n. Mais comme, par sa définition même, p^k divise le produit $n = p^\ell q'$ et est premier avec q', le théorème de Gauss garantit qu'il divise p^ℓ. Donc $p^k \leq p^\ell$ et donc $k \leq \ell$. Par conséquent, $k = \ell$.

Nous avons donc démontré que, quelque soit p, il intervient dans toute décomposition en nombres premiers de n précisément avec l'exposant k défini ci-dessus. Cela démontre bien qu'il n'existe qu'une seule décomposition de cette sorte ! $\square$

Remarquons encore que la démonstration fournit une méthode pour trouver la décomposition en nombres premiers d'un entier quelconque. Il suffit de trouver, un par un, pour tous les nombres premiers p, l'exposant k et de multiplier les facteurs ainsi obtenus. Bien évidemment, il n'y a qu'un nombre fini de nombres premiers pour lesquels k est différent de 0. Cet algorithme peut donc être programmé sur un ordinateur.

1.5.5 Le petit théorème de Fermat

Le dernier théorème d'arithmétique que je vous inflige est le petit théorème de Fermat, qui est important dans la théorie des nombres et qui joue un rôle crucial dans la cryptographie à clés publiques, dont je vous dis quelques mots dans la section suivante.

Théorème 1.35. (Petit théorème de Fermat) *Soit p un nombre premier et x un entier quelconque. Alors*
$$x^p \equiv x\,[p]. \tag{1.15}$$
Si $x \not\equiv 0$ $[p]$, on a
$$x^{p-1} \equiv 1\,[p]. \tag{1.16}$$

Démonstration : Pour une démonstration élégante, je vous renvoie à [DKM]. Je me contenterai d'esquisser ici une démonstration utilisant la formule du binôme de Newton (2.7), démontrée dans la section 2.9. Je vous laisse le soin de donner les détails du raisonnement (que vous pouvez également trouver dans [LM]).

En remarquant que
$$C_p^\ell \ell!(p-\ell)! = p!,$$
une application judicieuse du lemme d'Euclide montre que p divise C_p^ℓ lorsque $1 \leq \ell < p$. La formule (2.7) avec $a \in \mathbb{Z}$ et $b = 1$ implique alors que
$$(a+1)^p - a^p \equiv 1\ [p].$$
Si x est un entier positif, le résultat (1.15) est ensuite obtenu en utilisant un raisonnement par récurrence sur a. Pour $x < 0$, il suffit de remarquer que $x = - \mid x \mid$.

Pour démontrer (1.16), on remarque que (1.15) implique
$$(x^{p-1} - 1)x \equiv 0,$$
d'où l'on conclut en utilisant encore une fois le lemme d'Euclide. □

Le lecteur s'entraîne

1. (Les nombres de Mersenne) Soient $p, q \in \mathbb{N}^*$. Montrer que $2^p - 1$ et $2^q - 1$ divisent $2^{pq} - 1$. En déduire que si $2^n - 1$ est premier, alors n est premier. Montrer que la réciproque est fausse, en prenant $n = 11$.

2. Soient p et q des nombres premiers distincts. Montrer que, si p et q divisent $c \in \mathbb{Z}$, alors pq divise c.

1.6 La cryptographie à clés publiques*

1.6.1 Introduction

La cryptographie est l'art ou la science de chiffrer des messages et de décrypter des textes chiffrés. Depuis très longtemps les militaires et les diplomates utilisent différents systèmes de chiffrement afin de protéger des informations sensibles de regards indiscrets. Un des points faibles (parmi bien d'autres) des systèmes classiques de chiffrement est que le déchiffrement est facilement fait par celui qui connaît la clé de chiffrement. Jules César, par exemple, chiffrait ses messages en remplaçant chaque lettre de l'alphabet par celle qui se trouvait 3 (ou 4, ou 5) places plus loin dans l'ordre lexicographique. Ainsi,

mdliurlgdxaslhgv

est en clair

J'ai froid aux pieds.

Il est évident que celui qui s'empare de la clé de chiffrement utilisée par César peut ensuite facilement décoder tous les messages de l'empereur. Il y a au moins deux façons d'obtenir la clé. La première consiste à analyser les messages cryptés et à essayer de retrouver la clé utilisée pour les crypter, c'est à dire à briser le code. Le chiffre décrit ci-dessus est bien évidemment assez naïf et on pourrait facilement le briser de cette façon. La deuxième consiste à mettre la main directement sur la clé de chiffrement, par exemple en faisant parler un des espions de César.... Ces dangers forcent César de changer de clé de chiffrement régulièrement et lui posent alors un autre problème : il doit communiquer la nouvelle clé à tous ses espions au plus vite, et ceci de façon sûre, c'est à dire, sans que la nouvelle clé soit interceptée par l'ennemi. Des systèmes de chiffrement bien plus sophistiqués que le chiffre de César décrit ci-dessus et très difficiles à briser ont été développés au fil des siècles, mais ils continuent néanmoins tous à souffrir de ce deuxième problème : si la clé de chiffrement tombe entre les mains de l'ennemi pendant sa transmission, celui-ci est en mesure de déchiffrer tous les messages cryptés avec la clé en question. Ce casse-tête a contrarié tous les services secrets à travers les siècles.

Dans les années 70, deux professeurs de Stanford University, W. Duffie et M.E. Hellmann et trois mathématiciens de MIT, R.L. Rivest, A. Shamir et L. Adleman (RSA) ont proposé une méthode de chiffrement qui court-circuite ces problèmes de façon spectaculaire. Il s'agit d'un système de chiffrement apparemment impossible à briser d'une part et dans lequel la clé utilisée pour chiffrer le message ne peut pas servir à le déchiffrer ! En d'autres termes, la clé de chiffrement (celle qui sert à transformer le message en clair en un charabia incompréhensible) ne permet pas de décoder un message chiffré ! Pour cela, il faut une clé complémentaire, la clé de déchiffrement. Par conséquent, le destinataire des messages chiffrés peut tout simplement rendre la clé de chiffrement public et il peut en particulier sans problème changer régulièrement de clé, sans que cela pose des problèmes de sécurité ! On parle donc dans ce contexte de *cryptographie à clés publiques*. Pour garder le secret des messages transmis, il suffit de conserver en lieu sûr la clé de déchiffrement. Il n'est en particulier jamais nécessaire de transmettre cette dernière aux émetteurs des messages, ce qui réduit de façon spectaculaire le risque qu'elle tombe dans des mains hostiles. Qu'une telle chose soit possible est difficile à s'imaginer, mais je vais vous en convaincre en vous montrant le système proposé par Rivest-Shamir-Adleman (RSA) : elle est basée sur quelques notions simples d'arithmétique et se sert en particulier du petit théorème de Fermat. Le génie des inventeurs de la cryptographie à clés publiques ne réside en effet pas dans la sophistication des outils mathématiques utilisés, mais dans le fait d'avoir imaginé la possibilité de créer un système de chiffrement asymétrique dans lequel la clé de chiffrement ne permet pas de déchiffrer les messages cryptés.

La prolifération des messages électroniques, les achats sur internet et les communications entre institutions financières ont fait exploser ces dernières décennies les besoins en cryptographie et ont fait sortir cette dernière du monde militaire et diplomatique. Quand vous faites par exemple un achat sur internet, votre numéro de carte bleue est crypté par un chiffre du type RSA. La cryptographie à clés publiques a en effet un autre avantage majeur sur les systèmes de chiffrement classiques qu'il est important de signaler. Si l'on utilisait un système de chiffrement classique, chaque client et chaque magasin proposant un article sur la toile devraient se mettre d'accord sur la clé à utiliser pour chiffrer le numéro de carte bancaire du client. Mais comment communiquer cette clé de façon sûre ? On pourrait s'imaginer une clé différente pour chaque couple fournisseur-client, qui serait communiquée une fois pour toutes par le fournisseur au client, via une lettre recommandée, par exemple. Avec un système de chiffrement à clés publiques, il suffit que chaque fournisseur dispose d'une seule clé de chiffrement, qui peut servir pour tous ces clients, et que le fournisseur peut rendre publique ! Cela réduit de façon considérable le nombre de clés différentes nécessaires et élimine bien des problèmes de logistique.

1.6.2 Le système RSA

On pourra s'imaginer que les messages que l'on souhaite transmettre sont des nombres M. On peut en tout cas transformer n'importe quelle phrase en un nombre en remplaçant les lettres par des entiers : $A \to 01, B \to 02$, *etc.*. Par exemple

$$1305201920051903012119190520200519$$

est le nombre M qui correspond au message

"Mets tes chaussettes."

Toute personne souhaitant recevoir des messages cryptés procède ainsi. Il choisit deux nombres premiers p et q distincts et les multiplie pour obtenir un nombre $N = pq$. Puis il choisit un entier $e > 1$ premier avec $m = (p-1)(q-1)$:

$$\mathrm{PGCD}(e, m) = 1.$$

Il rend ensuite les nombres N et e publics, les facteurs premiers p et q formant la partie privée de la clé. Toute personne souhaitant communiquer un message confidentiel à l'émetteur de la clé procède ainsi. Il calcule le message codé C à partir du message en clair M (qu'on supposera inférieur à N : $M < N$) en calculant le reste de la division euclidienne de M^e par N :

C est le reste de la division euclidienne de M^e par N, et donc $C \equiv M^e\ [N]$. Lorsque le message crypté est reçu par l'émetteur de la clé (N, e), il peut le décrypter à l'aide de la connaissance de p, q de la façon suivante. Il détermine d'abord (une fois pour toutes) un entier positif d tel que

$$de \equiv 1\ [m].$$

Remarquons que l'existence d'un tel nombre est garantie par le théorème de Bézout et qu'il peut être trouvé à l'aide de l'algorithme d'Euclide. Remarquons aussi que, pour déterminer d il faut connaître m, et donc p et q ! Le récepteur des messages qui ont été cryptés à l'aide de N et de e détermine finalement le message original M de la façon suivante :

M est le reste de la division euclidienne de C^d par N.

Pour montrer cette dernière affirmation, calculons $C^d \equiv M^{ed}\ [N]$. Comme $de \equiv 1\ [m]$, il existe un entier positif k tel que $de - 1 = km$ et par conséquent

$$C^d \equiv M^{ed} \equiv M^{1+k(p-1)(q-1)}\ [N].$$

Or, une application directe du théorème de Fermat révèle que

$$M^{1+k(p-1)(q-1)} \equiv M\ [p], \qquad M^{1+k(p-1)(q-1)} \equiv M\ [q],$$

quelque soit M. Une application du théorème de Gauss permet finalement de conclure que, comme q et p divisent $M^{1+k(p-1)(q-1)} - M$, il en est de même pour $N = pq$, d'où

$$C^d \equiv M^{ed} \equiv M^{1+k(p-1)(q-1)} \equiv M\ [N].$$

Comme M est inférieur à N, on a bien montré que M est le reste de la division euclidienne de C^d par N.

Exercice 1.36. *Compléter les détails du raisonnement ci-dessus.*

Pourquoi ce système de chiffrement est-il fiable ? En effet, si je rends public le nombre N, n'importe qui ne peut-il pas trouver les facteurs premiers de N, à savoir p et q, puis déterminer d tel que $de \equiv 1\ [m]$, et finalement calculer le reste de la division euclidienne de C^d par N pour trouver M ? La réponse à cette interrogation est : "En principe oui, en pratique non !" En effet, dans la pratique, on choisit pour p et q des nombres de l'ordre de 10^{100}, ce qui est facile à faire avec un ordinateur convenable. Le nombre N est alors de l'ordre de 10^{200}. Le secret de l'efficacité de l'algorithme RSA réside dans l'observation qu'on ne connaît pas d'algorithme de factorisation de nombres en facteurs premiers suffisamment efficace pour pouvoir factoriser un nombre de cette taille en un temps raisonnable, même à l'aide d'ordinateurs très puissants. En fin de compte, la connaissance de la clé de chiffrement, à savoir N et e suffit donc *en principe* pour déchiffrer les messages cryptés, mais en pratique il faut connaître également la partie privée de la clé, à savoir p et q. Une dernière remarque s'impose peut-être : il se peut qu'un tel algorithme ait déjà été trouvé par un service secret quelque part, au quel cas on peut être sûr qu'il sera gardé secret. En effet, le système RSA est très utilisé, et le détenteur d'un tel algorithme aurait accès à bien des informations confidentielles.

Pour voir comment ce système fonctionne, donnons un exemple. Il ne sera pas réaliste, puisque je prendrai $p = 7$, $q = 5$, donc $N = 35$. Clairement, si je rends $N = 35$ public, n'importe qui peut en déduire p et q, mais je veux ici simplement illustrer le mécanisme. On a $m = 24$, et je peux choisir $e = 55$. Je rends public $N = 35$ et $e = 55$, ce qui permet à qui le souhaite de m'adresser des messages cryptés. On vérifie facilement que, si $M = 2$, alors $C = 23$ et si $M = 7$, alors $C = 28$. Je vous laisse le soin de calculer, pour chaque valeur de M entre 2 et 34, la valeur correspondante de C. Pour que je décode les messages reçus, j'ai besoin de d : ici $d = 7$ convient puisque $de \equiv 7 \cdot 55 \equiv \cdot 7 \cdot 7 \equiv 1$ [24]. Un calcul confirme alors que $23^7 \equiv 2$ [35] et $28^7 \equiv 7$ [35], comme prévu.

Exercice 1.37. *On pourrait penser qu'il y a une autre façon de déjouer le système RSA. En effet, le codage consiste à remplacer chaque nombre M entre 1 et $N-1$ par un nombre C, lui aussi entre 1 et $N-1$, selon un algorithme rendu public. On pourrait alors s'imaginer calculer, pour chaque M possible, le C correspondant. Dès qu'on intercepte un C, il suffit alors de chercher dans la liste ainsi établie à quel M il correspond. Pourquoi ça ne marchera pas ?*

Pour en savoir plus : L'histoire de la cryptographie est merveilleusement décrite dans [S], qui se lit par endroits comme un vrai roman policier. Vous y apprendrez en particulier que la cryptographie à clés publiques avait été développée quelques années avant les équipes de Stanford et de MIT par les experts en cryptographie des services secrets britanniques, qui n'ont révélé cette information qu'en 1997. Pour des compléments d'information sur les mathématiques utilisées dans la cryptographie, je vous recommande vivement [C], qui traite la matière à un niveau tout à fait à votre portée. Pour en savoir plus sur la factorisation des grands nombres et la construction de grands nombres premiers, vous pouvez également consulter [De].

1.7 Les nombres : au delà de l'entier

Le nombre, et plus particulièrement le nombre entier, est sans nul doute l'objet mathématique par excellence. Beaucoup de non-mathématiciens pensent d'ailleurs que les mathématiques, c'est l'étude des nombres et que les mathématiciens ne font qu'une chose à longueur de journées : calculer. Du coup, ils ont beaucoup de mal à s'imaginer qu'on peut encore “trouver quelque chose de nouveau” en mathématiques. Cette impression est triplement fausse. D'abord, rares sont les mathématiciens qui calculent particulièrement bien : pour ne donner qu'un exemple, la plupart d'entre eux ont besoin d'une calculette pour trouver $\sqrt{342567}$. Ensuite, comme on l'a déjà signalé au début de ce chapitre, les entiers sont loin d'avoir livré tous leurs secrets. Finalement, à part les nombres, les mathématiciens professionnels étudient toute une pléthore d'autres objets mathématiques. Nous en rencontrerons quelques-uns dans ce cours, mais d'abord nous avons besoin d'approfondir le concept de "nombre" au delà de celui d'entier relatif.

Pourquoi le concept de nombre a-t-il besoin d'être élargi ? Vous savez sûrement que les mathématiciens passent beaucoup de temps à résoudre des équations de tout genre. En voici un exemple excessivement simple. Soit c un entier naturel ; trouvez un entier naturel x tel que

$$x + c = 0. \tag{1.17}$$

C'est évidemment impossible, vous me direz, sauf si $c = 0$, et dans ce cas il existe une solution unique $x = 0$. Mais qu'une équation aussi simple que celle-ci n'ait pas de solution n'est pas très satisfaisant, et c'est en partie pour pallier cette carence que les mathématiciens ont introduit, après quelques réticences, la notion d'entier relatif que nous avons déjà utilisée dans le Chapitre 1.

Je tiens à insister sur le fait que les entiers négatifs sont des objets beaucoup moins naturels que les entiers positifs. A 5 ans, un enfant maîtrise déjà raisonnablement bien le dénombrement d'une petite quantité d'objets (jusqu'à une vingtaine). Le concept de nombre négatif ne nous vient pas si facilement. Il n'intervient pas de façon naturelle dans la vie quotidienne et est introduit dans les cours de mathématiques au collège. S'il vous paraît simple aujourd'hui (enfin, je l'espère), ce n'est que parce vous l'avez manipulé pendant de longues heures au collège et au lycée. Par exemple, que 3 fois 5 vaut 15 semble tout à fait évident : si je vous donne 3 fois 5 pommes, vous en avez bel et bien 15. Mais pourquoi $(-3)(-5) = 15$? Aucune intuition provenant de la vie quotidienne ne permet de le comprendre. Les nombres négatifs n'interviennent dans la vie courante que dans le contexte bancaire (votre compte en rouge), sur l'échelle des températures (lorsqu'il fait froid) ou dans les parkings aux sous-sols. Dans aucun de ces contextes on n'a l'occasion de multiplier des quantités négatives. Les raisons pour lesquelles le produit de deux nombres négatifs est positif sont internes aux mathématiques : je ne m'y attarderai pas d'avantage.

Retournons maintenant aux équations et compliquons un peu les choses : existe-t-il un x dans $\mathbb{Z}$, tel que

$$bx + c = 0 \tag{1.18}$$

si b et c sont des entiers relatifs donnés ? L'équation

$$2x + 6 = 0$$

a une unique solution entière $x = -3$, tandis que

$$2x + (-1) = 0 \quad \text{ou} \quad 2x = 1$$

n'en a pas. Plus généralement, l'équation

$$b \cdot x = 1, \quad b \in \mathbb{Z}, \tag{1.19}$$

n'a jamais de solution x appartenant à $\mathbb{Z}$, sauf si b est égal à 1 ou -1. La situation est donc tout à fait analogue à celle rencontrée plus haut, lorsque nous cherchions à résoudre $x + c = 0$ ($c \neq 0$) avec x un entier naturel. Tout comme $x + c = 0$ ($c \neq 0$) n'avait pas de solution dans $\mathbb{N}$, $b \cdot x = 1$ ($|b| \neq 1$) n'a pas de solution dans $\mathbb{Z}$.

Pour régler ce problème, il suffit d'élargir une deuxième fois le concept de "nombre" et d'introduire l'ensemble $\mathbb{Q}$ des nombres rationnels. J'écrirai $r = \frac{p}{q}, (p \in \mathbb{Z}, q \in \mathbb{Z} \setminus \{0\})$ pour désigner un élément quelconque de $\mathbb{Q}$ et je vous rappelle que

$$\frac{p}{q} = \frac{p'}{q'} \quad \text{si et seulement si} \quad pq' = p'q.$$

Lorsque $\mathrm{PGCD}(p, q) = 1$, on dit que la fraction est simplifiée. Revenons alors à l'équation (1.19) : elle a une unique solution $x = 1/b$ appartenant à $\mathbb{Q}$, pourvu que $b \neq 0$. En généralisant un peu, on conclut maintenant facilement que toute équation (1.18), avec b et c appartenant à $\mathbb{Q}$, admet une unique solution rationnelle $x = -c/b$, pourvu bien sûr que $b \neq 0$.

Les rationnels ont une autre propriété que les entiers n'ont pas : entre deux rationnels distincts, il y en a toujours un troisième :

Soient $r_1, r_2 \in \mathbb{Q}$. Si $\quad r_1 < r_2 \quad$ alors il existe $\quad r_3 \in \mathbb{Q} \quad$ tel que $\quad r_1 < r_3 < r_2$.

Ça veut dire en particulier qu'on ne peut pas parler du "rationnel suivant", comme on peut parler de l'entier suivant : si n est un entier, $n+1$ est le suivant. Si vous représentez les entiers sur un axe, vous les placez à une distance fixe, les uns après les autres. Si vous essayez aussi de représenter les rationnels, vous aurez l'impression de remplir progressivement tout l'axe. Cette impression est néanmoins fausse, comme je vous l'ai déjà signalé dans le Chapitre 1 : il y a sur l'axe beaucoup de points qui n'ont pas de coordonnée rationnelle (beaucoup plus que de points ayant une coordonnée rationnelle !). Cette affirmation un peu vague est difficile à comprendre et sa signification n'a été clarifiée qu'au dix-neuvième siècle par de très grands mathématiciens après de considérables efforts. Vous n'avez donc pas à rougir si vous la trouvez bizarre ou mystérieuse. La comprendre complètement vous demandera à vous aussi beaucoup de travail. Une partie de ce travail sera fait dans le Chapitre 9, mais je veux tout de même vous donner immédiatement une indication de l'insuffisance des nombres rationnels.

Dans ce but, je poursuis ma pensée de tout à l'heure. Ayant constaté que je sais résoudre (1.18) complètement dans $\mathbb{Q}$, je me demande ce qu'il en est de

$$ax^2 + bx + c = 0, \tag{1.20}$$

où a, b, c appartiennent à $\mathbb{Q}$. En prenant deux exemples, je constate que

$$8x^2 - 6x + 1 = 0$$

a exactement deux solutions rationelles $x = \frac{1}{2}$ et $x = \frac{1}{4}$, tandis que

$$x^2 = 2 \tag{1.21}$$

n'a pas de solution rationnelle du tout : nous avons en effet montré plus tôt dans ce chapitre qu'il n'existe pas de nombre rationnel dont le carré vaut 2.

Cette observation nous fait tout de suite sentir qu'il faut élargir encore le concept de "nombre" au delà de celui de nombre rationnel pour incorporer les solutions de (1.21) et plus généralement de (1.20). Après tout, je n'ai certainement pas envie de faire des mathématiques sans "racine de deux", ne fût-ce que parce que je sais que l'hypothénuse d'un triangle rectangle de côtés 1 mesure $\sqrt{2}$ et je ne veux pas faire des mathématiques sans triangle. D'ailleurs, en dessinant un triangle rectangle comme dans la figure, on voit que le point C, qui est à distance $\sqrt{2}$ de l'origine, n'a donc pas de coordonnée rationnelle. Il en est de même pour $\sqrt{p}$, avec p un nombre premier.

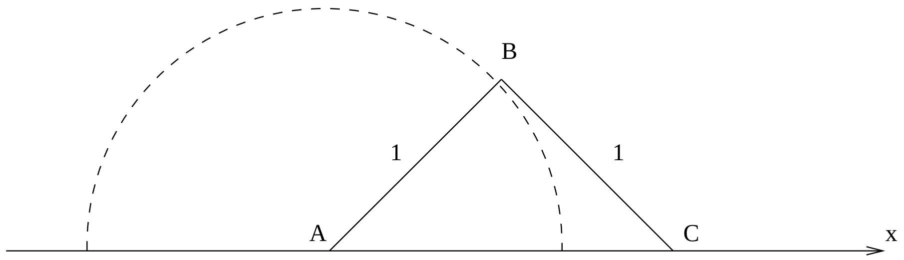

FIG. 1.1 – Peut-on vivre sans $AC = \sqrt{2}$?

Tout ceci nous amène donc à considérer l'ensemble des nombres réels $\mathbb{R}$, contenant, outre les nombres rationnels, les nombres "irrationnels" comme $\sqrt{2}$, $\sqrt{5}$, π, e, et bien d'autres encore. C'est précisément à l'ensemble $\mathbb{R}$ que Poincaré fait allusion quand il parle du "continu" dans la citation au début du Chapitre 9, où nous explorerons en plus de détail les subtilités de la notion de nombre réel. Vous pouvez pour le moment vous représenter les nombres réels comme les coordonnées des points sur un axe. Nous admettrons également pour le moment l'existence, pour tout nombre réel positif, d'une racine carré (cube, ...) positive.

Finalement, je signale que le problème de résoudre (1.20) n'est pas tout à fait réglé dans $\mathbb{R}$. En effet, il n'y a évidemment pas de nombre réel x tel que

$$x^2 = -1.$$

Pour avoir une solution à cette équation, il faudra encore élargir une dernière fois le concept de nombre en introduisant les *nombres complexes*. Ce sera fait dans le Chapitre 10.

Chapitre 2

Un peu de logique

Le génie est fait de 1% d'inspiration et de 99% de transpiration.
T. Edison

2.1 Introduction

Dans le mini-cours d'arithmétique du chapitre précédent nous avons établi quelques propriétés non-évidentes des entiers dont la plus surprenante est sans nul doute le Théorème 1.32. C'est probablement le seul résultat de ce chapitre dont on peut être tout à fait sûr que personne au monde ne l'a jamais trouvé évident. Si nous sommes néanmoins persuadés que ce théorème est vrai, c'est sans doute parce que nous pensons ne pas avoir fait de faute de logique dans sa démonstration. La logique est l'art de raisonner correctement ainsi que l'étude de cet art. C'est traditionnellement une branche de la philosophie. Le philosophe s'intéresse en effet à établir un savoir sûr et une base solide pour ses connaissances. L'art de raisonner correctement lui importe donc. Pour les mêmes raisons, la logique constitue également une branche des mathématiques. Je n'en dirai que quelques mots ici, sans entrer dans les détails, qui deviennent rapidement très compliqués.

Pour la suite de nos explorations, nous aurons besoin également de quelques éléments de la "théorie des ensembles." Il s'agit d'une théorie relativement difficile, faisant partie des fondements des mathématiques, mais dont nous ne visiterons que quelques lieux très faciles d'accès. Tout d'abord, pour nos besoins, il sera suffisant de définir un ensemble comme "une collection d'objets de notre perception ou de notre entendement" (Cantor) ou, plus simplement encore comme une "collection d'éléments ayant en commun certaines propriétés" (Robert). La Fédération Française du Tennis forme ainsi un ensemble dont les éléments sont ses adhérents. Cet ensemble ne nous intéressera pas davantage dans ce cours. Nous avons déjà introduit l'ensemble $\mathbb{N}$ des entiers naturels, l'ensemble $\mathbb{Z}$ des entiers relatifs, l'ensemble $\mathbb{Q}$ des nombres rationnels, l'ensemble $\mathbb{R}$ des réels et l'ensemble $\mathbb{C}$ des nombres complexes. Dans la suite, nous aurons principalement affaire à des ensembles construits à partir de ceux-là par des procédés très simples que je décrirai rapidement dans ce chapitre.

2.2 L'implication

Ce qui saute immédiatement aux yeux dans les énoncés de théorèmes, propositions et lemmes est leur structure en hypothèse – conclusion. On appelle "implication" une phrase qui a la structure "Si…, alors …" ou "…entraîne …" ou "…implique ….." Quand une telle phrase est-elle vraie ? Pour y voir clair, prenons un exemple non-mathématique. Supposons que je vous dis :

"Si je gagne au loto demain, je m'achète une belle voiture après-demain."

Pour que trois jours plus tard, vous ne puissiez me traiter de menteur, il faut qu'une des trois choses suivantes se soient passées. J'ai gagné (hypothèse vraie) et acheté (conclusion vraie), je n'ai pas gagné (hypothèse fausse) et tout de même acheté (conclusion vraie) ou je n'ai ni gagné (hypothèse fausse), ni acheté (conclusion fausse). C'est seulement si je gagne (hypothèse vraie) et que je n'achète pas (conclusion fausse) que vous pourrez me dire que j'ai menti. On en conclut en particulier qu'une implication est vraie, dès que l'hypothèse est fausse ! Dans cet exemple, cela paraît bien naturel, mais considérez donc l'implication :

"Si $2 = 3$, alors $3 = 4$."

En vertu de ce qui a été dit, elle est vraie ! Le débutant a souvent un peu de mal avec ça, parce qu'il ne fait pas la distinction essentielle entre "La conclusion est vraie" et "L'implication est vraie." Dans le cas présent, la conclusion est fausse, ainsi que l'hypothèse, mais l'implication, elle, est vraie !

Nous avons par ailleurs déjà rencontré de telles implications dans le chapitre précédent, sans que vous vous en êtes étonnés. Considérez par exemple le lemme d'Euclide (voir Exercice 1.22). En spécialisant au cas où $n = 2$ et $a = 3$, il dit

"Si 2 divise 9, alors 2 divise 3,"

ce qui est vrai, comme cas particulier du résultat

"Si p est un nombre premier qui divise a^n, alors p divise a."

En résumé, l'implication

"Si P, alors Q" est vraie si et seulement si Q est vraie ou P est fausse.

On dit que

"Si P, alors Q" est logiquement équivalent à "(non P) ou Q." (2.1)

Remarquons encore qu'on utilise souvent la notation $P \Rightarrow Q$ pour une implication, plus commode que "Si P, alors Q".

2.3 Le "ou" non-exclusif

Il faut comprendre ici que le "ou" en mathématiques n'est pas un "ou" exclusif : en mathématiques, on adopte la convention que l'affirmation "A ou B" est vraie lorsque un de ses deux membres *au moins* est vrai. Par exemple, si x est un entier, alors l'affirmation "$x \geq 0$ ou $x \leq 0$" est vraie ; si $x = 0$, on remarque qu'à la fois $x \geq 0$ et $x \leq 0$. Dans l'exemple avec le loto, l'implication est équivalente à : "Soit je ne gagne pas au loto demain, soit je m'achète une voiture après-demain," où il est entendu que les deux événements peuvent se produire simultanément. Il est un peu difficile de s'habituer à ce nouvel usage de "ou". Dans le language courant, "ou" est exclusif. Si je dis à mon fils le matin, en le déposant à l'école : "Ce soir, maman ou moi viendrons te chercher à la garderie," il sera surpris de nous voir arriver tous les deux parce qu'il interprète le "ou" comme étant exclusif.

2.4 La contraposée d'une implication

L'implication "Si P, alors Q" est également logiquement équivalente à sa contraposée, définie par "Si (non Q), alors (non P)" :

"Si P, alors Q" est logiquement équivalent à "Si (non Q), alors (non P)." (2.2)

Pour le voir, testons d'abord ce que ça donne pour le loto et la voiture : "Si je n'achète pas de belle voiture après-demain, je n'aurai pas gagné au loto demain." Il est clair que ceci est vrai si et seulement si l'implication originelle l'est. Plus formellement, on peut le voir aussi ainsi. L'implication "Si (non Q), alors (non P)" est, grâce à (2.1) logiquement équivalente à "non(non Q) ou (non P)," c'est à dire à "(non P) ou Q," qui est bien équivalent à "Si P alors Q," toujours selon (2.1). Cette observation est la base du raisonnement par contraposée, que nous avons déjà eu l'occasion d'utiliser dans la démonstration du Lemme 1.31, et que nous rencontrerons encore très souvent : quand on veut montrer "P implique Q," il est en effet parfois plus facile de montrer plutôt "(non Q) implique (non P)."

2.5 La négation

J'ai utilisé ci-dessus "non P" pour désigner la négation de P. Lorsque P est "Je gagne au loto," (non P) est "Je ne gagne pas au loto." En général, "non P" est l'affirmation qui est vraie lorsque P est fausse et vice-versa. Du coup, "non(non P)" est logiquement équivalent à P. Quelle est alors la négation de "P ou Q" ? Un moment de réflexion révèle que c'est "(non P) et (non Q)." En effet, pour que "P ou Q" soit fausse, il faut qu'à la fois P et Q soient fausses. On a donc :

"non(P ou Q)" est logiquement équivalent à "(non P) et (non Q)." (2.3)

De même, on a

"non(P et Q)" est logiquement équivalent à "(non P) ou (non Q)." (2.4)

Testons tout ceci sur un exemple. Imaginez-vous que j'arrive chez vous après un long voyage et que vous dites : "Vous avez sûrement faim et soif." Sur quoi je réponds laconiquement : “Non.” Que pouvez-vous logiquement conclure de cette réponse peu polie ? Seulement que je n'ai pas “faim et soif”, c'est à dire que je n'ai pas faim, mais peut-être tout de même soif, ou pas soif mais éventuellement faim, ou bien encore ni faim, ni soif. En d'autres termes, que je n'ai pas faim ou que je n'ai pas soif, avec un “ou” non-exclusif !

Essayons aussi de déterminer la négation d'une implication : “non(P implique Q).” Avec les règles établies, c'est maintenant facile. Etant donné (2.1) et (2.3), on a

$$\text{“non(P implique Q)” est équivalent à “P et (non Q)”.} \tag{2.5}$$

Testons cette règle sur le loto et la voiture. S'il n'est pas vrai que “Si je gagne au loto demain, je m'achète une belle voiture après-demain”, alors il est vrai que “Je gagne au loto et je ne m'achète pas de voiture.” De même, s'il est vrai que “Si je gagne au loto demain, je m'achète une belle voiture après-demain”, alors il est faux que “Je gagne au loto et je ne m'achète pas de voiture.” Remarquez que la négation d'une implication n'est pas elle-même une implication et en particulier n'a rien à voir avec “(non P) implique (non Q).”

2.6 L'implication réciproque – l'équivalence

Nous avons parlé d'implications, de leurs contraposées et de leurs négations. Reste à introduire l'implication réciproque de “P implique Q”, définie par “Q implique P.” On dit que “P est équivalent à Q” lorsque les deux implications “Si P, alors Q” et “Si Q, alors P” sont toutes les deux vraies. Vous vérifierez facilement que P est équivalent à Q est vraie lorsque P et Q sont deux affirmations vraies ou deux affirmations fausses. On dit aussi, pour plus de rapidité, “P si et seulement si Q” à la place de “P est équivalent à Q” et on note $P \Leftrightarrow Q$.

2.7 Le raisonnement par l'absurde I

Les résultats les plus intéressants du chapitre précédent ont été établis à l'aide du raisonnement par l'absurde, sur la structure duquel je voudrais brièvement revenir. Quand on veut démontrer une affirmation “P”, on peut procéder ainsi. On essaie de trouver une affirmation “Q”, qui est vraie, et on montre que “(non P) implique (non Q).” Par exemple, dans la première version de la démonstration du Théorème 1.28, l'affirmation Q est tout simplement “il n'existe pas d'entier plus grand que 2 qui divise 1.” Et dans la deuxième version de la démonstration du Théorème 1.28, l'affirmation Q est “tout entier plus grand que 2 a au moins un diviseur premier” : on sait qu'elle est vraie grâce au Lemme 1.29. Une fois qu'on a établi l'implication “(non P) implique (non Q)”, on a aussi sa contraposée, “Q implique P”, qui lui est logiquement équivalente. On peut alors conclure que, comme Q est vraie, P l'est aussi ! La difficulté dans l'utilisation de la démonstration par l'absurde réside partiellement dans le fait qu'à priori, on ne sait pas quel choix de Q sera utile : l'expérience joue un rôle évident ici et nous rencontrerons plein d'autres exemples du raisonnement par l'absurde dans la suite (Voir aussi la Section 4.10).

2.8 La rigueur en mathématiques

Je voudrais terminer cette section par une courte réflexion sur la "rigueur" à laquelle les mathématiciens sont tellement attachés.

Parmi les mots qui viennent le plus souvent à l'esprit lorsqu'on mentionne les mathématiques figure sans nul doute en première ligne le mot "axiome". Pourtant, je n'en ai nullement parlé jusqu'ici. Pour construire un raisonnement, il faut partir d'une hypothèse et enchaîner des implications pour aboutir à une conclusion. L'hypothèse elle-même peut déjà être la conclusion d'une autre chaîne d'implications, mais en remontant ces chaînes on aboutit forcément à une ou plusieurs hypothèses qu'on accepte sans chercher à les démontrer. Ce sont alors ce qu'on appelle les axiomes.

Quand un mathématicien parle de "raisonnement rigoureux", il entend par cela un raisonnement correctement construit dans lequel à chaque étape les hypothèses sont bien explicitées, et dans lequel aucune hypothèse implicite n'est jamais utilisée. Sur ce dernier critère, le présent texte est certainement défaillant, puisqu'il ne spécifie pas les axiomes sur lequel il se fonde. En effet, j'ai basé mes raisonnements sur certaines propriétés "évidentes" des entiers, sans toutefois les expliciter. Par exemple, étant donnés a, b, c des entiers, j'ai souvent utilisé que $a + b = b + a$, que $ab = ba$, que $(a + b)c = ac + bc$, ou que $a \leq b$ implique $a + c \leq b + c$, ainsi que quelques autres propriétés de ce genre. Je me suis ainsi également servi de l'égalité $a \cdot 0 = 0$ et du fait que $ab = 0$ implique que a ou b sont zéro. Dans la démonstration du Lemme 1.2 j'ai écrit :

> "...il est clair que le produit de deux entiers positifs est égal à 1 si et seulement si chacun des deux entiers vaut 1 ..."

sans pour autant démontrer cette affirmation. De même, dans la démonstration de la Proposition 1.11, j'ai annoncé de façon péremptoire que si a est un entier et si b est un entier positif, alors "il est clair que a se trouve entre deux multiples successifs de b." Vous pourriez ainsi vous amuser à faire la liste complète de toutes les propriétés des entiers que j'ai utilisées sans les démontrer. Elle n'est pas très longue. Si j'accepte ces propriétés comme axiomes, je pourrai prétendre que mon texte est devenu "complètement rigoureux", dans le sens donné à ce mot ci-dessus.

Il reste néanmoins un autre point à soulever. Il est à priori difficile de décider quelles propriétés des entiers on doit accepter comme axiomes et lesquelles peuvent alors être obtenues à partir de ceux-là via une preuve. Certainement, il ne faut pas prendre trop d'axiomes, pour deux raisons différentes. D'abord, certains pourraient alors être déduits des autres, et il ne serait ni élégant, ni intellectuellement satisfaisant de les inclure. C'est pour cette raison-là que j'ai choisi de démontrer les propriétés énoncées dans le Lemme 1.2, par exemple, même si elles sont certainement évidentes pour la plupart des gens. La seconde raison pour ne pas utiliser trop d'axiomes est qu'on risque d'inclure des propriétés contradictoires, sans s'en apercevoir. La question de savoir quel est l'ensemble minimal d'axiomes sur lesquels baser l'arithmétique, voire toutes les mathématiques, est une question difficile que je n'aborderai pas du tout.

Il faut sans doute une certaine maturité mathématique pour apprécier la problématique évoquée ci-dessus et j'aime bien citer H. Poincaré sur ce point [P1] : "Les débutants ne sont pas préparés à la véritable rigueur mathématique ; ils n'y verraient que de vaines et fastidieuses subtilités ; on perdrait son temps à vouloir trop tôt les rendre plus exigeants." En d'autres termes, la rigueur ne peut venir qu'avec l'expérience et est avant tout une question de profondeur de regard : plus on réfléchit, moins même les choses les plus simples paraissent évidentes et plus elles semblent nécessiter une démonstration. Si ces derniers paragraphes vous ont donc paru abscons, ne vous en inquiétez pas trop : vous pourrez très bien comprendre la suite de ce cours sans les avoir assimilés. Je ne les ai inclus que dans l'espoir d'éveiller votre curiosité.

Ceci dit, pour des étudiants de première année le problème de la rigueur se pose aussi de façon tout à fait concrète. Il se manifeste en effet de façon pressante lorsque, après le premier devoir surveillé, ils recoivent une copie corrigée couverte de rouge et de reproches d'un manque flagrant de rigueur et de précision. Ne devrait-on pas leur pardonner et faire preuve d'indulgence si même le professeur n'explicite pas toutes ses hypothèses et se cache derrière les paroles d'un grand mathématicien pour s'en excuser ? Sachez que les professeurs restent en général très raisonnables tant que les étudiants évitent d'admettre comme évidemment vrai ce qui est manifestement faux et tant qu'ils n'oublient pas que le manque d'imagination ne constitue jamais une preuve.

Pour en savoir plus : Une excellente introduction au raisonnement mathématique, avec beaucoup d'exercices et d'exemples montrant comment construire et rédiger correctement un raisonnement, se trouve dans les Chapitres 1 et 2 de [DV], dont je vous recommande l'étude vivement.

Si les questions des fondements des mathématiques vous intéressent, je vous conseille de consulter [H] et [Pe], qui sont d'excellents livres de vulgarisation sur le sujet.

2.9 Le raisonnement par récurrence : trois exemples

Le raisonnement par récurrence, que j'ai utilisé dans la démonstration du Lemme 1.5 (iv), est un outil efficace pour montrer des affirmations P_n, vraies pour tout entier naturel n à partir d'un certain rang N. Il est important d'apprendre à s'en servir, et ce n'est pas vraiment facile. Je vous donne encore trois exemples de son utilisation, après avoir fait quelques commentaires supplémentaires sur le principe de la démonstration.

Exercice 2.1. *(i) Montrer que, pour tout entier naturel $n \geq 5$, on a $2^n > n^2$.*

(ii) Montrer que, pour tout $x \in \mathbb{R}, x \neq 1$ et pour tout $n \in \mathbb{N}$, on a

$$1 + x + x^2 + x^3 + \cdots + x^n = \sum_{\ell=0}^{n} x^\ell = \frac{x^{n+1} - 1}{x - 1}. \tag{2.6}$$

(iii) Soient $a, b \in \mathbb{R}$. Montrer que, pour tout $n \in \mathbb{N}$, on a

$$(a + b)^n = \sum_{\ell=0}^{n} C_n^\ell a^\ell b^{n-\ell}, \tag{2.7}$$

où

$$C_n^\ell = \frac{n!}{\ell!(n - \ell)!}.$$

L'équation (2.7) est la formule du binôme de Newton. *Elle est souvent utile et il faut la connaître par coeur. La formule (2.6) est également très importante et à retenir par coeur.*

Il s'agit dans chaque cas de montrer une affirmation du type :

$$\text{“Pour tout entier naturel } n \geq N, P_n.\text{''} \tag{2.8}$$

Pour cela, on montrera :
(I) P_N est vraie ;
(II) Pour tout entier naturel $k \geq N$, on a : Si P_k, alors P_{k+1}.

On appelle le (I) l'étape d'initialisation de la démonstration et (II) la propriété d'hérédité. On peut alors montrer (2.8) comme dans le Lemme 1.5. Soit $n \in \mathbb{N}, n \geq N$. Si $n = N, P_N$ est vraie selon (I). Si $n > N$, on utilise d'abord (II) avec $k = N$ pour conclure que P_{N+1} est vraie. Puis, on utilise (II) successivement avec $k = N + 1, \ldots k = (n - 1)$ pour conclure que P_n est vraie.

Le fait que (I) et (II) impliquent (2.8) est ce qu'on appelle le Principe de Récurrence. En pratique, lorsqu'il faut montrer (2.8), on montre (I) et (II), puis on invoque simplement ce Principe pour conclure.

Voici trois exemples de rédaction.

Solution de l'Exercice 2.1 : (i) On utilisera le Principe de Récurrence. Il suffira donc de montrer :
(I) $2^5 > 5^2$;
(II) Pour tout entier $k \geq 5$, on a : Si $2^k > k^2$, alors $2^{k+1} > (k + 1)^2$.

Comme $2^5 = 32 > 25 = 5^2$, (I) est vraie. Démontrons (II). Soit un entier $k \geq 5$. Supposons $2^k > k^2$. On a

$$2^{k+1} = 2\ 2^k > 2k^2 = k^2 + k^2.$$

Par ailleurs, comme $k \geq 5$, on a $k^2 \geq 5k = 2k + 3k \geq 2k + 15 > 2k + 1$ et donc

$$2^{k+1} = 22^k > 2k^2 = k^2 + k^2 > k^2 + 2k + 1 = (k + 1)^2.$$

Ceci démontre le (II) et conclut la démonstration du (i).

(ii) Soit $x \in \mathbb{R}, x \neq 1$. Soit P_n l'affirmation suivante :

$$\sum_{\ell=0}^{n} x^{\ell} = \frac{x^{n+1}-1}{x-1}. \tag{2.9}$$

On utilisera le Principe de Récurrence. Il suffira donc de montrer :

(I) P_0 est vraie ;

(II) Pour tout entier naturel k, on a : Si P_k, alors P_{k+1}.

Comme $\sum_{\ell=0}^{0} x^{\ell} = x^0 = 1 = \frac{x^{0+1}-1}{x-1}$, (I) est vérifié. Démontrons (II). Soit un entier naturel k. Supposons que P_k soit vraie. On a

$$\sum_{\ell=0}^{k+1} x^{\ell} = \sum_{\ell=0}^{k} x^{\ell} + x^{k+1} = \frac{x^{k+1}-1}{x-1} + x^{k+1} = \frac{x^{k+2}-1}{x-1}.$$

Par conséquent, P_{k+1} est vraie, ce qui montre le (II) et conclut la démonstration du (ii).

(iii) Soient $a, b \in \mathbb{R}$. Soit P_n l'affirmation suivante :

$$(a+b)^n = \sum_{\ell=0}^{n} C_n^{\ell} a^{\ell} b^{n-\ell}, \tag{2.10}$$

On utilisera le Principe de Récurrence. Il suffira donc de montrer :

(I) P_0 est vraie ;

(II) Pour tout entier naturel k, on a : Si P_k, alors P_{k+1}.

Comme $\sum_{\ell=0}^{0} C_0^{\ell} a^{\ell} b^{0-\ell} = C_0^0 = 1 = (a+b)^0$, (I) est vérifié. Démontrons (II). Soit un entier k. Supposons que P_k soit vraie. On montre, après un assez long calcul qu'alors P_{k+1} est vraie, ce qui conclue la démonstration de (iii). On a :

$$\begin{aligned}
(a+b)^{k+1} &= (a+b)(a+b)^k = (a+b)\sum_{\ell=0}^{k} C_k^{\ell} a^{\ell} b^{k-\ell} \\
&= \sum_{\ell=0}^{k} C_k^{\ell} a^{\ell+1} b^{k-\ell} + \sum_{\ell=0}^{k} C_k^{\ell} a^{\ell} b^{k+1-\ell}.
\end{aligned}$$

En posant $\ell' = \ell + 1$ dans la première somme, et en remarquant que $\ell' = 1$ lorsque $\ell = 0$ et que $\ell' = k+1$ lorsque $\ell = k$, on obtient, pour cette première somme :

$$\begin{aligned}
\sum_{\ell=0}^{k} C_k^{\ell} a^{\ell+1} b^{k-\ell} &= \sum_{\ell'=1}^{k+1} C_k^{\ell'-1} a^{\ell'} b^{k+1-\ell'} \\
&= \sum_{\ell'=1}^{k} C_k^{\ell'-1} a^{\ell'} b^{k+1-\ell'} + a^{k+1}.
\end{aligned}$$

Pour la deuxième somme, on obtient, en posant $\ell' = \ell$:

$$\begin{aligned}\sum_{\ell=0}^{k} C_k^\ell a^\ell b^{k+1-\ell} &= \sum_{\ell'=0}^{k} C_k^{\ell'} a^{\ell'} b^{k+1-\ell'} \\ &= b^{k+1} + \sum_{\ell'=1}^{k} C_k^{\ell'} a^{\ell'} b^{k+1-\ell'}.\end{aligned}$$

En ajoutant les deux, on trouve

$$(a+b)^{k+1} = a^{k+1} + \sum_{\ell'=1}^{k} (C_k^{\ell'-1} + C_k^{\ell'}) a^{\ell'} b^{k+1-\ell'} + b^{k+1}$$

Un petit calcul supplémentaire permet alors de conclure que P_{k+1} est vraie, ce qui montre le (II) et conclut la démonstration du (iii).

Le lecteur s'entraîne

1. Montrer par récurrence, pour tout $n \in \mathbb{N}$:

$$(i) \quad 1 + 2 + \cdots + n = \sum_{k=1}^{n} k = \frac{n(n+1)}{2};$$

$$(ii) \quad 1 + 2^3 + \cdots + n^3 = \sum_{k=1}^{n} k^3 = \left(\frac{n(n+1)}{2}\right)^2;$$

2. Et voici, finalement, un exercice un peu plus déroutant. Que dire de l'affirmation suivante :

"Pour tout $n \in \mathbb{N}, n \geq 2$, on a : si $2^n > n^2$, alors $2^{n+1} > (n+1)^2$."

Est-elle vraie ou fausse ?

2.10 Sous-ensembles

Tournons-nous maintenant vers le langage ensembliste. La première construction d'ensemble à partir des ensembles de nombres $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ que nous connaissons déjà est celle, évidente, d'un *sous-ensemble*. Etant donné un ensemble, on construit un sous-ensemble en spécifiant la (les) propriété(s) commune(s) à tous ses éléments. Par exemple, les nombres premiers forment un sous-ensemble de $\mathbb{N}$. Un entier naturel y appartient s'il a les propriétés d'être strictement plus grand que 1 et de n'avoir comme diviseurs que 1 et lui-même. L'ensemble des entiers naturels inférieurs à 10 contient les nombres $0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10$. On l'écrit

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}.$$

En général, pour désigner un ensemble, on écrit ses éléments entre des accolades, mais il est rarement facile ou commode d'énumérer explicitement les éléments d'un ensemble, surtout lorsqu'il y en a une infinité. Une autre façon, plus efficace, de représenter l'ensemble ci-dessus est ;

$$\{n \in \mathbb{N} \mid n \leq 10\},$$

ce qui se lit "l'ensemble des n appartenant à $\mathbb{N}$, tel que n est inférieur à 10." L'ensemble des entiers pairs, par exemple, peut s'écrire

$$\{n \in \mathbb{Z} \mid 2/n\},$$

et ça se lit "l'ensemble des n appartenant à $\mathbb{Z}$ tel que 2 divise n." C'est, bien évidemment, un sous-ensemble de $\mathbb{Z}$. Un autre exemple est l'intervalle $[1, \pi]$, qui est le sous-ensemble de $\mathbb{R}$ constitué de tous les nombres réels entre 1 et π. Plus précisément, en utilisant les notations introduites,

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

En général, pour tout $a, b \in \mathbb{R}, a \leq b$, on définit

$$\begin{array}{rcl} [a, b] & = & \{x \in \mathbb{R} \mid a \leq x \leq b\} \\ [a, b[& = & \{x \in \mathbb{R} \mid a \leq x < b\} \\ ]a, b] & = & \{x \in \mathbb{R} \mid a < x \leq b\} \\ ]a, b[& = & \{x \in \mathbb{R} \mid a < x < b\}. \end{array}$$

On dira qu'un tel ensemble est un intervalle lorsqu'il n'est pas vide, ce qui peut arriver lorsque $a = b$: $]a, a[$, $[a, a[$ et $]a, a]$ sont par exemple vides. En effet, aucun réel x ne satisfait à la condition $a < x < a$ où à la condition $a < x \leq a$. Par contre, on a $[a, a] = \{a\}$, c'est à dire que $[a, a]$ contient exactement un élément, à savoir a. Un ensemble ne contenant qu'un élément est appelé un *singleton*. On définit aussi les intervalles "semi-infinis" suivants $(a, b \in \mathbb{R})$:

$$\begin{array}{rcl} [a, +\infty[= \{x \in \mathbb{R} \mid a \leq x\} & \text{et} &]a, +\infty[= \{x \in \mathbb{R} \mid a < x\} \\ ]-\infty, b] = \{x \in \mathbb{R} \mid x \leq b\} & \text{et} &]-\infty, b[= \{x \in \mathbb{R} \mid x < b\} \end{array}$$

On a finalement aussi $]-\infty, +\infty[= \mathbb{R}$, $]-\infty, 0] = \mathbb{R}^-$ $[0, +\infty[= \mathbb{R}^+$, $]-\infty, 0[= \mathbb{R}^-_*$, $]0, +\infty[= \mathbb{R}^-_*$ et $\mathbb{R}_* = \mathbb{R}^-_* \cup \mathbb{R}^+_*$.

En général, étant donné un ensemble E, pour désigner le sous-ensemble F des x appartenant à E qui satisfont une propriété $P(x)$, on écrit

$$F = \{x \in E \mid P(x)\}.$$

On dit : "L'ensemble F des x appartenant à E tels que $P(x)$ est vraie." Cette écriture met bien en évidence qu'un sous-ensemble est déterminé entièrement par la propriété commune à ses éléments. On écrit aussi $F \subset E$ lorsque F est un sous-ensemble de E.

S. De Bièvre

2.11 L'union et l'intersection

Une seconde construction très répandue est celle de l'union et de l'intersection de deux ensembles F_1 et F_2 donnés. L'union de F_1 et de F_2 est l'ensemble, noté $F_1 \cup F_2$, contenant tous les éléments de F_1 et tous les éléments de F_2. En particulier, si $F_1 \subset E$ et $F_2 \subset E$:

$$F_1 = \{x \in E \mid P_1(x)\}, \quad F_2 = \{x \in E \mid P_2(x)\}$$

on a

$$F_1 \cup F_2 = \{x \in E \mid P_1(x) \text{ ou } P_2(x)\}. \tag{2.11}$$

L'intersection de F_1 et de F_2 est l'ensemble, noté $F_1 \cap F_2$, contenant tous les éléments appartenant à la fois à F_1 et à F_2. En particulier, si $F_1 \subset E$ et $F_2 \subset E$ on a

$$F_1 \cap F_2 = \{x \in E \mid P_1(x) \text{ et } P_2(x)\}. \tag{2.12}$$

2.12 Le complément et les lois de de Morgan

Lorsque F est un sous-ensemble de E ($F \subset E$), le complément de F dans E, noté F^c, est l'ensemble de tous les éléments de E qui n'appartiennent pas à F. Plus formellement, avec les notations qu'on vient d'introduire, on obtient : si

$$F = \{x \in E \mid P(x)\},$$

alors

$$F^c = \{x \in E \mid \text{non } P(x)\} = \{x \in E \mid x \notin F\}, \tag{2.13}$$

où $\notin$ se lit "n'appartient pas à." Voici un lemme simple, mais important :

Lemme 2.2. *(Les lois de de Morgan) Soient F_1 et F_2 deux sous-ensembles d'un ensemble E. Alors*

$$(F_1 \cup F_2)^c = F_1^c \cap F_2^c \quad \textit{et} \quad (F_1 \cap F_2)^c = F_1^c \cup F_2^c. \tag{2.14}$$

Exercice 2.3. *Montrer le lemme en utilisant (2.3)-(2.4)-(2.11)-(2.12)-(2.13).*

2.13 Le produit cartésien

Le dernier concept dont nous aurons besoin est celui de produit cartésien, noté $F_1 \times F_2$, de deux ensembles F_1 et F_2. C'est l'ensemble dont les éléments sont les couples (x_1, x_2), avec $x_1 \in F_1$ et $x_2 \in F_2$. Par exemple, $\mathbb{R} \times \mathbb{R}$ est l'ensemble des couples (x, y) avec $x \in \mathbb{R}$ et $y \in \mathbb{R}$. Si $F_1 = F_2 = F$, on écrit $F^2 = F \times F$. De la même façon, on définit le produit cartésien $F_1 \times F_2 \times \cdots \times F_n$ de plusieurs ensembles $F_1, F_2, \ldots F_n$ comme l'ensemble des n-tuplets $(x_1, x_2, \ldots, x_n)$ tels que $x_i \in F_i, i = 1, \ldots n$.

2.14 La somme d'ensembles de nombres

Lorsque F_1 et F_2 sont des sous-ensembles de $\mathbb{N}$, de $\mathbb{Z}$, de $\mathbb{Q}$, de $\mathbb{R}$ ou de $\mathbb{C}$, on définit également

$$\begin{aligned} F_1 + F_2 &= \{x_1 + x_2 \mid x_1 \in F_1, x_2 \in F_2\} \\ &= \{x \in \mathbb{E} \mid \exists x_1 \in F_1, \exists x_2 \in F_2, x = x_1 + x_2\}. \end{aligned}$$

où j'ai écrit $\mathbb{E}$ pour désigner un des ensembles $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$. De façon analogue, lorsque F est sous-ensemble de $\mathbb{E}$, et $a \in \mathbb{E}$ on définit

$$aF = \{ax | x \in F\} = \{y \in \mathbb{E} \mid \exists x \in F, y = ax\}.$$

Voici quelques petits exercices pour vous habituer à ces notations et pour vous forcer de revoir le chapitre sur l'arithmétique.

Exercice 2.4. *(i) Soient*

$$\begin{aligned} F_1 &= \{x \in \mathbb{Z} \mid \ PGCD(x, 24) = 1\}, \\ F_2 &= \{x \in \mathbb{Z} \mid \exists u, v \in \mathbb{Z}, xu + 24v = 1\}, \\ F_3 &= \{x \in \mathbb{Z} \mid x \notin 3\mathbb{Z}, x \notin 2\mathbb{Z}\}. \end{aligned}$$

Montrer que $F_1 = F_2 = F_3$.

(ii) Soient $a, b \in \mathbb{Z}$*, non nuls. Montrer que*

$$a\mathbb{Z} + b\mathbb{Z} = \text{PGCD}(a, b)\mathbb{Z}, \qquad a\mathbb{Z} \cap b\mathbb{Z} = PPCM(a, b)\mathbb{Z}.$$

Solution : (i) Pour montrer que deux ensembles sont égaux, il faut montrer que le premier est un sous-ensemble du second et vice-versa.

Montrons ainsi que $F_1 = F_2$ en montrant successivement que $F_1 \subset F_2$ et que $F_2 \subset F_1$. Soit x un élément de F_1. Alors, $\text{PGCD}(x, 24) = 1$. Le Théorème de Bézout implique alors qu'il existe $u, v \in \mathbb{Z}$ tels que $xu + 24v = 1$. Donc $x \in F_2$. Ceci montre que $F_1 \subset F_2$. Soit maintenant $x \in F_2$. Il existe alors $u, v \in \mathbb{Z}$ tels que $xu + 24v = 1$. Le Théorème de Bézout implique alors que $\text{PGCD}(x, 24) = 1$. Donc $x \in F_1$. Ceci montre que $F_2 \subset F_1$.

Je vous laisse vous débrouiller pour montrer de la même façon que $F_2 = F_3$.

(ii) Montrons que $a\mathbb{Z} \cap b\mathbb{Z} = \text{PPCM}(a, b)\mathbb{Z}$ en montrant successivement que $\text{PPCM}(a, b)\mathbb{Z} \subset a\mathbb{Z} \cap b\mathbb{Z}$ et que $a\mathbb{Z} \cap b\mathbb{Z} \subset \text{PPCM}(a, b)\mathbb{Z}$. Soit $x \in \text{PPCM}(a, b)\mathbb{Z}$. Alors x est un multiple de $\text{PPCM}(a, b)$. Mais alors x est à la fois un multiple de a et de b, et donc $x \in a\mathbb{Z} \cap b\mathbb{Z}$. Par conséquent, $\text{PPCM}(a, b)\mathbb{Z} \subset a\mathbb{Z} \cap b\mathbb{Z}$. Soit maintenant $m' \in a\mathbb{Z} \cap b\mathbb{Z}$. Alors, le Lemme 1.25 implique que m' est un multiple de $\text{PPCM}(a, b)$, ce qui implique que $a\mathbb{Z} \cap b\mathbb{Z} \subset \text{PPCM}(a, b)\mathbb{Z}$.

Le lecteur teste ses connaissances
Les barêmes sur 15 sont donnés à titre indicatif
Interrogation Ecrite Arithmétique-Logique 1 – durée 1h30

I [2pt] Les affirmations suivantes sont-elles vraies ou fausses ($a, b, c \in \mathbb{Z}$) ?
- Si a ne divise pas b et a ne divise pas c, alors a ne divise pas bc.
- $\mathrm{PGCD}(a, b) = \mathrm{PGCD}(a^2, b)$

II [1pt] Enoncer le théorème de Gauss.

III (i) [3pt] Calculer le reste de la division euclidienne de 333333^{444444} par 2 et par 7.

(ii) [2pt] Déterminer si l'équation suivante a des solutions $u, v \in \mathbb{Z}$;

$$333333^{444444}u + 14v = 8.$$

Attention : on ne demande pas de trouver les éventuelles solutions.

IV [3pt] Montrer, en utilisant un raisonnement par récurrence, que, pour tout $n \in \mathbb{N}$, $2^n \geq n$.

V [4] Montrer qu'il n'existe pas de nombre rationnel dont la puissance cube vaut 2. En d'autres termes, montrer que $\sqrt[3]{2}$ n'est pas rationnel.

Interrogation Ecrite Arithmétique-Logique 2 – durée 1h30

I Soit p un nombre premier. Montrer les affirmation suivantes :
(i) [3pt] Pour tout $x \in \mathbb{Z}$ on a : $x^2 \equiv 1[p]$ si et seulement si $x \equiv 1\ [p]$ ou $x \equiv -1\ [p]$.
(ii) [2pt] Pour tout $a \in \mathbb{Z}, a \not\equiv 0\ [p]$, l'équation $ax \equiv 1\ [p]$ a des solutions entières.

II [7pt] Trouver toutes les solutions de

$$12345x \equiv 676\ [27].$$

Même question pour

$$12345x \equiv 678\ [27].$$

III [3pt] Montrer par récurrence que l'on a, pour tout $n \in \mathbb{N}$, (*Attention à la rédaction !*)

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

Interrogation Ecrite Arithmétique-Logique 3 – durée 1h30

I (i) [1pt] Enoncer le lemme d'Euclide.

(ii) [1pt] L'affirmation suivante, est-elle vraie ou fausse $(a, b, m \in \mathbb{Z})$? (Justifier sa réponse !)

Si $ab \equiv 0\ [m]$, alors $a \equiv 0\ [m]$ ou $b \equiv 0\ [m]$.

II [2pt] Calculer le reste de la division euclidienne de $3456^{7890^{1234}}$ par 13.

III Soient k, ℓ des entiers non tous deux nuls.

(i) [3pt] Montrer par récurrence ou autrement que l'on a, pour tout $n \in \mathbb{N}^*$,

$$\text{PGCD }(k, \ell) = 1 \Rightarrow \text{PGCD}(k^n, \ell) = 1.$$

Attention à la rédaction !

(ii) [1pt] Utiliser le résultat du (i) pour montrer que, pour tout $n \in \mathbb{N}^*$,

$$\text{PGCD }(k, \ell) = 1 \Rightarrow \text{PGCD}(k^n, \ell^n) = 1.$$

Indication : Pas besoin de récurrence !

(iii) [2pt] Soient a, b des entiers non tous deux nuls. Utiliser le résultat du (ii) pour montrer que, pour tout $n \in \mathbb{N}^*$,

$$\text{PGCD }(a^n, b^n) = (\text{PGCD }(a, b))^n .$$

Indication : Penser à écrire $a = \text{PGCD }(a, b)k$, $b = \text{PGCD }(a, b)\ell$.

IV [3pt] Montrer par récurrence que 7 divise $2^{2^{2n+1}} + 3$ pour tout $n \in \mathbb{N}$. *Attention à la rédaction !*

V [2pt] Trouver toutes les solutions de

$$23571x \equiv 12174\ [12].$$

Même question pour :

$$23571x \equiv 12172\ [12].$$

Chapitre 3

Fonctions : quoi et pourquoi ?

On n'exécute pas tout ce qui se propose,
Et le chemin est long du projet à la chose.
Molière, Le Tartuffe

3.1 Introduction

Avec ce chapitre commence le cours d'analyse où les objets d'étude principaux seront les fonctions numériques d'une variable. En caricaturant un peu, les deux messages principaux que je veux transmettre sont les suivants. D'abord, au delà des fractions rationnelles, les seules fonctions intéressantes sont celles qui sont la solution d'une équation différentielle intéressante. Deuxièmement, pour connaître une fonction, il ne suffit pas de savoir réciter sa définition ; on ne la connaît que lorsqu'on sait comment on peut calculer ses valeurs avec une précision arbitrairement grande. Pour illustrer ces propos, je donne tout de suite un exemple. Au lycée, on vous a appris que la fonction exponentielle est la fonction réciproque de la fonction logarithme, qui est elle-même l'unique primitive de $1/x$ qui vaut 0 en 1. Ceci est tout à fait correct, mais ne fournit aucun moyen pour calculer les valeurs de la fonction exponentielle et n'explique pas son intérêt. Celui-ci provient de l'observation que la fonction exponentielle est complètement caractérisée par le fait qu'elle est l'unique solution de l'équation différentielle

$$\frac{df}{dx}(x) = f(x) \tag{3.1}$$

qui vaut 1 en $x = 0$. La fonction exponentielle sert donc à décrire des grandeurs $f(x)$ dont le taux de variation $\frac{df}{dx}(x)$ est propertionnel à la grandeur elle-même. Par exemple, dans des modèles simples de croissance de populations bactériennes on suppose que la vitesse avec laquelle la population $p(t)$ change est proportionnelle à $p(t)$. On aura donc

$$p'(t) = kp(t) \tag{3.2}$$

où k est une constante de proportionalité. Il en résulte que la population croîtra de façon exponentielle, ce qui donne une bonne approximation de ce qui se passe en réalité, au moins pour des temps relativement courts.

3.1.1 Le banquier et l'équation différentielle

Publié dans :
« L'oral du Capes de mathématiques : Face au jury »(Ellipses 2007).

3.1.2 Tout est (presque) un polynôme

Commençons par rappeler que les seules fonctions facilement calculables à la main sont les polynômes (et les fractions rationnelles). Imaginez-vous alors que vous êtes confrontés au problème de trouver une solution à l'équation (3.1) et de la calculer. Le plus simple est alors de vérifier si il existe un polynôme

$$P(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_N x^N,$$

solution de (3.1) ? Insérant $P(x)$ dans (3.1), on trouve

$$a_1 + 2a_2 x + 3a_3 x^2 + \cdots + N a_N x^{N-1} = a_0 + a_1 x + a_2 x^2 + \cdots + a_N x^N$$

d'où l'on tire :

$$n a_n = a_{n-1}, 1 \leq n \leq N \text{ et } \ a_N = 0.$$

En choisissant a_0 de façon arbitraire on en conclut

$$a_n = \frac{a_0}{n!}, 1 \leq n \leq N \text{ et } \ a_N = 0,$$

ce qui implique malheureusement $a_0 = 0 = \cdots = a_N$. Il n'y a donc pas de solution polynomiale (non-nulle). Néanmoins, le calcul ci-dessus suggère de chercher une solution sous la forme d'une "somme infinie"

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n + \cdots = \lim_{N\to\infty} \sum_{n=0}^{N} a_n x^n. \tag{3.3}$$

En répétant le même calcul que ci-dessus vous trouverez facilement que les coefficients de la somme doivent être de la forme $a_n = \frac{a_0}{n!}$. Tout ceci *suggère* très fortement que la solution $f(x)$ de (3.1) satisfaisant $f(0) = 1$ devrait être

$$\lim_{N\to\infty} \sum_{n=0}^{N} \frac{x^n}{n!}. \tag{3.4}$$

Nous montrerons en effet dans le Chapitre 6 que cette limite existe et qu'elle est égale à la fonction exponentielle telle qu'introduite au lycée. Nous verrons en plus que les polynômes

$$P_N(x) = \sum_{n=0}^{N} \frac{x^n}{n!}$$

sont de bonnes approximations de la fonction exponentielle. Pour vous en convaincre dès maintenant, j'ai demandé à mon ordinateur de tracer le graphe de ce polynôme avec $N = 3$ ainsi que le graphe de la fonction exponentielle. Le résultat est reproduit dans la figure 3.1. Apparemment, mon ordinateur ne fait que très peu de différence entre les deux pour x compris entre -1 et 1. Sur l'échelle de la figure, on ne voit d'ailleurs aucune différence entre les deux graphes pour $|x| < 0,6$. Pour le dire encore différemment, l'approximation de la fonction exponentielle que calcule mon ordinateur lorsque je lui demande de tracer la fonction exponentielle ne diffère pas de façon appréciable de $P_3(x)$ sur cet intervalle. Au delà, les choses se gâtent, mais la figure 3.2 suggère qu'il suffit de prendre un polynôme $P_N(x)$ de degré N plus élevé pour avoir une bonne approximation sur un intervalle plus grand.

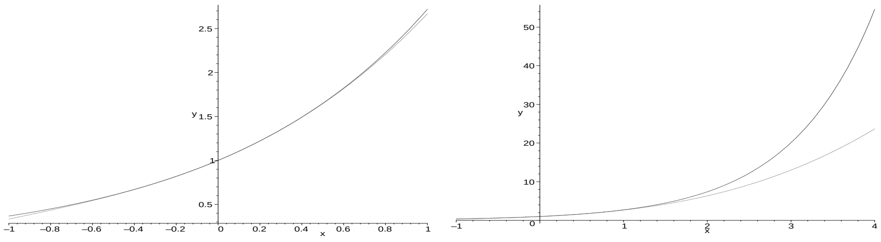

Fig. 3.1 – La fonction exponentielle (courbe du haut) et le polynôme $1 + x + \frac{x^2}{2} + \frac{x^3}{3!}$ (courbe du bas). Remarquer la différence d'échelle sur les deux dessins.

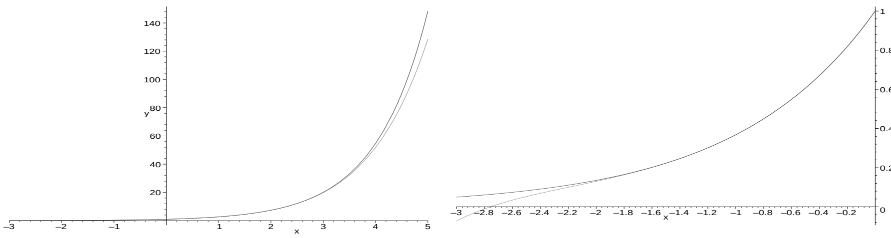

Fig. 3.2 – La fonction exponentielle (courbe du haut) et le polynôme $1 + x + \frac{x^2}{2} + \frac{x^3}{3!} + \cdots + \frac{x^7}{7!}$ (courbe du bas). Remarquer la différence d'échelle sur les deux dessins.

Comme $0,07$ est nettement inférieur à $0,6$, tout ceci suggère qu'on peut remplacer $\exp 0,07$ par $P_3(0,07)$ dans la formule pour votre dette et obtenir facilement, même sans calculatrice, une information nettement plus compréhensible sur votre dette :

"Après un an votre dette sera (approximativement) égale à

$5000P_3(0,07) = 5362,54\text{FF}$."

Vous constatez que les 362FF d'intérêts accumulés sont en effet supérieures aux 350FF d'intérêts qu'on aurait obtenus si on avait simplement calculé $5000 \times 0,07$. Ces 12 francs de différence peuvent vous paraître dérisoires, mais je vous invite à vérifier qu'on obtient des différences tout à fait importantes sur une période plus longue et/ou pour un capital initial plus conséquent. L'exercice qui suit vous propose quelques expériences permettant de comparer les $P_N(x)$ avec la fonction exponentielle.

Exercice 3.1. *(i) Demander à sa calculatrice la valeur de* $5000 \exp(0,07)$ *et de* $5000P_i(0,07)$ *pour* $i = 1,2,\dots 7\dots$ *et les comparer. Répéter l'expérience en remplaçant* $0,07$ *par d'autres valeurs, plus grandes. Qu'observe-t-on ?*

(ii) Tracer, à l'aide de sa calculatrice, sur un même graphique e^x *et* $P_1(x)$*, puis* e^x *et* $P_2(x), P_3(x)$ *etc. Qu'observez-t-on ?*

3.1.3 Retour chez le banquier

Publié dans :
« L'oral du Capes de mathématiques : Face au jury »(Ellipses 2007).

3.1.4 Les primitives existent-elles ?

Retournons alors à l'équation (**??**) et considérons le cas particulier où l'on prend $a(x) = 1, b(x) = 0$ pour obtenir

$$f'(x) = c(x). \tag{3.5}$$

Résoudre cette équation veut dire trouver une fonction f dont la dérivée est $c(x)$, ou encore, trouver une primitive de $c(x)$. Nous montrerons dans le Chapitre **??** que, si on sait résoudre (3.5) pour toute fonction $c(x)$, et si on sait résoudre (3.1), alors on sait résoudre toutes les équations du type (**??**). Il est donc important de savoir résoudre (3.5). Au lycée vous avez appris un certain nombre de techniques permettant de trouver les primitives d'une fonction c donnée, et nous reviendrons là-dessus dans les Chapitres 11 et **??**. Rappelons pour le moment que, si $c(x)$ est un polynôme, ceci est très simple à faire et f est alors aussi un polynôme, comme vous devriez être capable de vérifier facilement. Il est assez naturel de se demander ce qui se passe lorsque $c(x)$ est une fonction rationnelle. La situation est alors nettement moins simple. Premièrement, même si $c(x)$ est une fraction rationnelle, ses primitives ne le sont pas forcément. On montre par exemple facilement – Faites-le ! – qu'il n'existe pas de fraction rationnelle $f = P/Q$, telle que

$$(\frac{P}{Q})' = \frac{1}{x}.$$

On montre néanmoins – mais c'est loin d'être facile, et nous le ferons dans le Chapitre 11 – que $1/x$ a des primitives. Celle qui vaut 0 en $x = 1$ porte, depuis quelques siècles, le nom de "fonction logarithme".

Il y a d'autres fractions rationnelles dont les primitives ne sont pas des fractions rationnelles. Un exemple qui n'est pas traité au lycée est

$$f'(x) = \frac{1}{1+x^2}. \tag{3.6}$$

Aucune des méthodes enseignées au lycée permet de trouver la fonction f. L'exercice suivant suggère une méthode pour la trouver, au moins dans l'intervalle $-1 \leq x \leq 1$.

Exercice 3.2. *(i) Montrer que l'équation (3.6) n'a pas de solutions de la forme $f = P/Q$, avec P et Q des polynômes.*

(ii) Donner une expression pour les coefficients a_n pour que

$$f(x) = \lim_{N\to\infty} P_N(x), \ \textit{avec}\ P_N(x) = \sum_{n=0}^{N} a_n x^n, \tag{3.7}$$

puisse être une solution de (3.6).

(iii) Tracer, à l'aide de votre calculatrice, $P_1(x), P_3(x), P_5(x), P_7(x), \ldots$ pour $|x| \leq 0,5$. Répéter l'opération pour $|x| < 0,8$, puis pour $|x| < 1$ et pour $|x| < 2$. Faire d'autres expériences ; par exemple, calculer $P_i(0,5), i = 1,3,5,7,\ldots$. Même question pour $P_i(0,8)$ et $P_i(1,2)$. Qu'observe-t-on ?

(iv) Trouver une valeur approchée raisonnable pour l'aire sous le graphe de $\frac{1}{1+x^2}$ entre $x = -1$ et $x = 1$. La multiplier par 2. Deviner la valeur exacte de cette aire.

Solution : (i) Je vous laisse chercher. Quand nous aurons étudié l'arithmétique des polynômes au Chapitre **??**, ce sera très simple à démontrer.

(ii) Il suffit d'observer (utiliser l'Exercice 2.1 (ii)) que, pour $|x| < 1$,

$$\frac{1}{1+x^2} = \sum_{n=0}^{\infty} (-1)^n x^{2n}.$$

Un petit calcul montre alors que

$$a_{2n} = 0, a_{2n+1} = \frac{(-1)^n}{2n+1}.$$

(iii) Pour $-1 \leq x \leq 1$ on a l'impression que la suite $P_N(x)$ converge, mais si non elle semble diverger.

(iv) Il faut se souvenir du lien entre "primitive" et "aire". Vous avez appris au lycée que, si f est une primitive de $1/(1+x^2)$, alors l'aire en question est donnée par $f(1) - f(-1)$. Comme nous pensons que les polynômes trouvés ci-dessus devraient être de bonnes approximations de f pour $-1 \leq x \leq 1$, ceci vous suggère qu'une bonne approximation de l'aire en question est $P_N(1) - P_N(-1) = 2P_N(1)$. Il vous reste à programmer votre calculatrice pour qu'elle calcule $4P_1(1), 4P_3(1), \ldots 4P_N(1)$ et à deviner la limite de cette suite. Pour y voir clair, il est nécessaire de prendre N assez grand.

A part les fractions rationnelles, les fonctions exponentielle et logarithme, les seules autres fonctions que vous avez étudiées au lycée sont les fonctions trigonométriques, pour lesquelles on peut tenir un discours similaire : l'intérêt des fonctions sinus et cosinus provient principalement du fait qu'elles sont égales, à un signe près, à leur dérivée seconde. (Que les géomètres me pardonnent.) Elles sont donc des solutions de l'équation différentielle

$$f''(x) = -f(x). \tag{3.8}$$

Là aussi, je voudrais que vous preniez conscience du fait que – privés de calculatrices – vous ne disposez d'aucun moyen pour calculer leurs valeurs (Que vaut $\sin(1,2)$?). L'exercice suivant suggère une méthode pour y parvenir :

Exercice 3.3. *(i) Insérer une solution du type (3.3) dans (3.8) et montrer que les coefficients doivent satisfaire*

$$n(n-1)a_n = -a_{n-2}.$$

(ii) En déduire qu'il existe une unique solution f_1 à (3.8) telle que $f_1(0) = 1, f_1'(0) = 0$ et une unique solution f_2 telle que $f_2(0) = 0, f_2'(0) = 1$.

(iii) Tracer les polynômes qui sont des approximations de f_1 et de f_2. En déduire une façon de calculer les fonctions sinus et cosinus.

J'espère que cette longue introduction vous aura convaincu que les polynômes ont deux grands avantages. Ils sont faciles à calculer et on peut les utiliser pour reproduire à peu près n'importe quel comportement. On en a vu un premier exemple dans la figure 3.1-3.2 et si vous avez fait les exercices, vous en avez vu d'autres encore. Vous ne serez en particulier pas étonné si je vous dis que les deux graphes de la figure 3.3 sont des graphes de polynômes. Celui de

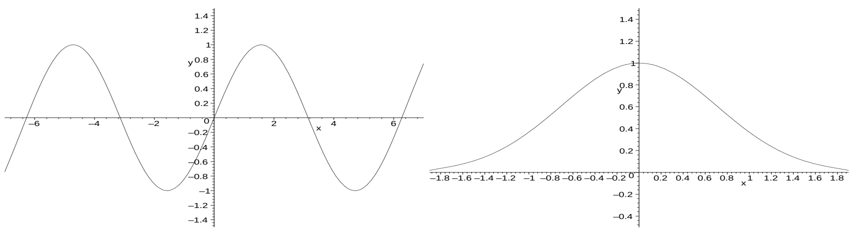

Fig. 3.3 – A quelles fonctions appartiennent ces graphes ?

gauche ressemble comme deux gouttes d'eau à celui que votre calculatrice produit lorsque vous lui demandez de tracer $\sin x$. Or, c'est le graphe du polynôme

$$x - \frac{x^3}{3!} + \frac{x^5}{5!} - \cdots + \frac{x^{17}}{17!}.$$

De même, le deuxième est le graphe du polynôme

$$1 - x^2 + \frac{x^4}{2!} - \cdots - \frac{x^{22}}{11!},$$

que je vous invite à comparer au graphe de $\exp -x^2$ tel que le dessine votre calculatrice. Nous montrerons plus tard que les polynômes en question sont en effet d'excellentes approximations de ces fonctions sur les intervalles considérés.

Exercice 3.4. *Expliquer la ressemblance entre le graphe de* $\exp -x^2$ *et du polynôme ci-dessus. (Indication : utiliser (3.4) ou remarquer que* $\exp -x^2$ *est une solution de l'équation* $f' = -xf$*.)*

3.1.5 Le programme

Les observations de cette introduction ne sont que spéculation, conjecture et présomption. Les transformer en théorèmes demandera un travail considérable. C'est la tâche du cours d'analyse, que nous entamons sérieusement dans le Chapitre 4 où la notion centrale sera celle – difficile – de limite d'une fonction en un point x_* de son domaine (Sections 4.1-4.2-4.8). Elle nous permettra de définir et d'étudier la continuité et la dérivabilité (Chapitre 5), puis de nous acheminer lentement vers le véritable but de ce cours, qui est le Chapitre **??**. J'introduirai aussi dans le Chapitre 4 les premières notions concernant les suites (Sections 4.5-4.6).

Pour mener à bien ce programme, nous aurons besoin d'un langage suffisamment riche et précis pour décrire le "comportement" des fonctions. Quelques éléments de ce langage sont rappelés rapidement dans la suite de ce chapitre. Comme les exemples que j'ai donnés le montrent, les fonctions servent à décrire des grandeurs qui dépendent d'un paramètre. Ce paramètre est souvent le temps, mais peut être un paramètre de contrôle. Par exemple, le nombre de cigarettes N fumées en France chaque année dépend de leur prix P. Il décroît lorsque le prix augmente. Le prix est un exemple de ce que j'ai appelé un paramètre de contrôle : le gouvernement peut contrôler dans une certaine mesure le prix par le biais des taxes sur le tabac et ainsi agir sur la consommation (et, bien sûr, sur son propre revenu ...). Connaître le comportement de la consommation en fonction du prix est donc important pour lui.

Il est utile de distinguer le comportement global, le comportement local et le comportement asymptotique ("à l'infini") d'une fonction. Par le comportement local d'une fonction j'entends le degré de régularité de la fonction. Fait-elle des sauts (continuité), admet-elle une tangente (dérivabilité) ? Il s'agit de notions difficiles, reposant justement sur la subtile notion de limite et qui seront au centre d'une bonne partie du cours d'analyse. Pour décrire le comportement global d'une fonction (ou d'une suite), nous disposons d'un vocabulaire qui vous est déjà largement familier (fonction croissante, décroissante, paire, impaire, bornée, périodique, injective, surjective, bijective, etc.) et que je vous rappelle rapidement dans la Section 3.4. Vous pouvez vous y référer en cas de besoin, les notions intervenant sont relativement simples. De même, comme vous le savez, un outil qui est souvent efficace dans la description (qualitative) du comportement des fonctions est leur graphe. J'en parlerai brièvement dans la Section 3.3 : il s'agit là aussi essentiellement d'une révision de matière que vous avez apprise au lycée, mais qui est souvent mal maîtrisée par les jeunes bacheliers que vous êtes.

J'ai ajouté à la fin de ce chapitre une section supplémentaire avec des considérations de logique qu'il conviendra de consulter au fur et à mesure que vous progressez dans le Chapitre 4 et les suivants.

Vous remarquerez que le début du cours d'analyse sera plutôt technique, mais avant de pouvoir s'attaquer à des questions intéressantes d'analyse dans les chapitres suivants, il nous faut un certain nombre d'outils qu'il convient de mettre en place. Contrairement à ce qui se passait dans le cours d'arithmétique, je ne pourrai pas répondre aux problèmes posés dans cette introduction très rapidement, mais il faudra attendre les chapitres ultérieurs pour cela. Je signale en particulier que le Chapitre 4 sera assez difficile parce que les notions qui y sont introduites sont bien plus sophistiquées que celles présentées dans le Chapitre 1. Vous ne pouvez pas espérer comprendre à fond toutes les démonstrations dès la première lecture de ce chapitre, et il conviendra d'y revenir à maintes reprises dans l'avenir. Je vous indiquerai au fur et à mesure quelles démonstrations sont plus faciles d'accès et pour lesquelles un peu plus de maturité et d'expérience est requise.

Exercice 3.5. *Nous avons trouvé une solution à (3.1) en forme de somme infinie. Mais peut-être ceci est-il inutilement compliqué et existe-t-il une fraction rationnelle qui est solution de (3.1) ? Après tout, certaines fractions rationnelles comme $1/(1-x)$ ou $1/(1+x^2)$ s'écrivent comme une somme infinie et il n'est pas à priori clair que, inversément, la somme (3.4) ne s'écrit pas comme une fraction rationnelle. Montrer que tel n'est pas le cas. (Indication : montrer qu'une solution de (3.1) ne peut pas être de la forme P/Q, avec P et Q des polynômes.)*

3.2 Qu'est-ce une fonction ?

Parmi les multiples significations du substantif "fonction" (la fonction respiratoire, la fonction publique, la fonction de maire ...) tel qu'il apparaît dans la vie courante, il y en a une qui exprime une dépendance : "Vos impôts sont déterminés en fonction de votre revenu" et "Votre succès sera fonction de votre investissement personnel." La notion générale de fonction utilisée en mathématiques est inspirée de cette dernière signification du mot, bien que cela ne soit pas évident à première vue :

Définition 3.6. *Etant donnés deux ensembles, une fonction (ou une application) est une règle qui associe à chaque élément du premier un élément du second. On appelle le premier ensemble le domaine de définition de la fonction ou encore l'ensemble de départ de la fonction et le second l'ensemble d'arrivée.*

Vous êtes familier, depuis le lycée, avec le cas où le premier ensemble est (un sous-ensemble de) $\mathbb{R}$ et le second est $\mathbb{R}$. La fonction logarithme, par exemple, est une règle qui associe à chaque nombre réel $x > 0$ son logarithme, noté $\ln x$. De même, la fonction sinus associe à x la valeur de son sinus, notée $\sin x$. La fonction "racine carré", elle, associe à chaque nombre réel positif ou nul x l'unique réel positif ou nul dont le carré vaut x.

Mais vous avez par ailleurs déjà manipulé d'autres fonctions, sans forcément le savoir. Par exemple, lorsque vous étudiez dans les cours de physique le mouvement d'un projectile dans l'espace, vous donnez à chaque instant t sa position en spécifiant les coordonnées cartésiennes $x(t), y(t)$ et $z(t)$ du point $P(t)$ où il se trouve, comme indiquée sur la figure 3.4.

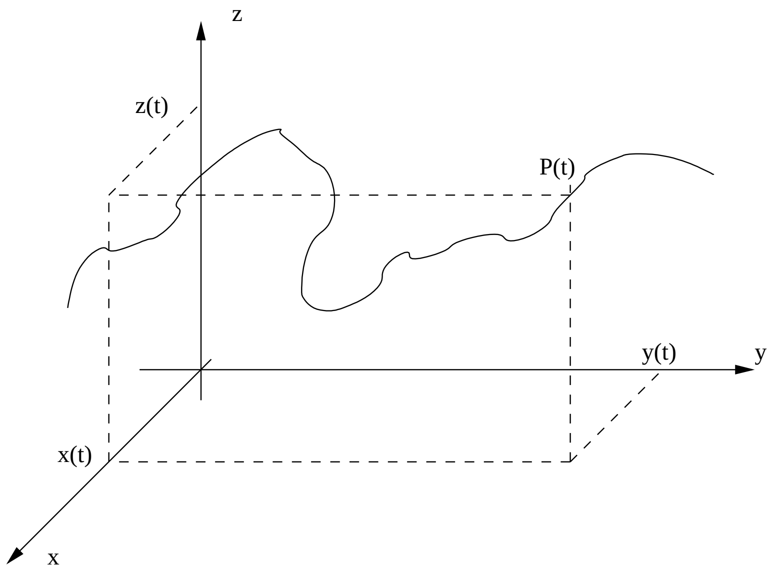

FIG. 3.4 – Le mouvement d'un projectile dans l'espace

Pour un projectile lancé de l'origine du système de coordonnées à l'instant 0 avec une vitesse $v = (v_1, v_2, v_3)$ on a très explicitement

$$x(t) = v_1 t, y(t) = v_2 t, z(t) = v_3 t - \frac{1}{2} g t^2.$$

Le mathématicien reconnaît ici une fonction dont l'ensemble de définition est $[0, \infty[$ et l'ensemble d'arrivée l'ensemble $\mathbb{R}^3$. On appelle ce type de fonction une courbe paramétrée. Dans cet exemple on voit bien comment la notion de "dépendance" est cachée dans la définition technique de fonction ci-dessus : la position du projectile dépend en effet du temps dans la mesure où elle varie avec le temps. Plus précisément, étant donné l'instant t, on connaît exactement la position $P(t)$ du projectile. On dit aussi parfois que t est la variable "indépendante" et (x, y, z) les variables "dépendantes". La température dans l'amphithéâtre est un autre exemple. En effet, la température varie d'un point à l'autre. En repérant les points dans l'espace par leurs coordonnées cartésiennes, on peut représenter la température comme une fonction T de trois variables (x, y, z). On obtient ainsi une fonction dont le domaine de définition est (un sous-ensemble de) $\mathbb{R}^3$ et l'ensemble d'arrivée $\mathbb{R}$. Cette fois-ci, ce sont les trois variables (x, y, z) qui sont indépendantes, et la température est considérée comme la variable dépendante.

Une suite aussi est une fonction. En effet, se donner une famille de nombres $u_n, n \in \mathbb{N}$ est la même chose que se donner une règle qui associe à chaque entier n un nombre. Une suite est donc une fonction dont le domaine est $\mathbb{N}$ et l'ensemble d'arrivée $\mathbb{R}$ (ou $\mathbb{C}$). Nous en avons vu un exemple dans l'arithmétique où nous avons parlé de $\pi(x)$, le nombre de nombres premiers inférieurs à $x \in \mathbb{N}$.

Dans l'étude du système de codage RSA (Section 1.6), nous avons déjà manipulé une fonction, sans avoir utilisé le terme explicitement. Il s'agit de la fonction qui associé à chaque entier $M \in \{1, \ldots N\}$ (le message), l'entier C appartenant à $\{1, \ldots N\}$ et défini par $C \equiv M^e\ [N]$ (le message codé). Ici l'ensemble d'arrivée est le même que l'ensemble de départ et il est clair que le message codé C "dépend" du message M.

Plus généralement, lorsque l'ensemble d'arrivée est $\mathbb{R}$, on dit que f est une fonction réelle ou une fonction numérique. Lorsque le domaine est un sous-ensemble de $\mathbb{R}$, on dit que f est une fonction d'une variable et, de même, lorsque le domaine est un sous-ensemble de $\mathbb{R}^2$, respectivement $\mathbb{R}^3$, que f est une fonction de deux, respectivement trois variables. Les fonctions logarithme, exponentielle, sinus, etc. sont donc des fonctions numériques d'une variable. Les courbes paramétrées sont des fonctions d'une variable, à valeurs dans $\mathbb{R}^2$ ou dans $\mathbb{R}^3$.

La définition de "fonction" ci-dessus vous paraît certes plutôt abstraite, même si les quelques exemples que j'ai donnés montrent déjà sa flexibilité. Au fait, les fonctions apparaissent sous diverses formes dans bien des branches des mathématiques et dans beaucoup de ses applications, ainsi qu'en informatique. Par conséquent, nous les rencontrerons sous diverses formes tout au long de ce cours.

Dans le Chapitre 4, nous entamons l'étude des fonctions numériques d'une variable et des suites numériques. Avant cela, rappelons quelques notations dans le cadre de la définition générale ci-dessus. On utilise souvent les lettres f, g ou h pour désigner des fonctions. En écrivant D pour l'ensemble de définition et E pour l'ensemble d'arrivée d'une fonction f, on écrit alors

$$f : D \to E,$$

ou, en plus de détail,

$$f : x \in D \mapsto f(x) \in E,$$

ce qui signifie que la fonction associe à l'élément x du domaine de définition D l'élément $f(x)$ de l'ensemble d'arrivée E. On dit que "f prend ses valeurs dans E" ou encore que "f est une fonctions à valeurs dans E." A part les fonctions numériques à une variable, les suites numériques, et les courbes paramétrées, vous rencontrerez cette année dans le cours d'algèbre linéaire une famille bien particulière de fonctions à plusieurs variables connues sous le nom d'applications linéaires. Les fonctions à plusieurs variables ne seront étudiées en plus de généralité qu'à partir de l'année prochaine (même si elles seront utilisées dès cette année dans le cours de physique).

Pour conclure cette section, une dernière remarque : dans une partie de la littérature on utilise systématiquement le terme "application" plutôt que "fonction" et on réserve le terme fonction pour ce que j'ai appelé ici "fonction numérique".

3.3 L'image et le graphe d'une fonction

Soit donnée une fonction $f : D \to E$ et soit y un élément de E. Il y a alors deux possibilités. Soit "f prend la valeur y", soit "f ne prend pas la valeur y". Avec le vocabulaire mis en place dans la Section 3.2, il devrait être clair ce que cela signifie. On dit que "f prend la valeur y" s'il existe un élément x dans le domaine D de f tel que $f(x) = y$. Par exemple, la fonction sinus prend la valeur 1 en $\pi/2$, mais ne prend la valeur 2 nullepart. Remarquez qu'une fonction peut prendre la même valeur en plusieurs points de son domaine : le sinus vaut 1 également en $5\pi/2$ et, plus généralement on a que $\sin(\frac{\pi}{2} + 2\pi k) = 1$ pour tout entier k. Lorsque $f(x) = y$, on dit que "x est un antécédent de y" ou encore que "y est l'image de x par f". On a alors la définition suivante :

Définition 3.7. *L'image de la fonction $f : D \to E$ est le sous-ensemble de E constitué des éléments de E ayant (au moins) un antécédent. On le désigne par $f(D)$. En d'autres termes, on a*

$$f(D) = \{y \in E | \exists x \in D, y = f(x)\},$$

ce qui se lit : "f(D) est l'ensemble des y appartenant à E tels qu'il existe un x appartenant à D ayant la propriété que $f(x) = y$." Très brièvement, on peut dire aussi que l'image de f est l'ensemble des valeurs que prend f.

Faites attention de ne pas confondre l'image $f(D)$ de f avec son ensemble d'arrivée E. Cette distinction paraît peut-être un peu bizarre, mais elle a son importance. Considérons par exemple tout simplement la fonction $f(x) = x/(x^2 + 1)$. Elle a clairement $D = \mathbb{R}$ comme domaine et prend ses valeurs dans $\mathbb{R}$, donc $E = \mathbb{R}$. Mais quel est son image ? C'est à dire quelles valeurs prend-elle effectivement ? Ce n'est pas tout de suite clair : néanmoins, avec les maths apprises au lycée, vous établirez facilement que f atteint son maximum en $x = 1$, avec $f(1) = 1/2$ et son minimum en $x = -1$, avec $f(x) = -1/2$. Donc $f(D) = [-1/2, 1/2]$ dans ce cas, et clairement l'image de f n'est pas égale à son ensemble d'arrivée. La situation décrite dans cet exemple est typique. Souvent nous savons à priori que telle ou telle fonctions prend ses valeurs dans $\mathbb{R}$, sans pouvoir décider d'avance quelles valeurs elle prend effectivement. D'où la nécessité (ou plutôt la commodité) de distinguer ensemble d'arrivée et image. Nous y reviendrons dans le Chapitre 8.

Dans le même style, on a les notions suivantes. Si B est un sous-ensemble du domaine, on appelle "l'image de B par f" le sous-ensemble de E défini par

$$f(B) = \{y \in E | \exists x \in B, y = f(x)\}.$$

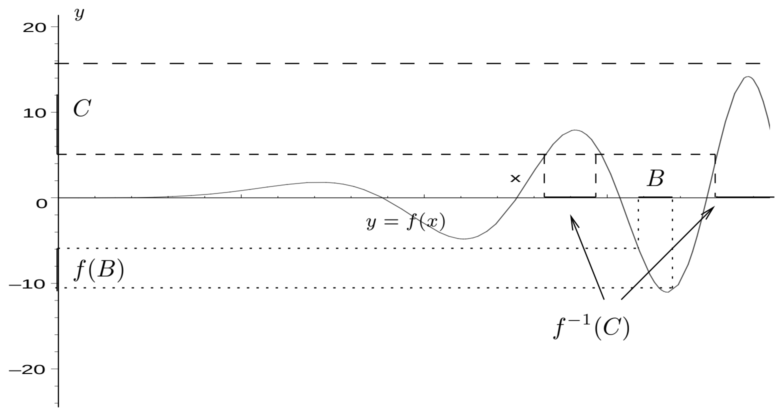

FIG. 3.5 – Image directe $f(B)$ et image réciproque $f^{-1}(C)$

Si C est un sous-ensemble de E, le "pré-image de C par f" est le sous-ensemble de D défini ainsi :

$$f^{-1}(C) = \{x \in D | f(x) \in C\}.$$

Un autre ensemble important dans l'étude des fonctions est son graphe, qui est un sous-ensemble du produit cartésien du domaine de f avec son ensemble d'arrivée. Il est défini ainsi :

Définition 3.8. *Le graphe de $f : D \to E$, noté G_f, est l'ensemble des couples (x, y) appartenant à $D \times E$ tels que y est l'image de x :*

$$G_f = \{(x, y) \in D \times E | y = f(x)\}.$$

Les définitions de cette section sont d'apparence simple, mais toutefois plutôt abstraites et elles recèlent plusieurs difficultés. Analysons-les en plus de détail dans le cadre familier des fonctions numériques d'une variable. Vous avez l'habitude de manipuler le graphe d'une fonction numérique $f : D \to \mathbb{R}$, qui est la collection de points du plan $\mathbb{R}^2$ de coordonnées (x, y) tels que $y = f(x)$. Vous l'avez souvent appelé "la courbe représentative de f", plutôt que "le graphe de f". On illustre facilement les notions de "image d'un intervalle" et "image réciproque d'un intervalle" sur un dessin (Fig. 3.5). Remarquez en particulier sur la figure que l'image réciproque de C est constituée de deux intervalles disjoints.

Pour les fonctions sympas, comme les polynômes, les fractions rationnelles, les fonctions trigonométriques et quelques autres que nous rencontrerons plus tard, on peut plus ou moins facilement tracer le graphe. Ce n'est pas toujours le cas ! Je vous invite par exemple à vous demander pourquoi j'ai fait tracer, par mon ordinateur, le graphe de la fonction $\sin(1/x)$ seulement entre $0,03$ et $0,4$, et pas entre 0 et $0,03$ (Fig. 4.8). Sauriez-vous le faire à la main ? Votre calculatrice

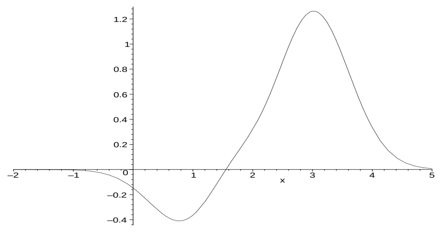

FIG. 3.6 – $y = f(x)$

sait-elle le faire ? Il y a des fonctions plus bizarres encore, dont le graphe n'est pas du tout une courbe. Il en résulte qu'on peut utiliser les graphes pour visualiser les notions, mais pas pour démontrer des théorèmes sur les fonctions.

Le lecteur s'entraîne

1. Dans la figure 3.6 vous trouvez le graphe d'une fonction $f : \mathbb{R} \to \mathbb{R}$. Tracez les graphes des fonctions

$$f_1(x) = f(x+2), f_2(x) = f(2x), f_3(x) = f(x) + 3, f_4(x) = 2f(x).$$

2. Etudier (par tous les moyens intellectuels et techniques dont vous disposez) le graphe de la fonction $f :]0, 1[\to \mathbb{R}$, $f(x) = \exp -\frac{\sin 10\pi x}{x^2}$. Décrivez son allure et discuter le comportement de votre calculatrice lorsque vous lui demander le graphe.

3.4 Comportement global d'une fonction numérique

La limite d'une fonction dépend du comportement local, proche du point x_* que l'on regarde. Pour étudier le comportement global d'une fonction, on dispose de tout un vocabulaire, que vous connaissez en grande partie et qui n'est pas très compliqué. Je vous rappelle rapidement les notions essentielles.

Soit $f : D \to \mathbb{R}$ une fonction. On dit que f est croissante (respectivement décroissante) si et seulement si pour tout $x \leq y, x, y \in D$, on a $f(x) \leq f(y)$ (respectivement $f(x) \geq f(y)$). On dit qu'elle est strictement croissante (respectivement décroissante) si et seulement si pour tout $x < y, x, y \in D$, on a $f(x) < f(y)$ (respectivement $f(x) > f(y)$). On dit qu'une fonction est monotone si et seulement si elle est croissante ou décroissante.

On dit que f est minorée (respectivement majorée) si et seulement si il existe $C \in \mathbb{R}$ tel que, pour tout $x \in D$, $f(x) \geq C$ (respectivement $f(x) \leq C$). Elle est bornée si et seulement si elle est à la fois minorée et majorée. Ceci est à comparer à la Définition 4.16.

Nous reviendrons plus tard sur les notions de fonction injective, surjective, bijective.

Le lecteur s'entraîne

1. Les affirmations suivantes, sont-elles vraies ou fausses ?
a) Une fonction impaire est toujours monotone.
b) La composée de deux fonctions décroissantes est croissante.
c) Le produit de deux fonctions croissantes est encore une fonction croissante.
d) Si f n'est pas croissante, alors f est décroissante.

3.5 Encore un peu de logique : les quantificateurs

Les énoncés des définitions, lemmes et théorèmes de l'analyse voient apparaître en masse des éléments de phrase que j'ai évités d'utiliser dans le chapitre sur l'arithmétique : il s'agit de "Pour tout ...," et "Il existe ...". Afin de bien comprendre les développements des chapitres suivants, il est indispensable d'apprendre à bien les interpréter et les utiliser, ne fût-ce que pour comprendre les diverses définitions de la notion de limite, ce qui n'est pas tout à fait facile. Ces constructions, ainsi que leurs négations, perturbent en effet beaucoup les débutants, partiellement parce qu'elles n'apparaissent pas dans le langage courant sous exactement la même forme. On dit

"Il y a une antenne sur chaque maison,"
"Il y a un prix pour chaque participant,"

plutôt que

"Sur toute maison, il existe une antenne",
"Pour tout participant, il existe un prix",

bien que cela revienne au même. Les mathématiciens préfèrent cette dernière formulation, parce qu'elle évite certaines ambiguités du langage courant, comme je vous explique tout de suite.

Si le président de l'université dit :

"A l'Université de Lille 1, il y a un ordinateur pour tous les étudiants,"

le sens de la phrase dépend de l'intonation qu'il lui donne et du contexte dans lequel elle est prononcée. S'il parle à un ministre qu'il doit convaincre de donner des crédits pour acheter du matériel informatique, il placera l'accent sur "un" et on comprendra qu'il n'y a qu'un seul ordinateur pour les 20.000 étudiants. Dans ce cas, le sens de son affirmation est

"A l'Université de Lille 1, il n'y a qu'un seul ordinateur pour tous les étudiants."

Cette interprétation de la phrase est à comparer avec

"Il y a, en France, un président pour tous les citoyens."

Elle a exactement la même structure que la phrase concernant les ordinateurs et tout le monde comprend qu'elle signifie qu'en France, il y a un seul président, qui est le président de tous les citoyens (n'en déplaise à certains).

Si, par contre, le président de l'université parle pendant une journée portes ouvertes devant des lycéens qu'il veut convaincre de venir s'inscrire à Lille 1, il placera l'accent sur "pour tous" et on comprendra qu'il y a beacoup d'ordinateurs à l'université. Le sens de son affirmation est alors analogue à celui qu'on donne à

"Il y a une réponse à toutes les questions,"

où tout le monde comprend qu'il faut des réponses différentes à des questions différentes. Dans ce cas, il pourrait aussi dire

"A l'Université de Lille 1, il y a un ordinateur pour chaque étudiant,"

ou – et c'est la tournure préférée par les mathématiciens –

"Pour tout étudiant de l'Université de Lille 1, il y a un ordinateur."

En résumé, on vient de constater que, si une phrase contient un "pour tout" et un "il existe" (ou un "il y a"), l'ordre dans lequel ils apparaissent, ainsi que d'autres petites variations dans la structure de la phrase ("pour tous, pour tout, pour chaque, ...") peuvent changer le sens de l'affirmation. Dans la vie courante, ceci ne pose que rarement problème, comme le contexte de la phrase indique le plus souvent le sens voulu. En mathématiques, ce genre d'ambiguïté n'est pas admissible, parce qu'elle mène a des confusions et des non-sens inacceptables.

Pour éviter qu'un seul énoncé puisse avoir plusieurs sens, les mathématiciens choisissent de toujours respecter les règles de base suivantes dans l'utilisation de "pour tout" et de "il existe" :

- Si "il existe" précède "pour tout", on entend que l'objet dont l'existence est affirmée ne dépend pas des objets visés par le "pour tout."
- Si "pour tout" précède "il existe", l'objet dont l'existence est affirmé *peut* (mais ne doit pas) dépendre des objets visés par le "pour tout".

Je répète que ces règles ne sont pas toujours respectées dans le langage courant, et ne nous viennent donc pas tout à fait naturellement, mais il faut savoir que, pour comprendre ou construire un énoncé mathématique, il est important de les appliquer systématiquement. Illustrons ces règles par quelques exemples.

"Il existe un entier a tel que, pour tout entier b, on a $b + a = b$."

Cette affirmation signifie qu'il y a *au moins* un entier a ayant la propriété que $a + b = b$, pour tous les entiers b. Elle est vraie, puisque $a = 0$ fait l'affaire ! Remarquez qu'aucun autre entier a n'a la propriété requise. Considérons maintenant :

"Il existe un entier a tel que, pour tout entier b, on a $a^2 b = b$."

Elle est vraie aussi, mais cette fois-ci il y a deux entiers a qui ont la propriété requise, à savoir $a = 1$ et $a = -1$. Regardons alors :

"Il existe un entier a tel que, pour tout entier b, on a $a \geq b$."

Cela signifie qu'il existe un entier plus grand que tous les entiers ! C'est évidemment faux, un tel entier n'existe pas. Par contre, l'affirmation

"Pour tout entier b, il existe un entier a tel que $a \geq b$,"

est vraie ! En effet, étant donné b, on peut prendre $a = b + 1$ (ou même $a = b$!) au quel cas on a bien $a \geq b$. On voit bien que la valeur de a dépend de b. Finalement, considérons encore :

"Pour tout entier b, il existe un entier a tel que $b + a = b$."

Vrai ou faux ? C'est bien évidemment vrai, mais cette fois-ci, pour chaque valeur de b le seul entier avec la propriété requise est $a = 0$.

Exercice 3.9. *Les affirmations suivantes, sont-elles vraies ou fausses ?*
"Pour tout entier b, il existe un entier a tel que $a^2 b < 0$."
"Pour tout entier a, il existe un entier b tel que $a^2 b < 0$."

Les exemples ci-dessus sont très simples. Ils ont la structure

"Pour tout a, il existe b tel que $P(a, b)$,"

où $P(a, b)$ est une propriété qui dépend de a et de b (comme $a^2 b > 0$, par exemple). Pour plus de briéveté, on écrit plutôt

$$\text{“}\forall a, \exists b, P(a, b),\text{”}$$

où les symboles $\forall$ et $\exists$ signifient "pour tout" et "il existe".

La définition de limite d'une fonction en un point (voir le Chapitre 4, Définition 4.1) a la même structure

$$\text{“}\forall \epsilon, \exists \delta, P(\epsilon, \delta),\text{”}$$

mais elle est difficile parce que l'affirmation $P(\epsilon, \delta)$ en question est elle-même assez complexe. Les choses se compliquent encore lorsqu'on essaie de formuler la négation de tels énoncés. Retournons un moment au langage courant. La négation de l'affirmation

"Tous les participants auront un prix",

est, toujours dans le langage courant,

"Tous les participants n'auront pas de prix."

Mais cette façon de formuler la négation peut prêter à confusion. En effet, la négation de "Toutes les portes sont ouvertes," est "Toutes les portes ne sont pas ouvertes", qui pourrait être confondu avec l'affirmation tout à fait différente : "Toutes les portes sont fermées." Dans la phrase "Toutes les portes ne sont pas ouvertes", la négation porte sur "toutes" et pas sur "ouvertes" ! Une façon de formuler la négation qui ne peut être mal interprêtée est de dire "Il existe (ou il y a) une porte qui n'est pas ouverte." C'est celle-là qui est constamment utilisée en mathématiques et à laquelle il faut donc s'habituer. Pour résumer, si une phrase a la structure :

$$\text{“}\forall x, P(x)\text{”}$$

sa négation est

$$\text{“}\exists x, \text{non } P(x).\text{”}$$

Appliquée à "Pour tout participant, il y a un prix," cela donne "Il y aura un participant qui ne gagnera pas de prix."

On en conclut tout de suite que la négation de

$$\text{“}\exists x, P(x)\text{”}$$

est

$$\text{“}\forall x, \text{non } P(x).\text{”}$$

Cela aussi peut paraître surprenant au premier abord. Dans le langage courant, la négation de "Il y a" est généralement formulée avec "Il n'y a pas." Par exemple, la négation de "Il y a des sportifs de talent en France" est tout simplement "Il n'y a pas de sportifs de talent en France." Mais on pourrait tout aussi bien dire que "Aucun sportif en France n'a du talent" ou encore que "Tous les sportifs en France sont sans talent." C'est cette dernière tournure de phrase qui est systématiquement utilisée en mathématiques.

Exercice 3.10. *Analyser les relations logiques entre les affirmations suivantes : "Tout le monde est riche", "Tout le monde n'est pas riche", "Il y a des gens pauvres", "Tout le monde est pauvre", etc.*

Que faire, lorsqu'il faut montrer une affirmation du type "$\forall x \in E, P(x)$" ? Les démonstrations commencent alors invariablement par "Soit $x \in E$." Dans le sens qu'il prend ici, l'expression "Soit..." n'est jamais utilisée dans le langage quotidien, et par conséquent déroute les apprentis mathématiciens. Voici un exemple simple de son usage mathématique, qui peut vous aider à vous y habituer. Considérons l'affirmation

$$\forall x \in \mathbb{R}, x^2 + 5 - x > 0.$$

Elle se démontre ainsi : "Soit $x \in \mathbb{R}$, alors

$$x^2 + 5 - x = x^2 + \frac{1}{4} - x + \frac{19}{4} = (x - \frac{1}{2})^2 + \frac{19}{4} \geq \frac{19}{4} > 0."$$

Le "Soit $x \in \mathbb{R}$, alors..." est ici un raccourci pour "Quelque soit le nombre réel x, on a la propriété suivante...". De façon plus désinvolte, on pourrait dire "Prenez donc n'importe lequel nombre réel x, alors vous voyez bien que ...." (Vous n'écrirez cette dernière phrase dans un devoir surveillé qu'à vos propres risques et périls, bien sûr. Un grand nombre de mes collègues me frapperont d'ailleurs d'anathème s'ils apprennent que j'ose utiliser un tel langage dans un texte mathématique.)

Montrer une affirmation du type "$\forall x \in E, \exists y \in F, P(x, y)$" signifie montrer que, quelque soit l'élément x de E, on peut toujours trouver un élément y de F tel que la propriété $P(x, y)$ soit vraie. Dans une telle démonstration il faut donc construire, pour chaque x, un y qui fait l'affaire. Illustrons ceci par un exemple. Supposons qu'on vous demande de montrer l'affirmation suivante :

$$\text{“}\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, \sin x = \cos y.\text{”}$$

La démonstration peut alors se faire ainsi. Soit x un réel quelconque. On a $\sin x = \cos(\frac{\pi}{2} - x)$. En posant $y = \frac{\pi}{2} - x$, on a $\sin x = \cos y$. On remarquera encore une fois dans cet exemple que le réel y qui remplit la condition dépend de x. Dans les démonstrations de propriétés $P(x, y)$ plus compliquées, on montre souvent l'existence du y sans pouvoir l'exhiber explicitement, ce qui augmente bien évidemment le degré d'abstraction de la démonstration. Vous trouverez facilement plusieurs exemples de ce phénomène dans le Chapitre 4.

Finalement, un dernier mot sur le langage mathématique courant. Le symbole $\forall$ n'est pas toujours lu "pour tout", mais parfois "quelque soit". Par exemple,

$$\text{“}\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, \sin x = \cos y.\text{”}$$

peut être lu "Quelque soit x appartenant à $\mathbb{R}$, il existe un réel y tel que $\sin x = \cos y$." C'est surtout pratique lorsque les énoncés sont très longs. Je ne m'en priverai pas dans la suite.

Le lecteur s'entraîne

1. Déterminer explicitement les sous-ensembles de $\mathbb{R}$ suivants :
a) $A = \{x \in [0,1] \mid \exists n \in \mathbb{N}^*, \frac{1}{n} \leq x \leq 1\}$;
b) $B = \{x \in [0,1] \mid \forall n \in \mathbb{N}^*, \frac{1}{n} \leq x \leq 1\}$.

2. Soit $f : D \to \mathbb{R}$. Les affirmations suivantes, sont-elles vraies ou fausses ?
(a) $\exists m, M \in \mathbb{R}, \forall x \in D, m \leq f(x) \leq M$.
(b) $\forall x \in D, \exists m, M \in \mathbb{R}, m \leq f(x) \leq M$.

3. L'affirmation suivante, est-elle vraie ou fausse ?

$$\forall b \in \mathbb{R}, \exists a \in \mathbb{R}, \forall r \in \mathbb{R},\ (a^2 + b^2 > r^2 \Rightarrow a^2 - b^2 > r^2).$$

Formuler sa négation.

Chapitre 4

Limites

A l'infini et au delà !
Buzz L'Eclair

4.1 Limite d'une fonction : la définition

4.1.1 La définition

L'outil essentiel pour comprendre le comportement local d'une fonction et en particulier les notions de continuité et de dérivabilité des fonctions est la limite d'une fonction en un point, que nous étudierons donc d'abord. Cette notion n'est pas simple et il est en particulier difficile (voir impossible) de paraphraser sa définition avec une phrase en bon français qui en capte correctement toutes les subtilités : ce n'est que le langage mathématique qui y arrive. Voici tout de même deux tentatives, avant de donner la définition formelle précise. Dans la suite, le domaine D d'une fonction sera toujours une union d'un nombre fini d'intervalles disjoints. Par exemple, la fonction $f(x) = \frac{1}{x^2-5x+6}$ est définie sur $D =]-\infty, 2[\cup]2, 3[\cup]3, \infty[$. Pour éviter des complications sans intérêt, j'excluerai systématiquement le cas où un des intervalles constituant D soit un singleton (c'est à dire ne contient qu'un seul élément). Je désignerai par $\overline{D}$ l'ensemble D auquel on a rajouté les extrémités de ces intervalles. Dans l'exemple ci-dessus on a donc $\overline{D} = \mathbb{R}$. *On dit que la fonction $f : D \to \mathbb{R}$ admet pour limite $\ell \in \mathbb{R}$ en un point $x_* \in \overline{D}$ si et seulement si*

(1) les valeurs que prend f lorsque x est proche de x_* sont proches de ℓ.

ou, alternativement

(2) les valeurs $f(x)$ que prend f sont aussi proches que l'on veut de ℓ pourvu que x est assez proche de x_*.

Voici la définition formelle :

Définition 4.1. *On dit que la fonction $f : D \to \mathbb{R}$ admet $\ell \in \mathbb{R}$ comme limite en un point $x_* \in \overline{D}$ si la condition suivante est satisfaite. Pour tout $\epsilon > 0$, il* *existe $\delta > 0$ avec la propriété que, pour chaque $x \in D$ tel que $0 < |x - x_*| < \delta$, on a $|f(x) - \ell| < \epsilon$. On écrit alors $\lim_{x \to x_*} f(x) = \ell$.*

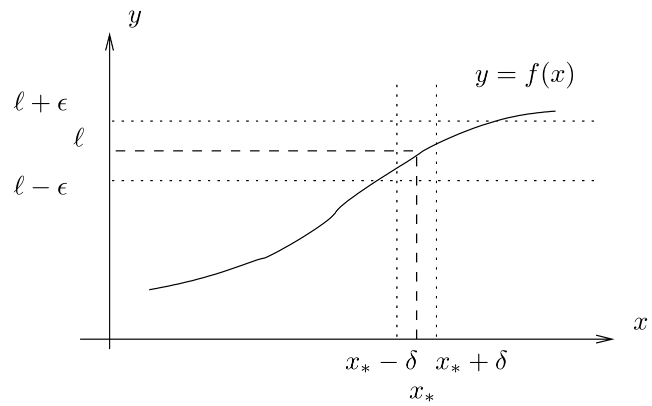

FIG. 4.1 – La définition de limite en images

On dit aussi que f tend vers ℓ ou converge vers ℓ lorsque x tend vers x_*. Dans les notations de la Section 3.5 l'affirmation "Pour tout $\epsilon > 0, \ldots |f(x) - \ell| < \epsilon$" de la définition s'écrit plus concisément :

$$\forall \epsilon > 0, \exists \delta > 0, \forall x \in D, (0 < |x - x_*| < \delta) \Rightarrow |f(x) - \ell| < \epsilon.$$

Comme avec toutes les notions nouvelles que vous rencontrerez, il est important dans un premier temps d'apprendre la définition tout simplement par coeur. Néanmoins, le seul fait de savoir réciter la définition ne suffit pas à comprendre la notion elle-même : la définition ci-dessus l'illustre, je pense, de façon convaincante. Pour cela, il faut la manipuler et l'utiliser longuement, et en avoir vu beaucoup d'exemples.

4.1.2 Utiliser la définition : un exemple

Pour faciliter la compréhension de la définition de limite, je vous donne quelques tuyaux. Premièrement : personne n'a jamais compris la notion de limite d'une fonction sans travailler de longues heures. Ensuite, si les "il existe" et les "pour tout" vous donnent le tournis, je vous recommande d'ores et déjà vivement la relecture de la Section 3.5. Troisièmement, il est très utile de se rappeler que "la valeur absolue de $x - x_*$ (resp. de $f(x) - \ell$)" est précisément la même chose que "la distance entre x et x_* (resp. entre $f(x)$ et ℓ)". Cette interprétation géométrique de la valeur absolue rend la lecture de la définition plus claire :

> "…pour chaque $x \in D$ tel que $0 < |x - x_*| < \delta$, on a que $|f(x) - \ell| < \epsilon$."

devient alors

> "...pour chaque x qui appartient à D et qui est à une distance d'au plus δ de x_* on a que $f(x)$ est à une distance d'au plus ϵ de ℓ."

Dans la Section 4.1.5 ci-dessous, je donne une représentation graphique de la notion de limite, qui aide également à la compréhension. Rien ne vous empêche de l'étudier dès maintenant.

Afin de clarifier la définition de limite, je traite quelques exemples. Montrons d'abord que

$$\lim_{x\to 2} x^3 = 8.$$

Ne me dites pas que c'est évident parce que la fonction x^3 est continue et que $2^3 = 8$. En effet, dans ce cas je vous demanderai de me montrer que la fonction x^3 est continue et ça reviendra au même que de montrer que $\lim\limits_{x\to 2} x^3 = 8$ (voir Section 5.1). Ce que je veux est une démonstration directe à partir de la définition de limite ci-dessus. Il faut donc montrer ceci : si ϵ est un nombre réel positif quelconque, on peut trouver $\delta > 0$ avec la propriété que, pour chaque $x \in \mathbb{R}$ satisfaisant les inégalités $0 < |x-2| < \delta$, on a que $|x^3 - 8| < \epsilon$.

Dans ce but, nous allons dans un premier temps explorer les valeurs de $|x^3 - 8|$ lorsque x est dans un intervalle autour de 2. Considérons donc $0 < a < 1$ quelconque et $x \in]2-a, 2+a[$, ou encore $|x-2| < a$. Rappelons que nous avons (utiliser (2.6))

$$|x^3 - 8| = |x-2|\ |4 + 2x + x^2|$$

et donc

$$|x^3 - 8| < a(4 + 2|x| + |x^2|).$$

Mais $0 < |x-2| < a$ implique également que $|x| < 3$, puisque $0 < a < 1$. (Faites un dessin si vous ne me croyez pas.) Par conséquent,

$$\text{Si } |x-2| < a, \text{ alors } |x^3 - 8| < a(4+6+9) = 19a.$$

On peut paraphraser cette affirmation en disant que, si x est proche de 2 (donc si a est petit), alors x^3 est proche de 8 (à savoir $|x^3 - 8| < 19a$).

Revenant à la définition formelle, nous pouvons alors conclure de la façon suivante. Soit $\epsilon > 0$ quelconque. Considérons $\delta = \min\{1, \frac{\epsilon}{19}\}$. En prenant $a = \delta$ dans la conclusion ci-dessus, on a, pour tout $0 < |x-2| < \delta$

$$|x^3 - 8| < 19\delta \le \epsilon,$$

ce qui conclut la démonstration.

Remarquez que nous avons trouvé un δ pour chaque ϵ et que ce δ dépend de ϵ puisque $\delta = \min\{1, \frac{\epsilon}{19}\}$. Par exemple, pour s'assurer que $|x^3 - 8|$ soit plus petit que 1, il suffit de prendre δ égal à $1/19$, et pour s'assurer que $|x^3 - 8|$ soit plus petit que $0,1$, il suffit de prendre δ égal à $1/190$. En d'autres termes, dans un intervalle de taille $2\delta = 1/95$ autour de 2, $|x^3 - 8|$ est plus petit que $0,1$. J'ai demandé à mon ordinateur de tracer $y = x^3$ pour x entre $1,7$ et $2,3$ et entre $1,9$ et $2,1$, ce qui vous permet de vérifier ces affirmations sur la figure 4.2. Le

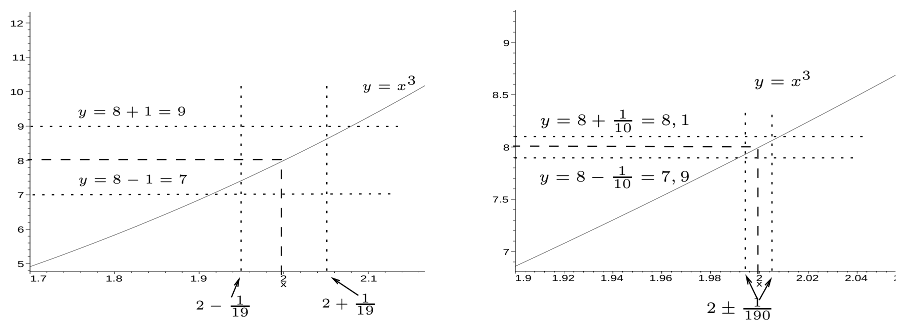

FIG. 4.2 – $\lim\limits_{x \to 2} x^3 = 8$. Il faut remarquer la différence d'échelle entre les deux dessins.

mécanisme de la démonstration ci-dessus, qui s'applique dans bien des cas, est donc le suivant. On a étudié

$$\max \{|f(x) - \ell| \mid x \in D, 0 < |x - x_*| < a\}$$

et on a montré que, si x est à une distance inférieure à a de x_*, alors ce maximum est inférieur à une constante fois a, ce qui permet de conclure.

4.1.3 Pas de limite

Considérons un exemple où la limite n'existe pas. Chaque fois qu'une nouvelle notion vous est présentée, il est utile de voir si vous comprenez sa négation. Si cette dernière a l'air difficile, vous pouvez soupçonner que la notion de départ n'était pas facile non plus. Par exemple, la notion de nombre premier est plutôt facile. Sa négation n'est pas difficile non plus : "$n \in \mathbb{N}$ n'est pas un nombre premier si et seulement si $n = 1$ ou n a un diviseur positif différent de 1 et de n." Par contre, "f n'a pas de limite" est nettement moins facile. Essayons : "f n'a pas de limite en un point $a \in \overline{D}$ si et seulement si pour tout réel ℓ la propriété suivante est satisfaite : il existe $\epsilon > 0$, tel que pour tout $\delta > 0$, il existe $x \in D, 0 < |x - a| < \delta$, ayant la propriété que $|f(x) - \ell| \geq \epsilon$." On ne peut pas prétendre que ce soit particulièrement transparent. En particulier, s'il faut montrer que f n'a pas de limite, il faut montrer qu'aucun réel ℓ ne peut être la limite de f, ce qui explique la présence de "pour tout réel ℓ" dans la phrase ci-dessus. Considérons alors la fonction suivante :

$$\begin{aligned} H(x) &= 0, \qquad x < 0, \\ &= 1, \qquad 0 \leq x. \end{aligned}$$

On l'appelle parfois la fonction de Heaviside. Il semble évident, à partir de la notion intuitive de "limite" exprimée dans les paraphrases de la définition ci-dessus, que H n'a pas de limite en 0. En effet, lorsque x s'approche de 0, $H(x)$

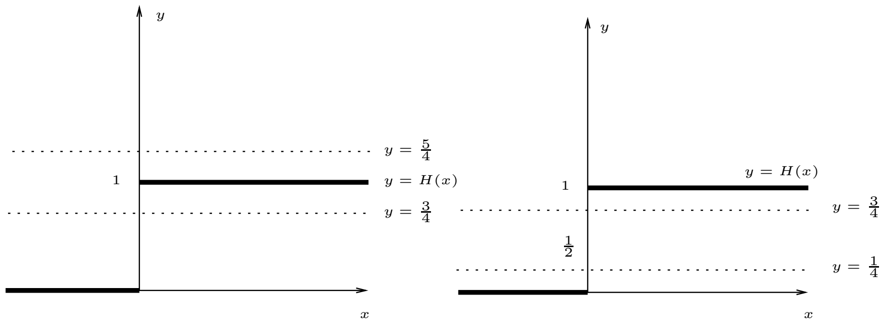

FIG. 4.3 – La fonction de Heaviside n'admet ni 1, ni 1/2 comme limite en 0.

vaut 1 si x est positif et $H(x)$ vaut 0 si x est négatif; $H(x)$ ne s'approche donc ni de 1, ni de 0, ni d'un quelconque autre réel. Ce résultat est également évident sur le graphe de H : en traçant, pour n'importe quel ℓ, la bande horizontale entre $y = \ell - 1/4$ et $y = \ell + 1/4$, on voit tout de suite que le graphe de $y = H(x)$ en sort, aussi proche que l'on soit de $x = 0$. Cela veut dire que $\mid H(x) - \ell \mid$ n'est pas forcément plus petit que $1/4$, même si x est très proche de 0. Cette observation est illustrée pour $\ell = 1$ et pour $\ell = 1/2$ dans la figure 4.3. Mais comment, en utilisant la définition (ou plutôt sa négation) montrer que H n'a pas de limite ? Ceci nécessite une certaine virtuosité dans la manipulation des ϵ et des δ et je le remets à plus tard (Section 4.8).

4.1.4 Tripoter les ϵ et les δ

Pour démarrer votre entraînement dans cette jonglerie des ϵ et des δ, je vous invite à étudier la démonstration du lemme suivant, qui rassemble quelques propriétés fondamentales, faciles à prouver et très utiles. Je me servirai des résultats de l'exercice suivant.

Exercice 4.2. *(i) Montrer que, pour tout $a, b \in \mathbb{R}$, on a*

$$|a| - |b| \leq \mid |a| - |b| \mid \leq |a \pm b| \leq |a| + |b|. \tag{4.1}$$

Ces petites inégalités anodines (qui s'appellent "les inégalités triangulaires") n'ont rien à voir directement avec la notion de limite, mais sont de la plus grande importance et très souvent utiles dans les démonstrations les plus variées.

(ii) Montrer l'affirmation suivante. Soient $0 \leq a < +\infty$. Si, pour tout $\epsilon > 0$, $a \leq \epsilon$, alors $a = 0$. En d'autres termes, un réel positif ou nul qui est inférieur à tout réel positif est égal à 0.

Solution : Le (i) se démontre facilement en regardant différents cas. Je vous recommande de commencer par

$$|a+b|^2 = (a+b)^2 = a^2 + b^2 + 2ab \leq |a|^2 + |b|^2 + 2|a|\ |b| = (|a| + |b|)^2$$

d'où l'on conclut immédiatement que $|a+b| \leq |a|+|b|$. Je montrerai le (ii) via un raisonnement par l'absurde. Supposons donc que $a \neq 0$, donc $a > 0$. On peut alors choisir $\epsilon = a/2$ pour conclure que $a \leq a/2$. On en conclut que $(a/2) \leq 0$ et donc $a \leq 0$, ce qui contredit l'hypothèse que $a > 0$. □

Lemme 4.3. *(i) Pour tout $x_* \in \mathbb{R}$ et pour tout $c \in \mathbb{R}$, on a*

$$\lim_{x \to x_*} x = x_* \quad \text{et} \quad \lim_{x \to x_*} c = c.$$

(ii) Soit $f : D \to \mathbb{R}$ et $x_* \in D$. Si f admet une limite en x_*, alors

$$\lim_{x \to x_*} f(x) = \lim_{h \to 0} f(x_* + h).$$

(iii) Si f a une limite en un point, alors cette limite est unique.
(iv) Soit $f : D \to \mathbb{R}$ et $x_* \in D$. On a

$$\lim_{x \to x_*} f(x) = 0 \text{ si et seulement si } \lim_{x \to x_*} |f(x)| = 0.$$

et

$$\lim_{x \to x_*} f(x) = \ell \text{ si et seulement si } \lim_{x \to x_*} (f(x) - \ell) = 0.$$

Démonstration* : Si ce n'est pas déjà fait, je vous conseille vivement d'étudier la Section 3.5 avant, ou en parallèle avec cette démonstration.

(i) Soit ϵ un réel positif quelconque. Il faut montrer qu'il existe $\delta > 0$ tel que

$$0 <| x - x_* |< \delta \Rightarrow | x - x_* |< \epsilon.$$

Mais un tel δ existe évidemment, il suffit de prendre $\delta = \epsilon$. C'est tellement simple que c'est déroutant ! Je vous laisse la deuxième partie du (i) en exercice et je procède tout de suite au (ii).

(ii) On sait que f admet comme limite ℓ en x_* et donc que, quelque soit ϵ, il existe δ tel que

$$0 <| x - x_* |< \delta \Rightarrow | f(x) - \ell |< \epsilon. \tag{4.2}$$

Il faut montrer que, étant donné un réel $\epsilon > 0$ quelconque, il existe $\delta' > 0$ tel que $| h |< \delta'$ implique que $| f(x_* + h) - \ell |< \epsilon$. Mais on peut évidemment choisir $\delta' = \delta$, puisque $| (x_* + h) - x_* |=| h |$ et l'hypothèse (4.2) implique donc que $| f(x_* + h) - \ell |< \epsilon$ pourvu que $| h |< \delta$!

(iii) La définition de limite n'exclut pas à priori la possibilité qu'une fonction admette deux limites ℓ, ℓ' distinctes en un même point x_*. L'affirmation à démontrer est donc que ceci est impossible. Supposons donc que $\ell, \ell' \in \mathbb{R}$ sont des limites de f en un point x_*. Soit $\epsilon > 0$, on sait alors qu'il existe $\delta > 0$ et $\delta' > 0$ tel que d'une part

$$0 <| x - x_* |< \delta \Rightarrow | f(x) - \ell |< \epsilon$$

et d'autre part

$$0 <| x - x_* |< \delta' \Rightarrow | f(x) - \ell' |< \epsilon.$$

Par ailleurs, pour tout $x \in D$, on a

$$\begin{aligned} |\, \ell - \ell' \,| &= |\, \ell - f(x) + f(x) - \ell' \,| \\ &\leq |\, \ell - f(x) \,| + |\, f(x) - \ell' \,| \,. \end{aligned}$$

En choisissant $x \in D$ tel que

$$0 <|\, x - x_* \,|< \min\,(\delta, \delta'),$$

(Pourquoi un tel x existe-t-il ?) on conclut donc que

$$0 \leq|\, \ell - \ell' \,|\leq 2\epsilon. \tag{4.3}$$

En retraçant la démonstration, vous constaterez que nous avons démontré que, quelque soit $\epsilon > 0$, on a (4.3). La deuxième partie de l'exercice ci-dessus permet de conclure que $\ell = \ell'$. $\square$

Je termine cette sous-section en attirant votre attention sur une petite subtilité, que j'ai escamotée jusque là. J'introduis d'abord la fonction “partie entière E”, définie pour tout réel x par :

“E(x) est le plus grand entier qui est plus petit que x”

ou, plus formellement

$$\mathrm{E}(x) = \max\{n \in \mathbb{Z} | n \leq x\}.$$

Considérons alors la fonction $f(x) = \mathrm{E}(\frac{1}{1+x^2})$. Il est facile de vérifier qu'elle vaut 0 partout, sauf en 0, où elle vaut 1. On en conclut qu'elle converge vers 0 en $x_* = 0$! En effet, la définition de limite exige que pour tout x tel que $0 < |x - 0| < \delta$, on a que $|f(x) - 0| < \epsilon$, ce qui est clair, puisque $0 < |x|$ implique que $f(x) = 0$! On a donc $f(0) = 1$ et $\lim_{x \to 0} f(x) = 0 \neq f(0)$. Si j'avais écrit dans la définition de limite “pour tout $0 \leq |x - 0| < \delta$”, la situation serait tout autre parce que $|f(0) - 0| = 1$. On observe sur cet exemple un phénomène qui est vrai en général, à savoir que l'existence de la limite d'une fonction f en un point x_* est tout à fait indépendante de la valeur que prend f en ce point. Comme je vous le disais, c'est une subtilité, ne vous inquiétez pas si elle vous échappe dans une première lecture.

4.1.5 Utiliser le graphe

L'utilisation du graphe permet souvent d'illustrer visuellement une nouvelle notion et donc de mieux l'appréhender. Considérons l'exemple de la limite. Pour cela, regardez d'abord la figure 4.4 où j'ai tracé le graphe d'une fonction f ayant comme limite ℓ en x_* et constatez que $|f(x) - \ell|$ est la distance entre le point $(x, f(x))$ du graphe de f et la droite horizontale $y = \ell$. Choisissez ensuite une valeur pour ϵ et tracez deux droites horizontales $y = \ell - \epsilon$ et $y = \ell + \epsilon$ un peu au dessus et un peu en dessous de la première. Tracez finalement deux droites verticales $x = x_* - \delta$ et $x = x_* + \delta$ et regardez la partie du graphe de f au

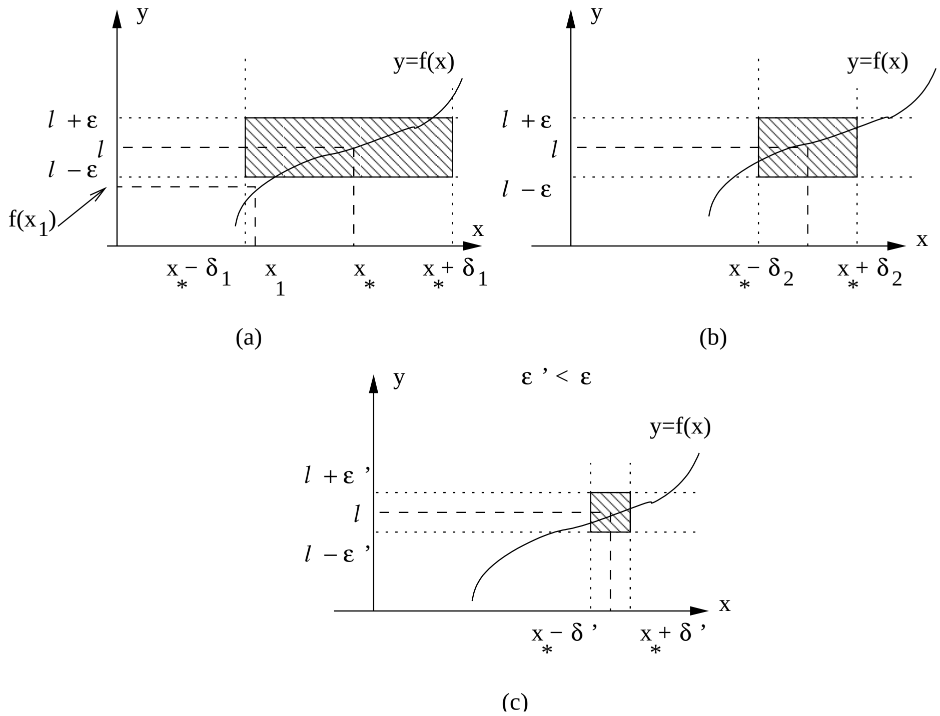

FIG. 4.4 – $\lim_{x \to x_*} f(x) = \ell$

dessus de l'intervalle $]x_* - \delta, x_* + \delta[$. La définition de limite dit que f admet $\ell \in \mathbb{R}$ comme limite en x_* si on peut choisir δ tel que cette partie du graphe se trouve entre les deux droites horizontales $y = \ell - \epsilon$ et $y = \ell + \epsilon$. Il est clair que si on choisit δ trop grand, la condition ne sera pas satisfaite, comme on le voit sur la figure 4.4 (a). On voit en effet sur cette figure que $|f(x_1) - \ell| > \epsilon$, tandis que $|x_1 - x_*| < \delta_1$. Dans la figure 4.4 (b), j'ai choisi $\delta = \delta_2 < \delta_1$ et on voit que cette fois-ci, la condition est satisfaite. Par ailleurs, au fur et à mesure que l'on prend ϵ plus petit, comme dans la figure 4.4 (c), la condition qu'on impose sur le choix de δ devient plus restrictive et on sera typiquement amené à prendre également δ plus petit. Si vous êtes mal à l'aise avec ces explications, c'est sans doute parce que vous n'avez pas l'habitude de manipuler les graphes de fonctions de façon un peu abstraite. Je vous conseille de revoir la Section 3.3 et de faire ou refaire les exercices que j'y propose.

Le lecteur s'entraîne

1. Trouver δ tel que, pour tout $|x - 5| < \delta$, $|3x^2 + 2x - 85| < 0,1$. Même question pour $|3x^2 + 2x - 85| < 0,01$. Utiliser sa calculatrice pour vérifier le résultat.

4.2 Limite d'une fonction : premières propriétés

4.2.1 Limite de sommes, produits et quotients

A grands coups de ϵ et de δ, nous avons montré dans la section précédente que $\lim_{x\to 2} x^3 = 8$ et que $\lim_{x\to x_*} x = x_*$. Que dire plus généralement de $\lim_{x\to x_*} P(x)$ lorsque P est un polynôme ? On a bien évidemment, vous vous y attendez :

Lemme 4.4. *Soit P, Q des polynômes. Alors, pour tout $x_* \in \mathbb{R}$ on a*

$$\lim_{x\to x_*} P(x) = P(x_*).$$

Si $Q(x_*) \neq 0$, on a également

$$\lim_{x\to x_*} \frac{P(x)}{Q(x)} = \frac{P(x_*)}{Q(x_*)}.$$

La démonstration de ce lemme sera très facile une fois qu'on aura montré :

Proposition 4.5. *Soient $f, g : D \to \mathbb{R}$ et $x_* \in \bar{D}$. Supposons que $\lim_{x\to x_*} f(x)$ et $\lim_{x\to x_*} g(x)$ existent. Alors*

(i) $\lim_{x\to x_*} (f+g)(x) = \lim_{x\to x_*} f(x) + \lim_{x\to x_*} g(x)$ *;*

(ii) $\lim_{x\to x_*} (fg)(x) = \lim_{x\to x_*} f(x) \ \lim_{x\to x_*} g(x)$ *;*

(iii) Si $\lim_{x\to x_*} g(x) \neq 0$,

$$\lim_{x\to x_*} \frac{f}{g}(x) = \frac{\lim_{x\to x_*} f(x)}{\lim_{x\to x_*} g(x)}.$$

Vous avez appris ces règles de calcul, sans démonstration, au lycée : “la limite d'une somme est la somme des limites”, *etc.*. Maintenant que nous disposons d'une définition précise de “limite”, nous pourrons les démontrer. C'est un excellent exercice dans la manipulation des ϵ et des δ, mais c'est assez difficile pour le débutant. Je vais donc d'abord montrer le Lemme 4.4, en admettant la Proposition 4.5, que je démontrerai après.

Démonstration du Lemme 4.4 : Je vais d'abord montrer que, pour tout $n \in \mathbb{N}$, on a

$$\lim_{x\to x_*} x^n = x_*^n.$$

Pour $n = 0, 1$, nous l'avons montré dans le Lemme 4.3 (i). En remarquant que $x^n = x \cdot x^{(n-1)}$, on démontre le cas général à l'aide de la Proposition 4.5 (ii) par un simple raisonnement par récurrence que je vous laisse le soin de rédiger en détail. Soit maintenant

$$P(x) = a_0 + a_1 x + \cdots + a_N x^N$$

un polynôme, alors on a

$$\lim_{x\to x_*} P(x) = \lim_{x\to x_*} a_0 + \lim_{x\to x_*} a_1 x \cdots + \lim_{x\to x_*} a_N x^N = P(x_*),$$

par une simple application de la Proposition 4.5 (i)-(ii). La deuxième partie du lemme est une conséquence immédiate de la première et de la Proposition 4.5 (iii). □

J'espère que vous serez d'accord avec moi pour dire que ce n'était vraiment pas dur. Je n'ai, en particulier, pas dû utiliser des ϵ ou des δ. Tournons-nous maintenant vers la démonstration de la Proposition 4.5, où les choses se corsent. Vous pourriez d'ailleurs, dans une première lecture, décider d'ignorer les démonstrations qui restent à faire dans cette section, pour y revenir plus tard.

Il est maintenant indispensable d'avoir bien compris la Section 3.5… . Nous aurons en outre, au cours de la démonstration de la Proposition 4.5, besoin des propriétés suivantes, qu'il convient de mettre en évidence, puisqu'elles serviront encore à de maintes reprises.

Lemme 4.6. *Si $f : D \to \mathbb{R}$ admet une limite ℓ en $x_* \in \overline{D}$, alors il existe un intervalle I contenant x_* ayant la propriété suivante : quelque soit $x \in I \cap D, x \neq x_*$, on a*

$$\frac{|\ell|}{2} \leq |f(x)| \leq |\ell| + 1. \tag{4.4}$$

En particulier, si f a une limite en x_*, alors f est bornée sur un intervalle autour de x_*. De plus, si $\ell > 0$, il existe un intervalle I contenant x_* ayant la propriété suivante : quelque soit $x \in I \cap D, x \neq x_*$, on a :

$$f(x) \geq \ell/2 > 0.$$

Les affirmations de ce lemme devraient vous paraître évidentes : en effet, en ce qui concerne la deuxième par exemple, si $f(x)$ est proche de $\ell > 0$ lorsque x est proche de x_*, alors $f(x)$ est certainement plus grand que $\ell/2$ et donc positif. Je vous invite à illustrer cette affirmation en traçant la droite $y = \ell/2$ sur la figure 4.1 : vous constaterez aisément que le graphe $y = f(x)$ est au dessus de cette horizontale lorsque x n'est pas trop loin de x_*, ce qui veut dire que $f(x) \geq \ell/2$ pour de tels x. La rédaction précise de cette idée simple est un peu fastidieuse et se trouve dans la démonstration du lemme ci-dessous. En guise d'échauffement, je vous propose encore un exercice, dont l'utilité deviendra évident dans les démonstrations de cette section.

Exercice 4.7. *Soit $f : D \to \mathbb{R}$ et $x_* \in \bar{D}, \ell \in \mathbb{R}$. Montrer que les affirmations suivantes sont toutes équivalentes :*

$$\begin{aligned}
&(i) && \forall\epsilon > 0, \exists\delta > 0, \forall x \in D, (0 < |x - x_*| < \delta) \Rightarrow |f(x) - \ell| < \epsilon && (4.5)\\
&(ii) && \forall\epsilon_1 > 0, \exists\delta_1 > 0, \forall x \in D, (0 < |x - x_*| < \delta_1) \Rightarrow |f(x) - \ell| < \epsilon_1 && (4.6)\\
&(iii) && \forall\epsilon > 0, \exists\delta > 0, \forall x \in D, (0 < |x - x_*| \leq \delta) \Rightarrow |f(x) - \ell| \leq \epsilon && (4.7)\\
&(iv) && \forall\epsilon > 0, \exists\delta > 0, \forall x \in D, (0 < |x - x_*| \leq \delta \Rightarrow |f(x) - \ell| < \epsilon && (4.8)\\
&(v) && \forall\epsilon > 0, \exists\delta > 0, \forall x \in D, (0 < |x - x_*| < \delta) \Rightarrow |f(x) - \ell| \leq \epsilon && (4.9)\\
&(vi) && \forall\epsilon > 0, \exists\delta > 0, \forall x \in D, (0 < |x - x_*| < \delta) \Rightarrow |f(x) - \ell| \leq 2\epsilon && (4.10)
\end{aligned}$$

Solution : Le (ii) est équivalent au (i) parce que c'est la même chose avec d'autres symboles : dire qu'une chose est vraie pour tout réel ϵ ou pour tout réel ϵ_1 est évidemment la même chose. Montrons que le (ii) implique le (iii) ; les autres implications se démontrent de la même façon. Soit $\epsilon > 0$. En posant $\epsilon_1 = \epsilon$ dans le (ii), on sait qu'il existe $\delta_1 > 0$ tel que, quelque soit $x \in D$,

$$0 < |x - x_*| < \delta_1, \Rightarrow |f(x) - \ell| < \epsilon_1 = \epsilon.$$

Posons alors $\delta = \frac{\delta_1}{2}$ et on obtient quelque soit $x \in D$,

$$0 < |x - x_*| \leq \delta \Rightarrow 0 < |x - x_*| < \delta_1 \Rightarrow |f(x) - \ell| < \epsilon \Rightarrow |f(x) - \ell| \leq \epsilon,$$

ce qu'il fallait démontrer. Tout cela est vraiment fastidieux, mais c'est fort utile dans les démonstrations, comme vous le verrez.

Démonstration du Lemme 4.6* : En mettant $\epsilon = 1$ dans la définition de limite, on obtient tout de suite qu'il existe $\delta_1 > 0$ tel que, quelque soit $x \in D$,

$$0 < |x - x_*| < \delta_1, \Rightarrow |f(x) - \ell| < 1.$$

Par conséquant, utilisant les incontournables inégalités triangulaires, on a, pour un tel x :

$$|f(x)| = |f(x) - \ell + \ell| \leq |f(x) - \ell| + |\ell| \leq 1 + |\ell|, \tag{4.11}$$

et on obtient la deuxiéme inégalité de (4.4). Pour l'autre inégalité dans (4.4), elle est évidente si $\ell = 0$. Si non, on pose $\epsilon = |\ell|/2$ dans la définition de limite pour obtenir qu'il existe $\delta_2 > 0$ tel que, pour tout $x \in D$,

$$0 < |x - x_*| < \delta_2, \Rightarrow |f(x) - \ell| < |\ell|/2. \tag{4.12}$$

Maintenant, remarquons que

$$|f(x)| = |\ell - (\ell - f(x))| \geq |\ell| - |\ell - f(x)| \geq |\ell| - \frac{|\ell|}{2} = \frac{|\ell|}{2}, \tag{4.13}$$

où j'ai encore une fois fait appel à une des inégalités triangulaires, cette fois-ci dans la forme $|a-b| \geq |a| - |b|$. En posant $\delta = \min(\delta_1, \delta_2)$ et $I =]x_* - \delta, x_* + \delta[$, on obtient alors, à partir de (4.11), (4.12) et (4.13) le résultat (4.4).

Pour la deuxième partie du lemme il suffit maintenant de remarquer que $\ell - f(x) \leq |\ell - f(x)| = |f(x) - \ell|$ de façon à ce que (4.12) implique que, pour tout $x \in D$,

$$0 < |x - x_*| < \delta_2, \Rightarrow \ell - f(x) \leq |f(x) - \ell| \leq \ell/2$$

et donc $f(x) \geq \ell/2 > 0$. En posant $I =]x_* - \delta_2, x_* + \delta_2[$, le résultat s'ensuit. □

Démonstration de la Proposition 4.5* : Ecrivons $\lim_{x \to x_*} f(x) = \ell_1$, $\lim_{x \to x_*} g(x) = \ell_2$. On sait, par hypothèse, que quelque soit $\epsilon_1, \epsilon_2 > 0$, il existe $\delta_1, \delta_2 > 0$ tels que

$$0 < |x - x_*| < \delta_1, x \in D \quad \Rightarrow \quad |f(x) - \ell_1| < \epsilon_1, \tag{4.14}$$
$$0 < |x - x_*| < \delta_2, x \in D \quad \Rightarrow \quad |g(x) - \ell_2| < \epsilon_2. \tag{4.15}$$

(i) Soit ϵ un réel positif quelconque. Il faut montrer qu'il existe $\delta > 0$ tel que, quelque soit $x \in D$,

$$0 < |x - x_*| < \delta \Rightarrow |f(x) + g(x) - (\ell_1 + \ell_2)\,| < \epsilon.$$

Etant donné ϵ, il faut donc construire δ. Je procède ainsi. Posons $\epsilon_1 = \epsilon_2 = \epsilon/2$. Posons aussi $\delta = \min(\delta_1, \delta_2)$. Alors, (4.14)-(4.15) garantissent que

$$\begin{aligned} 0 < |x - x_*| < \delta, x \in D \Rightarrow |f(x) + g(x) - (\ell_1 + \ell_2)\,| &\leq |f(x) - \ell_1| + |g(x) - \ell_2| \\ &< \epsilon_1 + \epsilon_2 = \epsilon, \end{aligned}$$

et l'affaire est réglée !

(ii) Soit ϵ un réel positif quelconque. Il faut montrer qu'il existe $\delta > 0$ tel que, quelque soit $x \in D$,

$$0 < |x - x_*| < \delta, \Rightarrow |f(x)g(x) - \ell_1\ell_2| < \epsilon.$$

Je commence par l'astuce suivante :

$$|f(x)g(x) - \ell_1\ell_2| = |f(x)g(x) - (\ell_1 g(x) - \ell_1 g(x)) - \ell_1\ell_2|.$$

A quoi bon, vous me direz, d'ajouter $0 = (\ell_1 g(x) - \ell_1 g(x))$ à l'expression considérée ? Voici la réponse :

$$\begin{aligned} |f(x)g(x) - \ell_1\ell_2| &= |(f(x) - \ell_1)g(x) + \ell_1(g(x) - \ell_2)| \\ &\leq |f(x) - \ell_1|\ |g(x)| + |\ell_1|\ |g(x) - \ell_2| \qquad (4.16) \end{aligned}$$

Le Lemme 4.6 garantit l'existence d'un $\delta' > 0$ tel que $|g(x)| \leq 1 + |\ell_2|$, pour tout $0 < |x - x_*| < \delta'$. Posons maintenant $\epsilon_1 = \frac{\epsilon}{2(1+|\ell_2|)}$ et $\epsilon_2 = \frac{\epsilon}{2(|\ell_1|+1)}$. Posons aussi $\delta = \min(\delta_1, \delta_2, \delta')$. Alors, (4.14)-(4.15) et (4.16) garantissent que, quelque soit $x \in D$,

$$0 < |x - x_*| < \delta, x \in D \Rightarrow |f(x)g(x) - \ell_1\ell_2| \leq \epsilon_1\ (1 + |\ell_2|) + |\ell_1|\ \epsilon_2 \leq \epsilon$$

et l'affaire est réglée !

(iii) La méthode de démonstration reste la même que dans les parties (i) et (ii). Il faut juste une nouvelle astuce pour démarrer. D'abord, je vais montrer le résultat lorsque $f(x) = 1$. Le cas général est alors une application de la partie (ii) :

$$\lim_{x \to x_*} \frac{f(x)}{g(x)} = \lim_{x \to x_*} f(x) \lim_{x \to x_*} \frac{1}{g(x)} = \frac{\lim_{x \to x_*} f(x)}{\lim_{x \to x_*} g(x)}.$$

On a

$$|\frac{1}{g(x)} - \frac{1}{\ell_2}| = \frac{|g(x) - \ell_2|}{|g(x)\ell_2|}.$$

Comme $\ell_2 \neq 0$, le Lemme 4.6 nous garantit l'existence de $\delta_3 > 0$ tel que, pour tout $x \in]x_* - \delta_3, x_* + \delta_3[$, $|g(x)| \geq |\ell_2|/2$ et donc $|g(x)|^{-1} \leq 2/|\ell_2|$. Donc, pour de tels x

$$|\frac{1}{g(x)} - \frac{1}{\ell_2}| \leq |g(x) - \ell_2| \frac{2}{|\ell_2|^2}. \qquad (4.17)$$

On peut alors conlure ainsi. Soit $\epsilon > 0$. Posons $\epsilon_2 = \frac{\epsilon|\ell_2|^2}{2}$ et $\delta = \min(\delta_2, \delta_3)$. On obtient alors de (4.15) et de (4.17) que, quelque soit $x \in D$,

$$0 < |x - x_*| < \delta \Rightarrow |\frac{1}{g(x)} - \frac{1}{\ell_2}| \leq \epsilon$$

ce qu'il fallait démontrer. □

J'espère que le rôle crucial joué par les inégalités triangulaires dans cette démonstration ne vous a pas échappé.

4.2.2 Les gendarmes

Deux dernières propriétés simples et utiles de la limite d'une fonction concernent le passage à la limite dans les inégalités et sont rassemblées dans la proposition suivante :

Proposition 4.8. *(i) Soient $f, g : D \to \mathbb{R}$ et $x_* \in \bar{D}$. Supposons que, pour tout $x \in D$, $f(x) \leq g(x)$ et que $\lim_{x \to x_*} f(x)$ et $\lim_{x \to x_*} g(x)$ existent. Alors*

$$\lim_{x \to x_*} f(x) \leq \lim_{x \to x_*} g(x).$$

(ii) Soient $f, g, h : D \to \mathbb{R}$ et $x_* \in \bar{D}$. Supposons que, pour tout $x \in D$,

$$f(x) \leq h(x) \leq g(x)$$

et que $\lim_{x \to x_*} f(x)$ et $\lim_{x \to x_*} g(x)$ existent et sont égales :

$$\lim_{x \to x_*} f(x) = \ell = \lim_{x \to x_*} g(x).$$

Alors $\lim_{x \to x_*} h(x)$ existe et

$$\lim_{x \to x_*} h(x) = \ell.$$

Le résultat énoncé dans la partie (ii) de la Proposition 4.8 est connu sous le nom de *théorème des gendarmes*. Nous en verrons une autre version, pour les suites. Ce résultat est parfois utile pour montrer l'existence d'une limite dont on ne sait pas calculer la valeur. Nous l'utiliserons en particulier dans la section suivante pour étudier les limites des fonctions trigonométriques en un point de leur domaine.

Exercice 4.9. *Illustrer la Proposition 4.8 avec quelques graphes.*

D'emonstration* : Je continuerai à utiliser les notations de la démonstration précédente. (i) Ici, j'utiliserai un raisonnement par l'absurde. Supposons donc que $\ell_1 > \ell_2$. Le Lemme 4.6 implique alors qu'il existe $\delta > 0$ tel que

$$0 < |x - x_*| < \delta, x \in D \Rightarrow f(x) > g(x). \tag{4.18}$$

En effet, si $\ell_1 > \ell_2$, alors $\lim_{x \to x_*} (f - g)(x) = \ell_1 - \ell_2 > 0$ et donc (Lemme 4.6) $f(x) - g(x) \geq \frac{\ell_1 - \ell_2}{2} > 0$ pour x proche de x_*, ce qui implique (4.18). Mais (4.18) contredit l'hypothèse que pour tout $x \in D, f(x) \leq g(x)$.

(ii) Ecrivons $\ell = \ell_1 = \ell_2$. Soit $\epsilon > 0$. En posant $\epsilon_1 = \epsilon_2$ et $\delta = \min(\delta_1, \delta_2)$, (4.14) et (4.15) impliquent que, pour tout $x \in D$,

$$0 < |x - x_*| < \delta, \Rightarrow -\epsilon \leq f(x) - \ell \leq h(x) - \ell \leq g(x) - \ell \leq \epsilon.$$

Par conséquent

$$0 < |x - x_*| < \delta, x \in D \Rightarrow |h(x) - \ell| \leq \epsilon.$$

□

Je termine par un commentaire. Les résultats de cette section sont très importants, mais pas de la même façon que le théorème de Bézout, par exemple. Ce dernier est une piece maîtresse de l'arithmétique. Il n'est pas du tout évident, même s'il est assez facile à démontrer. Les résultats ci-dessus, par contre, sont évidents dès qu'on comprend de façon intuitive la notion de limite. Par conséquent, n'importe quel mathématicien vous dira qu'il les considère comme triviaux. Remarquez, par ailleurs, qu'aucun d'eux ne porte le nom d'un mathématicien et que je ne les ai pas regroupés en un théorème, mais plus modestement dans des lemmes et des propositions. Néanmoins, ces résultats sont difficiles à démontrer pour celui qui n'a pas l'habitude de manipuler les arguments epsilon-delta ! Il s'avère que les astuces et raisonnements utilisés dans les démonstrations des Propositions 4.5 et 4.8 et du Lemme 4.6 seront encore utilisés à mainte reprise ; il est donc indispensable de se les approprier. Dans ce sens, on peut prétendre que les techniques de démonstration sont dans cette section plus importantes que les résultats obtenus.

Exercice 4.10. *L'affirmation suivante, est elle vraie ou fausse ? "Soient $f, g : D \to \mathbb{R}$ et $x_* \in \bar{D}$. Supposons que, pour tout $x \in D$, $f(x) < g(x)$ et que $\lim_{x \to x_*} f(x)$ et $\lim_{x \to x_*} g(x)$ existent. Alors*

$$\lim_{x \to x_*} f(x) < \lim_{x \to x_*} g(x)."$$

Solution : Elle est fausse, l'inégalité stricte peut être perdue dans la limite ! Pensez à $f(x) = 0$, $g(x) = x^2$, $D = \mathbb{R}_*$ et $x_* = 0$.

4.3 Les fonctions trigonométriques

Je veux ici rappeler la définition *géométrique* des fonctions sinus et cosinus. Souvenons-nous d'abord la définition du nombre π : c'est le périmètre du demi-cercle de rayon 1. On *admettra* pour la suite que c'est aussi l'aire du cercle de rayon 1 et que

$$3,141592 < \pi < 3,141593.$$

Considérons alors le cercle de rayon 1, centré à 0 (Fig. 4.5), et sur ce cercle un point P, de coordonnées x et y. Soit θ la longueur d'arc, mesurée le long du cercle, entre les points B et P (dans le sens inverse des aiguilles d'une montre). Clairement, $0 \leq \theta < 2\pi$. On *définit* alors

$$x = \cos\theta, y = \sin\theta.$$

Ceci définit le sinus et le cosinus comme des fonctions de domaine $[0, 2\pi[$, à

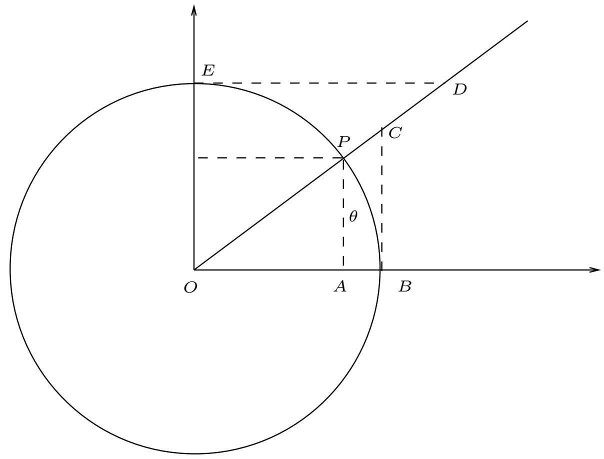

FIG. 4.5 – La définition des fonctions trigonométriques

valeurs dans $\mathbb{R}$. On peut les étendre à des fonctions de $\mathbb{R}$ dans $\mathbb{R}$, par périodicité, c'est à dire en posant, pour tout $x \in \mathbb{R}$,

$$\sin(x + 2\pi) = \sin x, \quad \cos(x + 2\pi) = \cos x.$$

On définit aussi $\tan\theta = \frac{\sin\theta}{\cos\theta}, \cot\theta = \frac{\cos\theta}{\sin\theta}$. En termes géométriques, $\tan\theta$ est la distance entre les point B et C de la figure, et $\cot\theta$ entre les points D et E. Les définitions entraînent immédiatement que

$$\sin^2\theta + \cos^2\theta = 1. \tag{4.19}$$

Quelques arguments simples de géométrie permettent de démontrer également [HW] :

$$\cos(\theta_1 + \theta_2) = \cos\theta_1 \cos\theta_2 - \sin\theta_1 \sin\theta_2, \tag{4.20}$$

et

$$\sin(\theta_1 + \theta_2) = \sin\theta_1 \cos\theta_2 + \cos\theta_1 \sin\theta_2. \tag{4.21}$$

Il faut absolument connaître par coeur les trois relations ci-dessus. Beaucoup d'autres sont souvent utiles, mais elles se déduisent facilement des trois précédentes par un peu de calcul élémentaire et il vaut mieux apprendre à les déduire rapidement que les apprendre par coeur.

Exercice 4.11. *Montrer que*

$$\tan(\theta_1 + \theta_2) = \frac{\tan\theta_1 + \tan\theta_2}{1 - \tan\theta_1 \tan\theta_2}.$$

Pour étudier la continuité et la dérivabilité des fonctions trigonométriques, nous aurons besoin des limites suivantes :

Lemme 4.12.

$$\lim_{x\to 0} \sin x = 0, \ \lim_{x\to 0} \frac{\sin x}{x} = 1, \lim_{x\to 0} \frac{\cos x - 1}{x} = 0$$

et, pour tout $x_* \in \mathbb{R}$, on a

$$\lim_{x\to x_*} \sin x = \sin x_*, \quad \lim_{x\to x_*} \cos x = \cos x_*.$$

Démonstration : La démonstration de ces résultats est de nature géométrique, et utilisera également le théorème des gendarmes. On remarque d'abord que l'aire du triangle OBP $(= \frac{1}{2}\sin\theta)$ est inférieure à celle du secteur de cercle OBP $(= \frac{1}{2}\theta)$, qui est inférieure à celle du triangle OBC $(= \frac{1}{2}\tan\theta)$. On a donc, pour $0 \leq \theta \leq \frac{\pi}{2}$:

$$\frac{1}{2}\sin\theta \leq \frac{1}{2}\theta \leq \frac{1}{2}\tan\theta. \tag{4.22}$$

De la première inégalité on conclut facilement, en utilisant que $\sin(-\theta) = -\sin\theta$, que, pour tout $-\frac{\pi}{2} \leq \theta \leq \frac{\pi}{2}$, on a

$$0 \leq |\sin\theta| \leq |\theta|,$$

d'où l'on conclut que $\lim_{\theta\to 0}\sin\theta = 0$, en invoquant le théorème des gendarmes. On en déduit facilement (en utilisant (4.19) que $\lim_{\theta\to 0}\cos\theta = 1$. Les inégalités de (4.22) permettent par ailleurs d'établir que

$$\cos\theta \leq \frac{\sin\theta}{\theta} \leq 1.$$

Une dernière application du théorème des gendarmes permet alors de conclure que $\lim_{\theta\to 0}\frac{\sin\theta}{\theta} = 1$. Les autres résultats s'ensuivent en application des identités trigonométriques (4.20) et (4.21) □

4.4 Racines

J'ai déjà signalé, dans la Section 1.7, que pour tout réel $b \geq 0$ il existe un unique réel $a \geq 0$ tel que $a^2 = b$. On écrit $a = b^{1/2}$ ou $a = \sqrt{b}$. De la même façon, je vais admettre que, pour tout $p \in \mathbb{N}^*$, et pour tout réel $b \geq 0$, il existe un unique $a \geq 0$ tel que $a^p = b$. On écrit $a = b^{1/p}$. Cette propriété des nombres réels peut être vue comme une conséquence du théorème des valeurs intermédiaires, que nous étudierons dans le Chapitre 8. On définit également, pour tout $r = p/q \in \mathbb{Q}$, $b^r = (b^{1/q})^p$. On vérifie alors facilement (Faites le !), *à partir de ces définitions*, les règles de calcul élémentaires comme

$$b'^r b^r = (b'b)^r, \quad b^r b^{r'} = b^{r+r'}, (b^r)^{r'} = b^{rr'} \ etc..$$

Nous admettrons pour le moment que

$$\lim_{x \to x_*} x^r = x_*^r.$$

Cette propriété pourra être démontrée comme conséquence du Théorème 8.20, bien plus tard dans ce cours (Section 8.8).

4.5 Limites de suites : définition

Même si nous avons réussi à déterminer la limite de polynômes, des fractions rationnelles et des fonctions trigonométriques, nous n'avons toujours pas de critère performant pour montrer qu'une fonction n'a pas de limite en un point. Pour montrer, par exemple, directement à partir de la définition de limite, que la fonction $\sin 1/x$ et la fonction de Heaviside n'ont pas de limite en 0, est pénible. Mieux vaut utiliser le résultat du Corollaire 4.27 ci-dessous. Pour énoncer et démontrer ce résultat, nous avons besoin de faire une première incursion dans la théorie des suites, qui a évidemment bien d'autres applications, comme l'introduction le suggère, et comme nous le verrons plus tard.

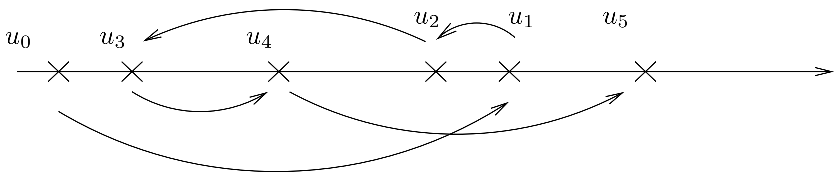

FIG. 4.6 – Une suite

Je vous ai déjà rappelé qu'une suite est une famille de nombres $(u_n)_{n\in\mathbb{N}}$, appelés les termes de la suite qui sont indexés par les entiers $n \in \mathbb{N}$ et que l'on peut voir comme une fonction de $\mathbb{N}$ dans $\mathbb{R}$. J'écrirai souvent tout simplement "la suite (u_n)" ou "la suite de terme général u_n". Pour bien comprendre les différentes notions concernant les suites, il est bon de disposer d'une représentation un peu plus concrète et imagée des suites. La représentation qui est le plus souvent utile est celle qui consiste à placer les termes successifs sur un axe : on s'imagine une puce qui saute le long d'un axe et qui, à l'instant n, se trouve au point de coordonnée u_n (Fig. 4.6). Considérons quelques exemples :

$$a_n = n^2, b_n = \sin n, c_n = \frac{n}{n^2+2}.$$

Ces suites sont toutes de la forme $u_n = f(n)$, avec f une fonction. On peut obtenir une image des u_n en traçant d'abord le graphe de f, pour ensuite indiquer sur l'axe verticale les valeurs $u_0, u_1, u_2, \ldots$. C'est alors comme si la puce saute le long de l'axe verticale comme on peut le constater pour la suite (b_n) dans la figure 4.7.

Exercice 4.13. *Tracer le graphe de la fonction* $f(x) = \frac{x}{x^2+2}$ *et utiliser le pour dessiner les termes de la suite* (c_n) *le long de l'axe vertical.*

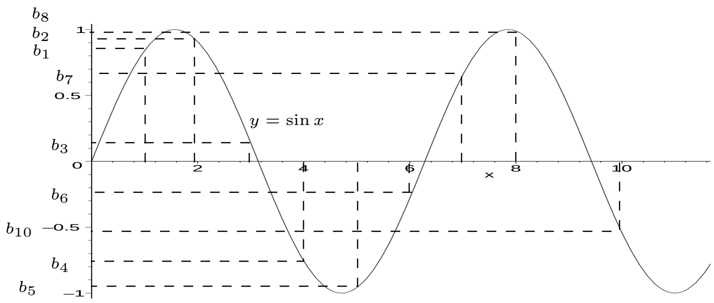

FIG. 4.7 – Quelques termes de la suite $b_n = \sin n$

La question centrale dans l'étude des suites est celle de leur comportement lorsque n tend vers l'infini. C'est, si vous voulez, la question : "Que fait la puce à la longue ?" La réponse est différente pour les suites $(a_n), (b_n)$ et (c_n) et la notion de limite d'une suite permet de distinguer le comportement de (c_n) de celui de (a_n) et (b_n).

Définition 4.14. *On dit que la suite* (u_n) *admet* $\ell \in \mathbb{R}$ *pour limite si pour tout* $\epsilon > 0$ *il existe* $N \in \mathbb{N}$ *tel que, pour tout* $n \geq N$ *on a*

$$|u_n - \ell| < \epsilon.$$

On dit aussi que la suite converge vers ℓ. On écrit

$$\lim_{n \to +\infty} u_n = \ell,$$

ou plus brièvement $u_n \to \ell$. Une suite qui a une limite $\ell \in \mathbb{R}$ est appelée convergente. Une suite qui n'est pas convergente est divergente. En termes de "puces", il est clair que la suite (u_n) tend vers ℓ si et seulement si la puce est aussi proche que l'on veut de ℓ, pourvu qu'on attende assez longtemps, c'est à dire pourvu que n soit assez grand. En regardant les exemples ci-dessus, on se convainc facilement que la suite (c_n) tend vers 0, tandis que (b_n) ne converge pas. On constate en effet sur la figure 4.7 que si la puce se trouve successivement à $y = b_1, b_2, b_3, \ldots$, alors elle sautille de haut en bas le long de l'axe, restant toujours entre $y = 1$ et $y = -1$, mais ne s'approchant d'aucun point de l'intervalle $[-1, 1]$ en particulier. Je donnerai des démonstrations de ces affirmations plus tard.

En complète analogie avec la limite de fonctions, on montre que la limite d'une suite est unique si elle existe et également que, quelque soit $k \in \mathbb{Z}$

$$\lim_{n\to+\infty} u_n = \lim_{n\to+\infty} u_{n+k},$$

ainsi que

$$\lim_{n\to+\infty} u_n = 0 \Leftrightarrow \lim_{n\to+\infty} |u_n| = 0.$$

La suite (a_n) ci-dessus diverge, mais elle a un comportement différent de la suite (b_n) : elle "tend vers l'infini". Donnons tout de suite un sens précis à cette notion importante.

Définition 4.15. *On dit qu'une suite (u_n) tend vers $+\infty$ (respectivement $-\infty$) si pour tout $M \in \mathbb{R}$, il existe $N \in \mathbb{N}$ tel que, pour tout entier $n \geq N$, on a*

$$u_n \geq M \ (\textit{respectivement } u_n \leq M).$$

On dit aussi que (u_n) a $+\infty$ (respectivement $-\infty$) comme limite, mais il faut faire très attention à la terminologie : une suite qui tend vers plus ou moins l'infini diverge ! D'ailleurs, une telle suite n'est pas bornée, or une suite convergente est bornée, comme on le montrera dans le Lemme 4.18. On écrira

$$\lim_{n\to+\infty} u_n = +\infty, \text{ ou } \ u_n \to +\infty,$$

et on continuera à dire dans ces cas que "la limite existe", mais que "la limite n'est pas finie" ! En d'autres termes, dire que la suite est convergente n'est pas la même chose que dire qu'elle a une limite : une suite est convergente si et seulement si elle a une limite *finie* $\ell \in \mathbb{R}$.

Voici encore un peu de terminologie simple :

Définition 4.16. *Une suite (u_n) est bornée si il existe $M \in \mathbb{R}$ tel que, pour tout $n \in \mathbb{N}$, $|u_n| \leq M$. Elle est minorée si il existe $M \in \mathbb{R}$ tel que, pour tout $n \in \mathbb{N}$, $u_n \geq M$ et elle est majorée si il existe $M \in \mathbb{R}$ tel que, pour tout $n \in \mathbb{N}$, $u_n \leq M$.*

Exercice 4.17. *Montrer qu'une suite est bornée si elle est minorée et majorée. Donner un exemple d'une suite majorée, mais pas bornée et un d'une suite minorée mais pas bornée. Les suites $(a_n), (b_n), (c_n)$ ci-dessus sont-elles minorées, majorées, bornées ?*

Les suites $(a_n), (b_n), (c_n)$ données comme exemples ci-dessus n'ont pas beaucoup d'intérêt. Comme les considérations de l'introduction le suggèrent, les suites

$$s_n = \sum_{k=0}^{n} \frac{1}{k!}, \text{ et } t_n = \sum_{k=0}^{n} \frac{(-1)^k}{k!}$$

sont déjà nettement plus intéressantes et nous les étudierons en détail dans le chapitre suivant : elles sont convergentes, mais nous ne disposons pas encore des outils nécessaires pour le montrer. Plus généralement, une suite (u_n) est souvent donnée sous la forme

$$u_n = u_0 + \sum_{k=1}^{n} d_k, \tag{4.23}$$

ou encore $(n \geq 1)$

$$u_n = u_{n-1} + d_n.$$

Une suite qui est de la forme donnée en (4.23) est souvent appelée une *série*. Les suites (s_n) et (t_n) sont de ce type, avec $d_k = \frac{1}{k!}$ et $d_k = \frac{(-1)^k}{k!}$, respectivement. En termes de puces, si u_n désigne la position de la puce à l'instant n, d_n est le n-ième saut de la puce ! En effet $u_n - u_{n-1} = d_n$! La position u_n est tout naturellement la somme des sauts ! Dans le cas de s_n, la puce saute toujours vers la droite, et avance donc tout le temps : la suite s_n est croissante. Dans le cas de t_n, la puce saute alternativement vers la droite et la gauche. Je vous invite à calculer et à dessiner une dizaine de termes de chacune de ces suites, c'est tout à fait instructif.

4.6 Limites de suites : premières propriétés

Cette section sera une copie conforme de la Section 4.2. Je ne ferai d'ailleurs que peu de démonstrations, vous laissant le soin de tester votre compréhension de la Section 4.2 en adaptant les démonstrations qui y sont faites à la situation traitée ici (qui est, en fait, plus simple). Voici d'abord le pendant du Lemme 4.6.

Lemme 4.18. *(i) Toute suite convergente est bornée.*

(ii) Soit (u_n) une suite convergente de limite $\ell > 0$. Alors, il existe $N \in \mathbb{N}$ tel que $\forall n > N, u_n > \frac{\ell}{2} > 0$.

Démonstration : (i) Si (u_n) admet ℓ comme limite, nous savons qu'il existe $N \in \mathbb{N}$ tel que, pour tout $n \geq N$,

$$|u_n - \ell| \leq 1.$$

Donc, pour de tels n,

$$|u_n| = |u_n - \ell + \ell| \leq |u_n - \ell| + |\ell| \leq 1 + |\ell|.$$

Soit maintenant

$$M = \max \{|u_n| | 0 \leq n \leq N\},$$

alors on a

$$\forall n \in \mathbb{N}, |u_n| \leq \max\{M, 1 + |\ell|\},$$

ce qui montre que la suite est bornée. (ii) A vous de jouer. □

Proposition 4.19. *Soient* $(u_n), (v_n)$ *des suites convergentes. Alors*

(i) $\lim_{n\to\infty}(u_n + v_n) = \lim_{n\to\infty} u_n + \lim_{n\to\infty} v_n$ *;*

(ii) $\lim_{n\to\infty} u_n v_n = \left(\lim_{n\to\infty} u_n\right)\left(\lim_{n\to\infty} v_n\right)$ *;*

(iii) Si $\lim_{n\to\infty} v_n \neq 0$,

$$\lim_{n\to\infty}\frac{u_n}{v_n} = \frac{\lim_{n\to\infty} u_n}{\lim_{n\to\infty} v_n}.$$

Démonstration* : Je ne démontrerai que le (ii). Je vous invite à comparer cette démonstration à celle de Proposition 4.5 (ii). Ecrivons $\lim_{n\to+\infty} u_n = \ell_1$, $\lim_{n\to+\infty} v_n = \ell_2$. On sait par hypothèse que, quelque soit $\epsilon_1 > 0, \epsilon_2 > 0$, il existe $N_1, N_2 \in \mathbb{N}$ tel que,

$$n \geq N_1 \quad\Rightarrow\quad |u_n - \ell_1| < \epsilon_1, \tag{4.24}$$
$$n \geq N_2 \quad\Rightarrow\quad |v_n - \ell_2| < \epsilon_2. \tag{4.25}$$

Soit $\epsilon > 0$. Il faut montrer qu'il existe $N \in \mathbb{N}$ tel que

$$n \geq N \Rightarrow |u_n v_n - \ell_1\ell_2| < \epsilon.$$

Etant donné $\epsilon > 0$, il faut donc construire N. On a, pour tout $n \in \mathbb{N}$,

$$|u_n v_n - \ell_1\ell_2| \leq |u_n - \ell_1|\ |v_n| + |\ell_1|\ |v_n - \ell_2|.$$

Comme (v_n) converge, on sait qu'il existe M tel que $|v_n| \leq M$, pour tout $n \in \mathbb{N}$ (Lemme 4.18). Posons $\epsilon_1 = \frac{\epsilon}{2M}$, $\epsilon_2 = \frac{\epsilon}{2(|\ell_1|+1)}$ et $N = \max\{N_1, N_2\}$. On a alors que

$$n \geq N \Rightarrow |u_n v_n - \ell_1\ell_2| < \epsilon_1 M + |\ell_1|\epsilon_2 \leq \epsilon,$$

ce qu'il fallait démontrer. □

L'équivalent de la Proposition 4.8 est :

Proposition 4.20. *(i) Soient* $(u_n), (v_n)$ *des suites. Supposons que, pour tout* $n \in \mathbb{N}$, $u_n \leq v_n$ *et que* $\lim_{n\to\infty} u_n$ *et* $\lim_{n\to+\infty} v_n$ *existent. Alors*

$$\lim_{n\to\infty} u_n \leq \lim_{n\to+\infty} v_n.$$

(ii) Soient $(u_n), (v_n), (w_n), n \in \mathbb{N}$ *des suites. Supposons que, pour tout* $n \in \mathbb{N}$, $u_n \leq v_n \leq w_n$ *et que* $\lim_{n\to\infty} u_n$ *et* $\lim_{n\to\infty} w_n$ *existent et sont égales :*

$$\lim_{n\to\infty} u_n = \lim_{n\to\infty} w_n.$$

Alors $\lim_{n\to\infty} v_n$ *existe et*

$$\lim_{n\to\infty} v_n = \lim_{n\to\infty} u_n = \lim_{n\to\infty} w_n.$$

La dernière partie de cette proposition vous est connue sous le nom de "théorème des gendarmes". Remarquez que l'hypothèse impose l'existence de la limite de (u_n) et de (v_n), mais la limite peut être infinie. Une dernière propriété fort utile est

Lemme 4.21. *Soient* $(u_n), (v_n)$ *des suites. Supposons que, pour tout* $n \in \mathbb{N}$, $u_n \leq v_n$ *et que* $\lim_{n\to\infty} u_n = +\infty$. *Alors*

$$\lim_{n\to\infty} v_n = +\infty.$$

Exercice 4.22. *Démontrer ce lemme et expliquer pourquoi il n'est pas un cas spécial de Proposition 4.20 (i). Formuler une version de ce lemme avec "limite* $-\infty$*".*

4.7 Quelques limites type

Voici quelques limites à connaître par coeur.

Lemme 4.23. *Soit* $k \in \mathbb{N}^*$, $a \in \mathbb{R}^*$.

(i) $\lim_{n\to+\infty} n^k = +\infty$;

(ii) Si $|a| < 1$, $\lim_{n\to+\infty} a^n = 0$. *Si* $a > 1$, $\lim_{n\to+\infty} a^n = +\infty$.

(iii) Si $a > 1$, $\lim_{n\to+\infty} \frac{a^n}{n^k} = +\infty$.

(iv) $\lim_{n\to+\infty} \frac{a^n}{n!} = 0$.

Il ne suffit en fait pas de connaître par coeur ces limites, il faut absolument vraiment comprendre ce qu'il se passe de façon intuitive dans chaque cas. Avant donc de vous donner une démonstration complète du lemme je tenterai de vous expliquer son intérêt. Le (i) et le (ii) sont intuitivement clair : la suite n^k est, pour k fixé, un *polynôme* dans la variable n et on ne s'étonne sans doute pas qu'elle tend vers l'infini. Pareillement, la dépendance de a^n en n est *exponentielle* et on s'attend bien que, lorsque $a > 1$, a^n tende aussi vers l'infini (Essayez avec $a = 2$, par exemple). Le (iii) et le (iv) sont déjà plus intéressants. Il s'agit ici de problèmes de croissances comparées ou encore de vitesses de convergence, dont on aura l'occasion de reparler plusieurs fois dans le futur. En effet, on sait par exemple d'après (i) et (ii) que les suites n^{100} ($k = 100$) et $(1,01)^n$ ($a = 1,01$) tendent toutes les deux vers $+\infty$. La question qui se pose alors est de savoir laquelle des deux "tend le plus vite" vers $+\infty$. Par exemple, prenant $n = 10$, on voit que 10^{100} est déjà un nombre gigantesque, tandis que $(1,01)^{10}$ ne vaut que $1,1$. Pareillement, lorsque $n = 1000$, $1000^{100} = 10^{300}$ est bien plus grand que $(1,01)^{1000}$ qui ne vaut que 20959 selon mon ordinateur. On pourrait donc penser que n^{100} croît plus vite que $(1,01)^n$. C'est pourtant faux. Par exemple, pour $n = 10^7$, on a $n^{100} = (10^7)^{100} = 10^{700}$ tandis que mon ordinateur m'informe que

$$(1,01)^n = (1,01)^{10^7} > 10^{43213}$$

ce qui est bien plus grand que 10^{700}. En fait, ce que le (iii) affirme est que, pour n assez grand, $(1,01)^n$ est beaucoup plus grand que n^{100}, puisque le quotient $(1,01)^n/n^{100}$ tend vers $+\infty$ (c'est à dire devient très grand) lorsque n devient grand ! En d'autres termes, la croissance *exponentielle* de $(1,01)^n$ finit par dominer la croissance polynomiale de n^{100}. Plus généralement, si (u_n) et (v_n) sont deux suites qui tendent vers $+\infty$ lorsque n tend vers $+\infty$, on dit que "(u_n) tend plus vite vers $+\infty$ que (v_n)" lorsque

$$\lim_{n\to+\infty} \frac{u_n}{v_n} = +\infty.$$

En effet, dans ce cas u_n/v_n sera "beaucoup plus grand que 1" lorsque n est suffisamment grand. Le (iii) affirme donc que, quelque soit $a > 1, k \in \mathbb{N}^*$,

"La suite a^n tend vers $+\infty$ plus vite que la suite n^k."

De façon générale, on retiendra qu'une croissance polynomiale est plus lente qu'une croissance exponentielle. On y reviendra encore une fois dans le Théorème 6.12. Avec cette terminologie, le (iv) du lemme dit finalement que la suite $n!$ tend vers plus l'infini plus vite que n'importe quelle suite a^n, c'est à dire plus vite que exponentiellement.

Un résultat utile dont je me servirai dans la démonstration du lemme est le suivant.

Lemme 4.24. *Soit* $(u_n > 0)$ *une suite. Alors*

$$\lim_{n\to+\infty} u_n = 0 \Leftrightarrow \lim_{n\to+\infty} \frac{1}{u_n} = +\infty.$$

Exercice 4.25. *Attention aux pièges ! Les affirmations suivantes sont-elles vraies ou fausses ?*

(i) Soit $(u_n \in \mathbb{R})$ *une suite. Alors*

$$\lim_{n\to+\infty} u_n = 0 \Leftrightarrow \lim_{n\to+\infty} \frac{1}{u_n} = +\infty.$$

(ii) Soit $(u_n \in \mathbb{R})$ *une suite. Alors*

$$\lim_{n\to+\infty} u_n = +\infty \Rightarrow \lim_{n\to+\infty} \frac{1}{u_n} = 0$$

(iii) Soit $(u_n \in \mathbb{R})$ *une suite. Alors*

$$\lim_{n\to+\infty} u_n = 0 \Rightarrow \left(\lim_{n\to+\infty} \frac{1}{u_n} = +\infty \text{ ou } \lim_{n\to+\infty} \frac{1}{u_n} = -\infty\right).$$

Solution : (i) C'est faux. Prendre $u_n = -1/n$.

(ii) C'est vrai ! Si $u_n \to +\infty$, u_n est positif à partir d'un certain rang et on peut appliquer le lemme pour conclure.

(iii) C'est faux. Prendre $u_n = \frac{(-1)^n}{n}$.

Démonstration : Montrons l'implication directe. Soit $M > 0$. On sait par hypothèse qu'il existe $N \geq 0$ tel que

$$n \geq N \Rightarrow u_n \leq \frac{1}{M}.$$

On a par ailleurs

$$\frac{1}{u_n} \geq M \Leftrightarrow u_n \leq \frac{1}{M}.$$

On conclut donc qu'il existe $N \geq 0$ tel que

$$n \geq N \Rightarrow \frac{1}{u_n} \geq M,$$

ce qu'il fallait démontrer.

Démonstration du Lemme 4.23 :

(i) Il n'y a rien à dire comme $n^k \geq n$.

(ii) Considérons $a > 1$ et montrons $a^n \to +\infty$. D'abord, ça doit vous paraître bizarre que je prétends avoir besoin d'une démonstration : après tout, ça paraît évident. Par exemple, si $a = 2$, on montre facilement par récurrence (Voir l'Exercice 2.1) que $2^n \geq n^2$ pour tout $n \geq 4$: le résultat s'ensuit via le théorème des gendarmes et le (i). Du coup, lorsque $a \geq 2$, on a $a^n \geq 2^n$ et donc on a, encore une fois grâce aux gendarmes, $a^n \to +\infty$ si $a \geq 2$. Mais cette démonstration ne permet pas de conclure pour $1 < a < 2$! Il me faut alors un argument un peu plus astucieux. Il suffit de remarquer que $a = 1 + (a - 1)$ et d'utiliser la formule du binôme pour obtenir

$$\begin{aligned} a^n &= (1 + (a-1))^n = \sum_{\ell=0}^{n} C_n^\ell (a-1)^\ell && (4.26) \\ &= 1 + n(a-1) + \frac{n(n-1)}{2}(a-1)^2 + \cdots + (a-1)^n && (4.27) \\ &\geq n(a-1) \end{aligned}$$

dont on conclut à nouveau en utilisant le théorème des gendarmes. L'autre partie de (ii) s'ensuit en utilisant le Lemme 4.24.

(iii) Il s'agit d'utiliser intelligemment (4.27). Par exemple, pour $k = 1$, on a, en retenant le troisiéme terme du membre de droite dans (4.27),

$$\frac{a^n}{n} \geq \frac{n(n-1)}{2n}(a-1)^2$$

d'où l'on conclut avec le théorème des gendarmes que $\frac{a^n}{n} \to +\infty$. Pour le cas général $k \in \mathbb{N}^*$, on remarque que

$$C_n^\ell = \frac{1}{\ell!} n(n-1)(n-2)(n-3)\ldots(n-\ell+1)$$

est, pour ℓ fixé, un polynôme de degré ℓ en n ayant $n^l/l!$ comme terme de plus haut degré. Donc, en utilisant (4.26) on obtient, en ne retenant que le terme avec $\ell = k+1$

$$\frac{a^n}{n^k} \geq \frac{1}{n^k} C_n^{k+1}(1-a)^{k+1}.$$

Comme $\frac{C_n^{k+1}}{n^k} \to +\infty$ (voir éventuellement l'Exercice) puisque C_n^{k+1} a $n^{k+1}/(k+1)!$ comme terme dominant, le résultat suit.

(iv) Je vais être bref. Soit $a > 1$. Posons $u_n = \frac{a^n}{n!}$. Choisissons un entier N tel que $N > 2a$. Comme pour tout $n \in \mathbb{N}^*$

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

on voit facilement que, pour tout $k \geq 1$,

$$u_{N+k} = \frac{a}{N+k} u_{N+k-1} \leq \frac{a}{N} u_{N+k-1} \leq \frac{1}{2} u_{N+k-1}$$

et donc, par récurrence, que

$$u_{N+k} \leq \frac{1}{2^k} u_N.$$

On en tire, via les fidèles gendarmes, que

$$\lim_{k \to +\infty} u_{N+k} = 0,$$

ce qui permet de conclure.

Le lecteur s'entraîne

1. Déterminer, si elles existent, les limites des suites de termes généraux suivants :

$$a)\ u_n = \frac{(-1)^n + 1}{n} \qquad b)\ u_n = \frac{(-1)^n}{n} \qquad c)\ u_n = \frac{3n^2 - 4n + 5}{-5n^2 + 3n - 1}$$

2. On pose, pour $n \geq 2$,

$$u_n = \left(1 - \frac{1}{2^2}\right)\left(1 - \frac{1}{3^2}\right) \cdots \left(1 - \frac{1}{n^2}\right).$$

Calculer (u_n). En déduire la limite de (u_n).

3. Les affirmations suivantes sont-elles vraies ou fausses (justifier) :

a) Si la suite $v_n = |u_n|$ converge, alors (u_n) converge.

b) Si une suite (u_n) est croissante alors la suite $v_n = u_n + \frac{1}{n}$ l'est aussi.

c) Si la suite nu_n est bornée, alors (u_n) converge.

d) Une suite convergente dont tous les termes sont des entiers est stationnaire à partir d'un certain rang.

e) De toute suite qui converge vers $+\infty$ on peut extraire une sous-suite strictement croissante.

f) Si $\cos u_n$ converge vers 1, alors (u_n) converge vers 0.

g) On ne modifie pas le comportement d'une suite en modifiant un nombre fini de ses termes.

h) Une suite à termes positifs qui converge vers 0 est décroissante.

i) Si (u_n) converge, alors la suite de terme général $u_{n+1} - u_n$ tend vers 0.

j) Si (u_n), une suite de réels non nuls, converge vers $+\infty$ alors $(1/u_n)$ converge.

k) Si (u_n), une suite de réels non nuls, converge vers 0 alors $(1/u_n)$ converge vers $+\infty$.

l) Si (u_n) est une suite convergente et (v_n) une suite divergente, alors $(u_n + v_n)$ est une suite divergente.

m) Si (u_n) est une suite convergente et (v_n) une suite divergente, alors $(u_n v_n)$ est une suite divergente.

n) Si (u_n) est une suite décroissante à termes positifs, alors elle tend vers 0.

o) Soit $f : \mathbb{R} \to \mathbb{R}$,

$$\lim_{x\to 0} f(x) = \ell \Rightarrow \lim_{x\to +\infty} f(\frac{1}{x}) = \ell.$$

p) Soit $f : \mathbb{R} \to \mathbb{R}$,

$$\lim_{x\to +\infty} f(\frac{1}{x}) = \ell \Rightarrow \lim_{x\to 0} f(x) = \ell.$$

q) Soit $f : \mathbb{R}^+ \to \mathbb{R}$,

$$\lim_{x\to +\infty} f(\frac{1}{x}) = \ell \Rightarrow \lim_{x\to 0} f(x) = \ell.$$

3. a) Soit (u_n) une suite qui converge vers un réel ℓ. On pose

$$v_n = \frac{u_1 + u_2 + \cdots + u_n}{n}.$$

Clairement, v_n est la moyenne des n premiers termes de la suite (u_n). Montrer que (v_n) converge aussi vers ℓ.
b) Peut-on montrer un résultat analogue si la suite (u_n) converge vers $+\infty$?

4. a) Soit (u_n) une suite de réels non nuls, et telle que pour tout $n \geq 1$, $\left|\frac{u_{n+1}}{u_n}\right| \leq k < 1$. Montrer que (u_n) converge vers 0.

b) Montrer que si $\left|\frac{u_{n+1}}{u_n}\right| \to L > 1$, alors (u_n) diverge.

c) Utiliser ce résultat pour étudier la suite de terme général $u_n = \frac{n^n}{n!}$.

5. Soit (u_n) une suite de réels positifs. Montrer que si $\frac{u_{n+1}}{u_n} \to 1$, pour $n \to +\infty$, alors il en va de même de $\sqrt[n]{u_n}$.

6. Etudier la suite $u_n = a^n$ lorsque $a < -1$ et comparer votre resultat au Lemme 4.23 (ii)

4.8 Limite d'une fonction en un point : un critère

Comme promis au début de la Section 4.5, je reviens maintenant au problème posé déjà en la sous-section 4.1.3, à savoir de trouver un critère simple à manipuler pour montrer qu'une fonction f n'a pas de limite en un point x_*. Pour vous convaincre qu'un tel critère sera fort utile, voici la démonstration directe du fait que la fonction de Heaviside n'admet pas de limite en 0. Soit ℓ un réel quelconque. Prenons $\epsilon = 1/4$ et montrons que pour tout $\delta > 0$, il existe $x \in D, 0 < |x-0| < \delta$ et $|f(x)-\ell| \geq \frac{1}{4}$, ce qui démontrera le résultat. En effet, si $x > 0$, on a $|f(x)-\ell| = |1-\ell|$ et si $x < 0$, on a que $|f(x)-\ell| = |\ell|$. Or, pour tout réel ℓ, on a que $|\ell| \geq \frac{1}{4}$ ou $|1-\ell| \geq \frac{1}{4}$. Donc dans tout intervalle $]-\delta, \delta[$ autour de $x_* = 0$, il existe un $x \neq 0$ tel que $|f(x)-\ell| \geq \frac{1}{4}$, ce qui termine la démonstration.

Cette démonstration est fastidieuse et il nous faut d'urgence développer des techniques qui permettent de montrer facilement que les fonctions que nous manipulons habituellement ont (ou n'ont pas) des limites. Le théorème et corollaire suivant s'avèrent souvent utiles dans ce contexte.

Théorème 4.26. *Soit $f : D \to \mathbb{R}$ une fonction et $x_* \in \bar{D}$. Soit $\ell \in \mathbb{R}$. Les deux affirmations suivantes sont équivalentes :*

(i) $\lim_{x \to x_*} f(x) = \ell$;

(ii) Pour toute suite $(x_n \in D \backslash \{x_*\})$ tel que $\lim_{n\to+\infty} x_n = x_*$, $\lim_{n\to+\infty} f(x_n) = \ell$.

Une conséquence immédiate de ce théorème est le corollaire suivant :

Corollaire 4.27. *Soit $f : D \to \mathbb{R}$ une fonction et $x_* \in D$.*

(i) S'il existe une suite $(x_n \in D \setminus \{x_*\})$ telle que $\lim_{n\to+\infty} x_n = x_*$ et telle que la suite $(f(x_n))$ n'est pas convergente, alors f n'a pas de limite en x_*.

(ii) S'il existe deux suites $(x_n, x'_n \in D \setminus \{x_*\})$ telles que $\lim_{n\to+\infty} x_n = x_* = \lim_{n\to+\infty} x'_n$ et telles que $\lim_{n\to+\infty} f(x_n) \neq \lim_{n\to+\infty} f(x'_n)$, alors f n'a pas de limite en x_*.

Voici un exemple d'application de ce corollaire :

Exercice 4.28. *(i) Soit $f :]0, \infty[\to \mathbb{R}$ définie par $f(x) = \sin(1/x)$. Montrer que f n'admet pas de limite en 0 ;*

(ii) Utiliser le corollaire pour montrer que la fonction de Heaviside n'admet pas de limite en 0.

Solution : (i) Soit $x_n = \frac{2}{\pi(4n+1)}$ et $x'_n = \frac{1}{\pi n}$ Alors

$$\lim_{n\to+\infty} \sin(1/x_n) = \lim_{n\to+\infty} \sin \pi(2n + \frac{1}{2}) = 1$$

et

$$\lim_{n\to+\infty} \sin(1/x'_n) = \lim_{n\to+\infty} \sin \pi n = 0.$$

Comme $\lim_{n\to+\infty} x_n = 0 = \lim_{n\to+\infty} x'_n$, le résultat résulte du (ii) du corollaire. Pour comprendre pourquoi j'ai choisi les suites x_n et x'_n, il faut regarder le graphe de $\sin\frac{1}{x}$ dans la figure 4.8.

(ii) A vous de jouer.

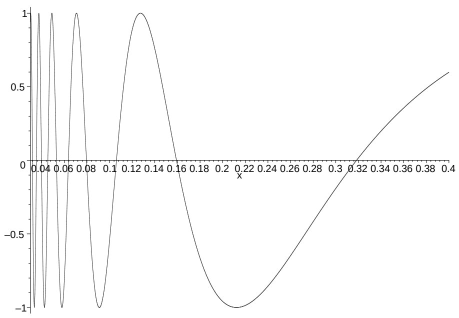

FIG. 4.8 – Le graphe de la fonction $\sin\frac{1}{x}$, pour x entre $0,03$ et $0,4$

Reste donc à montrer le théorème, ce qui n'est pas de tout repos.

Démonstration du Théorème 4.26* : Il faut montrer que $(i) \Rightarrow (ii)$ et que $(ii) \Rightarrow (i)$.

$(i) \Rightarrow (ii)$ Soit $(x_n \in D \setminus \{x_*\})$ telle que $\lim_{n\to+\infty} x_n = x_*$. On sait donc que, pour tout $\delta > 0$, il existe $M \in \mathbb{N}$ tel que, quelque soit $n \in \mathbb{N}$,

$$n \geq M \Rightarrow 0 < |x_n - x_*| < \delta. \tag{4.28}$$

On sait aussi, par l'hypothèse (i), que pour tout $\epsilon > 0$, il existe $\delta > 0$, tel que

$$0 < |x - x_*| < \delta \Rightarrow |f(x) - \ell| \leq \epsilon. \tag{4.29}$$

Il faut montrer que, pour tout $\epsilon > 0$, il existe $N \in \mathbb{N}$, tel que

$$n \geq N \Rightarrow |f(x_n) - \ell| \leq \epsilon.$$

En posant $N = M$ et en enchaînant les inégalités (4.28)-(4.29) ci-dessus on obtient bien ce résultat.

$(ii) \Rightarrow (i)$ C'est la partie la plus difficile de la démonstration. Je vais la montrer en montrant la contraposée, à savoir que (non (i)) $\Rightarrow$ (non (ii)). La difficulté de la démonstration provient précisément du fait que la négation de (i) n'est pas facile à manier, comme je l'ai déjà signalé plusieurs fois. Si (i) n'est pas vrai, il existe $\epsilon > 0$, tel que pour tout $\delta > 0$ on a :

$$\exists x \in]x_* - \delta, x_* + \delta[\cap D, x \neq x_*, |f(x) - \ell| \geq \epsilon.$$

Remarquer ici que le x dont l'existence est affirmé, dépend bien évidemment de δ. En particulier, soit $n \in \mathbb{N}$ et posons $\delta = \frac{1}{n}$. On obtient alors l'affirmation suivante :

$$\exists x_n \in]x_* - \frac{1}{n}, x_* + \frac{1}{n}[\cup D, x_n \neq x_*, |f(x_n) - \ell| \geq \epsilon.$$

On obtient ainsi une suite x_n qui converge clairement vers x_* (puisque $|x_n - x_*| < \frac{1}{n}$) et telle que la suite $f(x_n)$ ne converge pas vers ℓ (puisque pour tout $n \in \mathbb{N}$, $|f(x_n) - \ell| \geq \epsilon$. □

4.9 Limite à l'infini, limite infinie

Comme je l'ai expliqué, étudier la convergence d'une suite revient à étudier le comportement des termes de la suite lorsque n est grand. On peut se poser la même question pour une fonction, définie sur une demi-axe. De manière tout à fait analogue à la définition de limite d'une suite (Définition 4.14) nous avons alors la définition de limite d'une fonction en $+\infty$:

Définition 4.29. *Soit $a \in \mathbb{R}$ et soit $f : [a, +\infty[\to \mathbb{R}$. Soit $\ell \in \mathbb{R}$. On dit que f tend vers ℓ lorsque x tend vers $+\infty$ si et seulement si pour tout $\epsilon > 0$, il existe $X \in \mathbb{R}$ tel qu'on a : pour tout $x > X$, $|f(x) - \ell| \leq \epsilon$. On écrit alors : $\lim_{x \to +\infty} f(x) = \ell$.*

Il est évident que les propriétés énoncées dans les Propositions 4.5 et 4.8 restent vraies si on remplace x_* dans les énoncés par $+\infty$ ou $-\infty$ et D par $[a, +\infty[$ ou $]-\infty, a]$. Je vous invite par ailleurs à trouver l'analogue du Lemme 4.6 en regardant aussi le Lemme 4.18. Les démonstrations sont semblables à celles de la section 4.6. L'analogue de la Définition 4.15 est

Définition 4.30. *Soit $a \in \mathbb{R}$ et soit $f : [a, +\infty[\to \mathbb{R}$. On dit que f tend vers $+\infty$ lorsque x tend vers $+\infty$ si et seulement si pour tout $M > 0$, il existe $X \in \mathbb{R}$ tel qu'on a : pour tout $x > X$, $f(x) \geq M$. On écrit alors : $\lim_{x \to +\infty} f(x) = +\infty$.*

On peut de la même façon écrire la définition de

$$\lim_{x \to +\infty} f(x) = -\infty, \lim_{x \to -\infty} f(x) = +\infty, \lim_{x \to -\infty} f(x) = -\infty,$$

un exercice qui vous permettra de tester votre compréhension de la notion de limite et que je vous recommande donc vivement.

Exercice 4.31. *Calculer, pour tout $n \in \mathbb{N}$,*

$$\lim_{x \to +\infty} \frac{x^2 + 3x + 2}{x^n + 5x^2 + 2}.$$

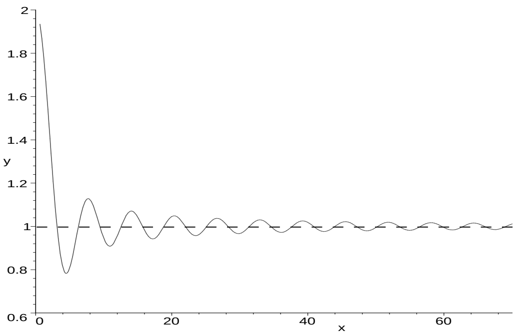

FIG. 4.9 – $\lim_{x\to+\infty} \frac{x+\sin x}{x} = 1$

Solution : Si $n = 0$, on a, pour tout $x > 0$

$$\frac{x^2+3x+2}{x^n+5x^2+2} = \frac{x^2+3x+2}{5x^2+3} = \frac{x^2(1+3x^{-1}+2x^{-2})}{x^2(5+3x^{-2})},$$

d'où

$$\lim_{x\to+\infty} \frac{x^2+3x+2}{x^n+5x^2+2} = \frac{\lim_{x\to+\infty}(1+3x^{-1}+2x^{-2})}{\lim_{x\to+\infty}(5+3x^{-2})} = \frac{1}{5}.$$

Pour $n = 1$, on obtient le même résultat et pour $n = 2$, on obtient $1/6$, chaque fois avec un calcul comparable. Si $n > 2$, on a

$$\frac{x^2+3x+2}{x^n+5x^2+2} = \frac{x^2(1+3x^{-1}+2x^{-2})}{x^n(1+5x^{2-n}+3x^{-n})}.$$

Par conséquent

$$\lim_{x\to+\infty} \frac{x^2+3x+2}{x^n+5x^2+2} = \lim_{x\to+\infty} x^{2-n} \lim_{x\to+\infty} \frac{(1+3x^{-1}+2x^{-2})}{(1+5x^{2-n}+3x^{-n})} = 0.$$

Cet exercice n'a pas beaucoup d'intérêt, mais montre qu'on peut facilement déterminer

$$\lim_{x\to+\infty} \frac{P(x)}{Q(x)}, \lim_{x\to-\infty} \frac{P(x)}{Q(x)},$$

pour tout polynôme P et Q.

Je vous laisse en exercice la démonstration du résultat suivant (voir Lemme 4.21) :

Lemme 4.32. *Soit $a \in \mathbb{R}$ et soit $f, g : [a, +\infty[\to \mathbb{R}$. Si, pour tout $x \in [a, +\infty[$, $f(x) \le g(x)$ et si $\lim_{x\to+\infty} f(x) = +\infty$, alors $\lim_{x\to\infty} g(x) = +\infty$.*

C'est encore une version du théorème des gendarmes, et je vous invite à en trouver des versions adaptées lorsque $\lim_{x\to+\infty} f(x) = -\infty$ ou $\lim_{x\to-\infty} f(x) = +\infty$, *etc.*.

Finalement, on peut aussi définir $\lim_{x\to x_*} f(x) = +\infty$ ou $-\infty$ lorsque $x_* \in \overline{D}$. C'est utile dans l'étude des asymptotes verticales des fonctions.

Le lecteur s'entraîne

1. Déterminer les limites en $\pm\infty$ des fonctions suivantes, si elles existent :

$$x \sin x, x^2 \sin x, x(2 + \sin x), x^2(2 + \sin x).$$

2. Soient $f, g : \mathbb{R} \to \mathbb{R}$. Les affirmations suivantes, sont-elles vraies ou fausses ?

(a) Si $g(x) \geq f(x)$ et si $\lim_{x\to-\infty} g(x) = -\infty$, alors $\lim_{x\to-\infty} f(x) = -\infty$.

(b) Si $\lim_{x\to+\infty} f(x) = \ell \in \mathbb{R}$, et si $\lim_{x\to+\infty} g(x) = +\infty$, alors $\lim_{x\to+\infty} f(x)g(x) = +\infty$.

(c) Si $\lim_{x\to+\infty} g(x) = \ell \in \mathbb{R}$ et $\lim_{x\to-\infty} g(x) = \ell' \in \mathbb{R}$, alors f est bornée.

4.10 Encore un peu de logique : retour au raisonnement par l'absurde

Je voudrais finalement revenir une seconde fois sur la démonstration par l'absurde. J'en ai expliqué le fonctionnement dans la Section 2.7 : si on doit montrer P, on peut essayer de montrer "(non P) implique (non Q)," où Q est une affirmation vraie. Le problème est de trouver une affirmation Q appropriée. Lorsque l'affirmation P à démontrer est elle-même une implication comme "A implique B," il est parfois utile de procéder ainsi. On prend pour Q l'affirmation "A ou (non A)", qui est toujours vraie, quelque soit A. Rappelons que "A et (non A)" est dans ce cas la négation de Q. On montre alors "A et (non B) impliquent (non A)," c'est à dire "(non P) implique (non A)." Comme évidemment "A et (non B) implique A," on peut conclure que "(non P) implique (non Q), ce qui démontre finalement P." En conclusion, il est fort utile de se souvenir que

> Pour montrer "A implique B", il suffit de montrer "(A et (non B)) implique (non A)."

Lorsque il utilise cette idée dans une démonstration, l'auteur écrira souvent qu'il fait une démonstration par l'absurde. Il y a néanmoins une autre façon de voir que cette idée est correcte, sans faire référence à la démonstration par l'absurde. En effet, "A implique B" est logiquement équivalent à "B ou (non A)." Par ailleurs, "A et (non B) impliquent (non A)" est logiquement équivalent à "(non A) ou non(A et (non B))," et donc à "(non A) ou ((non A) ou B)" qui est à son tour équivalent à "(non A) ou B." On en conclut finalement que "A implique B" est logiquement équivalent à "A et (non B) impliquent (non A)."

Exercice 4.33. *(i) Identifier dans la démonstration de l'Exercice 4.2 (ii) les affirmations "A" et "B" et se convaincre que j'ai bien montré que "A et (non B) implique (non A)."*

(iii) Retrouver toutes les démonstrations par l'absurde dans les chapitres précédents et suivants et analyser leur structure logique.

Le lecteur teste ses connaissances

Le barême sur 20 est donné à titre indicatif

Devoir Surveillé Arithmétique-Analyse 1 – durée 3h00

I [5pt] Questions de cours

(i) Donner la définition de suite convergente et de suite bornée.

(ii) Démontrer qu'une suite convergente est bornée.

(iii) Soit $f : D \to \mathbb{R}$. Donner la définition de "f tend vers $\ell \in \mathbb{R}$ lorsque x tend vers $x_* \in \bar{D}$."

II [4 pt] Soit $f : \mathbb{R} \to \mathbb{R}$ définie par $f(x) = 3x^3 - 2x^2 + x - 1$.

(i) Trouver une valeur $\delta, 0 < \delta < 1$, telle qu'on ait :

$$x \in]1 - \delta, 1 + \delta[\Rightarrow |f(x) - 1| \leq 0,01.$$

Indication : on remarquera qu'on a $3x^3 - 2x^2 + x - 2 = (x - 1)(3x^2 + x + 2)$, et que $(3x^2 + x + 2)$ est borné sur $[0, 2]$.

(ii) Soit $\epsilon > 0$. Trouver une valeur $\delta, 0 < \delta < 1$, telle qu'on ait :

$$x \in]1 - \delta, 1 + \delta[\Rightarrow |f(x) - 1| \leq \epsilon.$$

III [3pt] Soit $f : \mathbb{R}^* \to \mathbb{R}$ définie par $f(x) = \sin^2 \frac{1}{x^2}$. La fonction f admet-elle une limite en $x_* = 0$? Même question pour $f(x) = x^2 \sin \frac{1}{x^2}$ et pour $f(x) = x^{-2} \sin \frac{1}{x^2}$.

IV [2pt] Soit (u_n) une suite de nombres strictement positifs. Montrer que, si $\lim\limits_{n\to\infty} \dfrac{u_{n+1}}{u_n} = \dfrac{1}{2}$, alors $\lim\limits_{n\to\infty} u_n = 0$.

V [2pt] Démontrer qu'on a :

$$\forall n \in \mathbb{N}, 7^{2n+1} + 6\ 10^n \equiv 0[13].$$

VI [4pt] Les affirmations suivantes, sont-elles vraies ou fausses ? Ne pas oublier de justifier ses réponses !

(i) Si (u_n) est une suite telle que $(\sin u_n)$ converge, alors $\cos u_n$ converge.

(ii) Soit p un nombre premier. Soient $a, b \in \mathbb{Z}$. Si p divise ab, alors p divise a ou b.

(iii) Il y a un entier n tel que 14^n ait 5 comme chiffre des unités.

Devoir Surveillé Arithmétique-Analyse 2 – durée 3h00

I [6pt] Questions de cours. Soient $f, g : \mathbb{R} \to \mathbb{R}$.

(i) Rappeler la définition de “f tend vers $-\infty$ lorsque x tend vers $+\infty$.”

(ii) Montrer que, si pour tout $x \in \mathbb{R}$, $g(x) \leq f(x)$, et si $\lim_{x\to+\infty} f(x) = -\infty$, alors $\lim_{x\to+\infty} g(x) = -\infty$.

(iii) Montrer qu'il y a une infinité de nombres premiers.

(iv) L'affirmation suivante, est-elle vraie ?

$$\forall a \in \mathbb{R}, \exists b \in \mathbb{R}, \forall x \in \mathbb{R}, (|x| \leq b \Rightarrow x \leq a^2).$$

Si oui, la montrer. Ecrire sa négation.

II [4pt] Soit $f : \mathbb{R} \to \mathbb{R}$ définie par $f(x) = x^3 - 4x^2 + x + 6$.

(i) Trouver une valeur $\delta, 0 < \delta < 1$, telle qu'on ait :

$$x \in]-1-\delta, -1+\delta[\Rightarrow |f(x)| \leq 0,01.$$

(ii) Soit $\epsilon > 0$. Trouver une valeur $\delta, 0 < \delta < 1$, telle qu'on ait :

$$x \in]-1-\delta, -1+\delta[\Rightarrow |f(x)| \leq \epsilon.$$

III [5pt] On considère l'équation

$$4x^3 + 2x^2 - 1 = 0. \qquad (*)$$

(i) Montrer que cette équation n'admet pas de solution $x \in \mathbb{Z}$. **Indication :** On pourra par exemple montrer que, si $x \in \mathbb{Z}$ est solution, alors x divise 1.

(ii) On veut trouver les solutions rationnelles de $(*)$, c'est à dire de la forme $x = \frac{a}{b}$, avec $a \in \mathbb{Z}, b \in \mathbb{N}^*$ et $a \wedge b = 1$. On procèdera ainsi :

• Montrer que $a \wedge b^3 = 1$ et que $a^3 \wedge b = 1$.

•• Montrer que, si a/b est solution, alors

$$4a^3 + 2a^2b - b^3 = 0.$$

En déduire que a divise 1 et que b divise 4.

• • • Calculer toutes les solutions rationnelles de l'équation $(*)$.

IV [2pt] Etudier la convergence de la suite $u_n = \frac{\sin(e^n)}{n}$.

V [3pt] Les affirmations suivantes, sont-elles vraies ou fausses ? Ne pas oublier de justifier ses réponses !

(i) Si (u_n) est une suite telle que $\lim_{n\to+\infty} u_n = 0$ alors $\lim_{n\to+\infty} \frac{1}{u_n} = +\infty$.

(ii) Soient (u_n) et (v_n) des suites telles que

$$\lim_{n\to+\infty} u_n = 0, \qquad \lim_{n\to+\infty} v_n = +\infty.$$

Alors

$$\lim_{n\to+\infty} u_n v_n = 0 \quad \text{ou} \quad \lim_{n\to+\infty} u_n v_n = +\infty.$$

S. De Bièvre

Chapitre 5

Fonctions continues et dérivables

Le talent n'est qu'une longue patience. Travaillez.
G. Flaubert à G. de Maupassant

5.1 Les définitions

La plus faible des notions de régularité d'une fonction que nous rencontrerons est celle de "continuité". En voici, sans détour, la définition.

Définition 5.1. *Soit $f : D \to \mathbb{R}$ et $x_* \in D$. On dit que f est continue en x_* si $\lim_{x \to x_*} f(x)$ existe et vaut $f(x_*)$, c'est à dire*

$$\lim_{x \to x_*} f(x) = f(x_*),$$

ou encore, pour tout $\epsilon > 0$, il existe $\delta > 0$ tel que pour tout $x \in D$ on a

$$0 \leq |x - x_*| < \delta \Rightarrow |f(x) - f(x_*)| < \epsilon.$$

On dit que f est continue si f est continue en chaque point de son domaine.

Comme nous avons beaucoup travaillé dans le chapitre précédent pour comprendre la notion de limite, la notion "continue" devrait maintenant sembler facile : une fonction est continue si elle admet en chaque point x_* de son domaine comme limite sa valeur $f(x_*)$ en ce point. La subtilité de la notion est donc cachée dans celle de limite. Il y a aussi une autre difficulté avec la notion de continuité qui provient du fait que la notion mathématique de continuité ne coincide pas complètement avec le sens de ce mot dans le langage courant. En effet, le mot "continu" signifie dans le langage courant "sans interruption" ou "fait de parties non-séparées." C'est cette deuxième signification qui est à l'origine de la notion de fonction continue en mathématiques. En effet, on verra plus loin (Théorème 8.5) qu'une fonction définie sur un intervalle est continue si et seulement si son graphe et son image sont faits d'une seule partie : la fonction ne fait pas de “sauts” et “on peut tracer son graphe sans lever le crayon du papier”. Par contre, la notion mathématique de continuité ne reflète pas toujours l'idée de phénomène sans interruption tel qu'on le conçoit dans la vie quotidienne. Imaginons-nous par exemple qu'on enregistre le débit d'eau dans le tuyau d'évacuation du toit d'une habitation en fonction du temps (exprimé en litres par seconde). Alors, les jours de fortes pluie, il y a un débit important et les jours de sècheresse, il y a un débit nul. On obtient donc un graphe comme celui de la figure5.1. Ce graphe est le graphe d'une fonction continue dans le sens

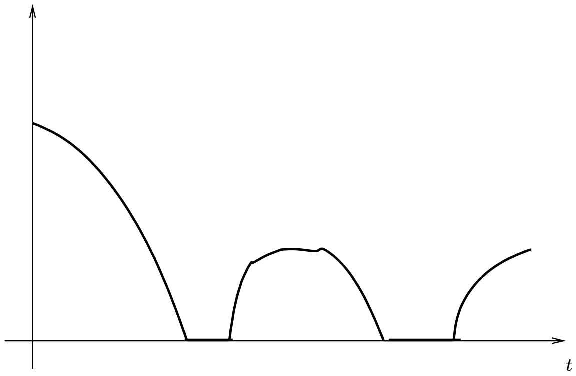

FIG. 5.1 – Un débit d'eau

mathématique du terme. Néanmoins, dans le langage courant, il s'agit d'un phénomène intermittent ou interrompu, que nous qualifierions de discontinu parce qu'il y a des jours où le débit est nul !

Exercice 5.2. *Discuter la paraphrase suivante de la définition de “fonction continue” :*

> *“Une grandeur dépend continûment d'un paramètre si on ne peut pas changer sa valeur d'une quantité fixée (aussi petite soit-elle) en effectuant une variation arbitrairement petite du paramètre. De façon équivalente, ceci veut dire que, pour obtenir un changement fixé de la valeur de la grandeur considérée, il faut effectuer une variation minimale du paramètre.”*

Le Lemme 4.4 affirme la continuité des polynômes et des fractions rationnelles, et le Lemme 4.12 celle des fonctions cosinus et sinus. A quelques rares exceptions près, toutes les fonctions que vous rencontrerez en DEUG seront continues, sauf éventuellement en quelques points isolés de leur domaine. La fonction de Heaviside, par exemple, n'est pas continue en 0, mais l'est partout ailleurs. Ceci peut laisser à l'étudiant l'impression qu'il faut faire des choses peu naturelles pour fabriquer des fonctions non-continues et que seulement un esprit véritablement tordu peut s'imaginer des fonctions discontinues en tout point de leur domaine. Ceci n'est pas (complètement) vrai, mais l'expliquer en plus de détail irait bien au delà de ce cours et devra attendre la licence de mathématiques, si un jour vous vous y retrouvez.

En fait, les fonctions de DEUG sont bien plus que continues, elles sont presque toutes infiniment dérivables, sauf éventuellement en quelques points isolés de leur domaine. Je vous rappelle la définition de fonction dérivable :

Définition 5.3. *Soit $f : D \to \mathbb{R}$ et $x_* \in D$. On dit que f est dérivable en x_* si*

$$\lim_{x \to x_*} \frac{f(x) - f(x_*)}{x - x_*}$$

existe. On désigne alors cette limite par $f'(x_*)$ ou par $\frac{df}{dx}(x_*)$ et on l'appelle la dérivée de f en x_*. On dit que f est dérivable si f est dérivable en chaque point de son domaine. Dans ce cas la fonction

$$f' : x \in D \mapsto f'(x) \in \mathbb{R}$$

est appelée la dérivée de f.

Bien évidemment, une fois que f est dérivable, on peut se poser la question pour f'. On dit que f est deux fois dérivable si f' est dérivable et on écrit $f'' = (f')'$. On introduit de la même façon les fonctions n fois dérivables et on désigne par $f^{(n)}$ la n-ième dérivée de f lorsqu'elle existe. Une fonction n fois dérivable pour tout $n \in \mathbb{N}$ est appelée infiniment dérivable. Bien évidemment, les polynômes, fractions rationnelles et fonctions trigonométriques sont infiniment dérivables. L'exercice suivant vous invite à *démontrer,* à partir de la définition ci-dessus, les formules pour leurs dérivées que vous avez apprises par coeur au lycée.

Exercice 5.4. *(i) Montrer que, pour tout $n \in \mathbb{N}$, on a*

$$\frac{d}{dx} x^n = n x^{n-1}.$$

(ii) Montrer que

$$\frac{d}{dx} \sin x = \cos x, \quad \frac{d}{dx} \cos x = -\sin x.$$

(iii) Montrer que, pour $x > 0$,

$$\frac{d}{dx} \sqrt{x} = \frac{1}{2\sqrt{x}}.$$

Solution : (i) C'est certainement vrai pour $n = 0$. (Vérifiez-le !) Il suffit alors d'appliquer une récurrence, la définition, et une petite astuce que vous devriez reconnaître :

$$\begin{aligned} \lim_{x \to x_*} \frac{x^n - x_*^n}{x - x_*} &= \lim_{x \to x_*} \frac{x(x^{n-1} - x_*^{n-1}) - x_*^{n-1}(x_* - x)}{x - x_*} \\ &= x_* \lim_{x \to x_*} \frac{x^{n-1} - x_*^{n-1}}{x - x_*} + x_*^{n-1}. \end{aligned}$$

Je vous laisse le soin de rédiger les détails du raisonnement.

(ii) Le travail dur a déjà été fait dans la Section 4.3, dont j'utiliserai les résultats librement :

$$\begin{aligned}
\lim_{x\to x_*}\frac{\sin x-\sin x_*}{x-x_*} &= \lim_{h\to 0}\frac{\sin(x_*+h)-\sin x_*}{h}\\
&= \lim_{h\to 0}\frac{\sin x_*\cos h+\cos x_*\sin h-\sin x_*}{h}\\
&= \sin x_*\lim_{h\to 0}\frac{\cos h-1}{h}+\cos x_*\lim_{h\to 0}\frac{\sin h}{h}\\
&= \cos x_*
\end{aligned}$$

(iii)

$$\begin{aligned}
\lim_{x\to x_*}\frac{\sqrt{x}-\sqrt{x_*}}{x-x_*} &= \lim_{x\to x_*}\frac{(\sqrt{x}-\sqrt{x_*})(\sqrt{x}+\sqrt{x_*})}{(x-x_*)(\sqrt{x}+\sqrt{x_*})}\\
&= \lim_{x\to x_*}\frac{x-x_*}{(x-x_*)(\sqrt{x}+\sqrt{x_*})}=\frac{1}{2\sqrt{x_*}}
\end{aligned}$$

Importante, mais évidente et triviale est la propriété suivante :

Lemme 5.5. *Si f est dérivable en un point de son domaine, alors f y est continue.*

Démonstration : On a

$$\lim_{x\to x_*}(f(x)-f(x_*))=\lim_{x\to x_*}\frac{f(x)-f(x_*)}{x-x_*}(x-x_*)=f'(x_*)\ 0=0,$$

ce qui démontre le résultat. □

Attention, l'implication réciproque est fausse, comme l'exercice suivant le montre.

Exercice 5.6. *Montrer que la fonction $f(x)=|x|$ est continue, mais n'est pas dérivable en 0.*

Quel est l'intérêt de ces nouvelles notions ? Pour la dérivée, on a déjà remarqué qu'elle apparaît tout à fait naturellement dans le problème du banquier (Section 3.1) : $C'(t)$ est le taux de variation (exprimé en francs par unité de temps) de la dette. En physique aussi, vous l'avez déjà rencontrée comme la vitesse instantanée : elle est exprimée en mètres par seconde (ou kilomètres par heure) et exprime comment la position varie avec le temps. En général, la dérivée d'une fonction f est le taux de variation de la grandeur que décrit f lorsque le paramètre x change. Dans la Section **??** je présenterai une autre façon de voir l'importance de la dérivée, en la reliant au problème du calcul des fonctions, expliqué dans la Section 3.1.

5.1.1 Continuité : une définition alternative

Pour terminer cette section vous trouverez dans l'exercice suivant un critère de continuité en termes des notions introduites dans la Section 3.3 .

Exercice 5.7. *(i) Montrer qu'une fonction $f : D \to \mathbb{R}$ est continue en un point x_* de son domaine D si et seulement si pour tout intervalle ouvert J contenant $f(x_*)$ il existe un intervalle ouvert I contenant x_* tel que $f(I \cap D) \subset J$.*

(ii) Ecrire la négation de l'affirmation ci-dessus.

Cette formulation de la continuité ne fait pas du tout référence à la notion de limite et ne fait donc pas intervenir les epsilons-deltas tant redoutés, ce qui doit vous paraître un avantage majeur. Elle est néanmoins moins facile à utiliser dans certaines démonstrations que la définition elle-même. Par contre, cette dernière est très peu intuitive, tandis que la formulation ci-dessus est plus suggestive, surtout si on l'utilise avec le graphe de la fonction pour obtenir une idée géométrique de la continuité. En effet, elle suggère de regarder l'image par f des intervalles I contenant x_* pour voir si ces images se retrécissent autour de $f(x_*)$ lorsque I se retrécit autour de x_*. Si c'est le cas, la fonction est continue, sinon, elle ne l'est pas. On voit ainsi facilement que la fonction de Heaviside n'est pas continue : en effet, l'image $H(I)$ de n'importe quel intervalle ouvert contenant $x_* = 0$ est $H(I) = \{0\} \cup \{1\}$, indépendamment de I. Or, il est facile de trouver un intervalle ouvert J contenant $H(x_*) = 1$ qui ne contient pas $H(I)$. Par exemple $J =]1/2, 3/2[$ ne contient pas $H(I)$! Alternativement, on peut remarquer que $f(I \cap D) \subset J$ est la même chose que $(I \cap D) \subset f^{-1}(J)$. Donc pour vérifier si une fonction est continue on peut procéder ainsi. D'abord on étudie (ou on dessine) l'image inverse d'un intervalle ouvert J *quelconque* qui contient $f(x_*)$ et on vérifie qu'il contient toujours un intervalle ouvert autour de x_*. Si c'est le cas, la fonction est continue, sinon elle ne l'est pas.

Exercice 5.8. *Soit $f : \mathbb{R} \to \mathbb{R}$ définie par $f(x) = \sin(1/x)$ si $x \neq 0$ et $f(0) = 0$. Soit $\epsilon > 0$ et $J_\epsilon =]-\epsilon, \epsilon[$. Etudier $f^{-1}(J_\epsilon)$. Que peut-on conclure concernant la continuité de f ?*

5.2 Continuité : propriétés simples

En application directe de la Proposition 4.5, on conclut que la somme, le produit et le quotient de fonctions continues est également continue. De même, le théorème suivant n'est qu'une variante du Théorème 4.26

Théorème 5.9. *Une fonction $f : D \to \mathbb{R}$ est continue en $x_* \in D$ si et seulement si pour toute suite $(x_n \in D)$ qui converge vers x_* on a que la suite $(f(x_n))$ converge vers $f(x_*)$.*

Ce résultat peut-être utilisé pour donner un critère qui est parfois utile lorsqu'on veut montrer qu'une fonction n'est pas continue, en parfaite analogie avec le Corollaire 4.27. Je ne m'y attarde pas davantage.

Le lecteur s'entraîne

1. Etudier la continuité de la fonction f définie par : $f(0) = 1$ et $f(x) = xE\left(\frac{1}{x}\right)$ pour $x \neq 0$. $E(a)$ désigne la partie entière de $a \in \mathbb{R}$.

2. Déterminer l'ensemble des fonctions f définies sur $[0,1]$, continues en 0, telles que pour tout $x \in [0,1]$, $f(x^2) = f(x)$.

3. a) Montrer que, quelque soit $a \in \mathbb{R}$, la fonction $f(0) = a$, $f(x) = \cos\left(\frac{1}{x}\right)$ $(x \neq 0)$ n'est pas continue en $x_* = 0$. Et en $x_* \neq 0$?

b) Considérer le même problème pour la fonction $x \cos\left(\frac{1}{x}\right)$.

Dans les exercices suivants, on pourra utiliser que, pour tout $a \in \mathbb{R}$, il existe une suite (a_n) de nombres *rationnels* telle que $\lim_{n\to\infty} a_n = a$. Cette propriété des nombres réels sera démontrée plus tard (Section **??**).

4. Soit $f : \mathbb{R} \to \mathbb{R}$, continue en 0, et telle que pour tout couple (x, y) on a $f(x + y) = f(x) + f(y)$.

a) Montrer que $f(0) = 0$, puis que f est impaire.

b) Montrer que f est continue en tout point de $\mathbb{R}$ (on remarquera que $f(x - y) = f(x) - f(y)$).

c) Pour n entier naturel, puis n entier relatif, exprimer $f(n)$ en fonction de $f(1)$.

d) Montrer que $\forall\, r \in \mathbb{Q}$, on a $f(r) = rf(1)$.

e) Conclure en déterminant f pour tout $x \in \mathbb{R}$.

5. Etudier la continuité de f définie sur $\mathbb{R}$ par

$$f(x) = x \text{ si } x \in \mathbb{Q}\,, \qquad \text{et } f(x) = \frac{1}{3} \text{ sinon.}$$

5.3 Dérivabilité : propriétés simples

Proposition 5.10. *Soient $f, g : D \to \mathbb{R}$ dérivables en un point x_* de D. Alors $f + g$ et fg sont également dérivables en D et on a*

$$(f + g)'(x_*) = f'(x_*) + g'(x_*), \quad (fg)'(x_*) = f'(x_*)g(x_*) + f(x_*)g'(x_*).$$

Si $g(x_*) \neq 0$, f/g est également dérivable en x_* et

$$\left(\frac{f}{g}\right)'(x_*) = \frac{f'(x_*)g(x_*) - f(x_*)g'(x_*)}{g^2(x_*)}.$$

Démonstration : Il s'agit de simples calculs, utilisant la Proposition 4.5, le Lemme 5.5 et un peu de jugeote. Au charbon ! □

Le lecteur s'entraîne

1. Etudier la dérivabilité en 0 des fonctions $f(x) = |x|$ et $g(x) = x|x|$.

2. Soit $n \in \mathbb{N}^*$. Considérer la fonction $f(x) = x^n \sin\frac{1}{x}$, si $x \neq 0$, et $f(0) = 0$. f est-elle une, deux, trois, ... fois dérivable ? Si oui, ses dérivées successives sont-elles continues ? **Indication :** Commencer par faire l'étude pour $n = 1$, puis pour $n = 2$.

3. Soit f définie sur $\mathbb{R}$. Montrer que si f est dérivable en un point a alors

$$\lim_{h\to 0^+} \frac{f(a + h) - f(a - h)}{2h}$$

existe (et vaut $f'(a)$). Qu'en est-il de la réciproque ? **Indication :** Penser à $|x|$.

5.4 L'interprétation géométrique de la dérivée

5.4.1 Approcher f par une fonction affine

J'ai déjà expliqué dans la Section 3.1 que les seules fonctions qu'on peut calculer sont les polynômes. Cela suggère que, pour calculer par exemple $\sin 0,5$, on essaie d'approcher la fonction sinus par un polynôme, pour calculer ensuite la valeur de ce dernier. Les observations de la Section 3.1 font penser que ceci devrait être possible pour beaucoup de fonctions. Je vais faire, dans cette section, un premier pas dans cette direction, et montrer comment la notion de dérivée se présente de façon incontournable lorsqu'on essaie d'approcher la fonction f par un polynôme de degré 1 tout simplement (c'est à dire par une fonction affine). Le traitement général du problème de l'approximation de fonctions par des polynômes est remis à un chapitre ultérieur (Chapitre **??**).

Soit donc $f : D \to \mathbb{R}$ une fonction continue. Soit $x_* \in D$. Je cherche à approcher f dans un voisinage de x_* par un polynôme de degré 1, que j'écris

$$P_1(x) = a_0 + a_1(x - x_*)$$

et le problème qui se pose est alors de trouver les coefficients a_0 et a_1 de façon à ce que $f(x) - P_1(x)$ soit aussi petit que possible lorsque x est proche de x_*. Afin d'avoir une interprétation géométrique de cette exigence, on se rappellera que $d(x) = f(x) - P_1(x)$ représente la distance verticale entre le point de coordonnées $(x, f(x))$ sur le graphe de f et le point $(x, P_1(x))$ sur la droite d'équation $y = P_1(x)$ (Figure 5.2). Je vais donc certainement exiger que les coefficients soient choisis tels que

$$\lim_{x \to x_*} (f(x) - P_1(x)) = 0. \tag{5.1}$$

On en conclut aisément que $a_0 = f(x_*)$, ce qui revient à dire que parmi toutes les droites possibles, seules celles qui passent par le point $(x_*, f(x_*))$ sont retenues. C'est plutôt raisonnable. L'équation (5.1) n'impose aucune contrainte sur le choix de a_1, c'est à dire sur le coefficient directeur ou la pente de la droite $y = P_1(x)$. (Un petit rappel sur les droites du plan est donné en fin de section.) Pour déterminer ce coefficient, je ne vais pas me contenter d'exiger seulement (5.1), mais je vais demander que $f(x) - P_1(x)$ tend vers 0 *rapidement.* Il faut d'abord que je donne un sens précis à cette notion.

Soient $g, h : D \to \mathbb{R}$ deux fonctions et $x_* \in \bar{D}$. Supposons que

$$\lim_{x \to x_*} g(x) = 0 = \lim_{x \to x_*} h(x).$$

On peut se poser la question de savoir laquelle des deux fonctions "tend le plus vite vers 0." Ça peut se lire sur leurs graphes : dans la figure 5.3 la fonction g tend plus vite vers zero en $x_* = 1$ que h. En effet, proche de $x_* = 1$, elle est (beaucoup) plus petite que h. Comment donner un sens précis à ce phénomène ? Une façon de le faire consiste à remarquer que, si g tend plus vite vers 0 que h en x_*, alors, pour x proche de x_*, $|g|$ est beaucoup plus petit que $|h|$ et donc

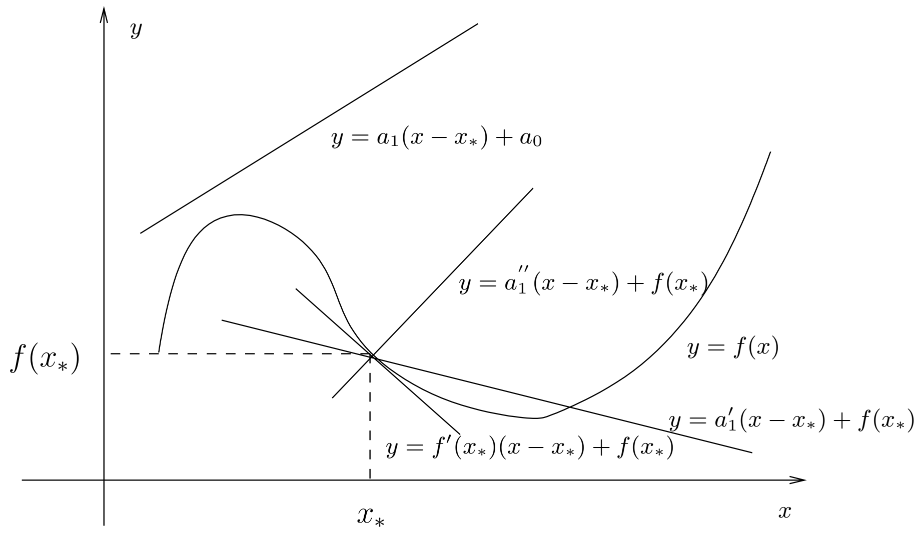

FIG. 5.2 – Le graphe de f, d'une droite quelconque d'équation $y = a_0 + a_1(x - x_*)$ et de trois droites d'équation $y = f(x_*) + \alpha(x - x_*)$, pour différentes valeurs du coefficient directeur $\alpha = a_1', a_1''$ et $f'(x_*)$. Laquelle de toutes ces droites semble "coller" le plus au graphe de f, proche de $(x_*, f(x_*))$?

$|g/h(x)|$ est très petit. Je dirai donc que "g tend vers 0 plus vite que h" si

$$\lim_{x \to x_*} \frac{|g(x)|}{|h(x)|} = 0. \tag{5.2}$$

On dit aussi (et c'est plus standard) que "g est négligeable par rapport à h". On voit ainsi aisément que $a(x - x_*)^n$ tend vers 0 plus vite que $b(x - x_*)^m$ $(a, b \in \mathbb{R})$ si et seulement si $n > m$. Ceci est illustré dans la figure 5.4. On y voit bien que les puissances plus élevées "s'écrasent" davantage contre l'axe des x, même si elles sont précédées d'un grand coefficient.

Exercice 5.11. *Montrer que* $10^{10} \sin^2(x - 3)$ *tend vers* 0 *plus vite que* $(x - 3)$ *en* 3.

Solution : Il suffit de calculer

$$\lim_{x \to 3} \frac{10^{10} \sin^2(x - 3)}{x - 3} = 10^{10} \lim_{x \to 3} \frac{\sin(x - 3)}{x - 3} \lim_{x \to 3} \sin(x - 3) = 10^{10} \times 1 \times 0 = 0.$$

Il faut néanmoins remarquer que, lorsque $x = 3,001$, $10^{10} \sin^2(x - 3)$ est à peu près égal à 10^4, qui est bien plus grand que $x - 3 = 10^{-3}$! Ce n'est que lorsque x est encore beaucoup plus proche de 3 que $10^{10} \sin^2(x - 3)$ devient plus petit que $x - 3$.

L'idée est maintenant de choisir, si possible, le polynôme $P_1(x)$ de façon à ce que $f(x) - P_1(x)$ tende vers 0 plus vite que $(x - x_*)$, c'est à dire on cherchera

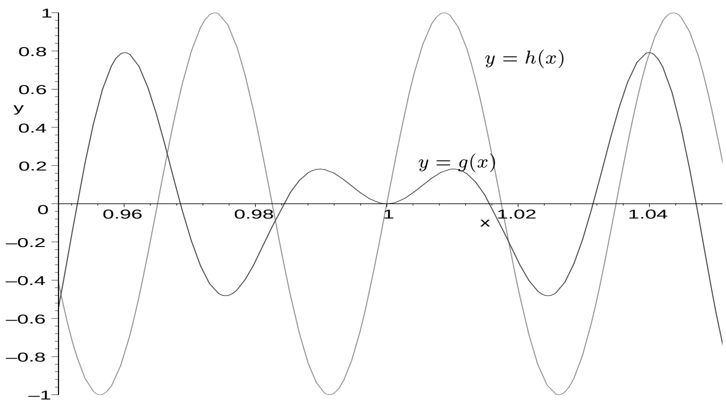

FIG. 5.3 – g tend vers 0 plus vite que h !

a_1 tel que

$$\lim_{x \to x_*} \frac{f(x) - P_1(x)}{x - x_*} = 0. \tag{5.3}$$

Si un tel $P_1(x)$ existe, on pourra dire que, parmi toutes les droites du plan, celle dont l'équation est $y = P_1(x)$ est le plus proche du graphe de f lorsque x est proche de x_*. C'est cette droite là qu'on appelle alors la *droite tangente* à $y = f(x)$ en $(x_*, f(x_*))$. L'exercice suivant donne quelques exemples instructifs de telles droites.

Exercice 5.12. *(i) Soit $f(x) = \sin x$. Montrer que le polynôme $P_1(x) = x$ satisfait (5.3) en $x_* = 0$.*

(ii) Soit $f(x) = \sin x$. Montrer que le polynôme $P_1(x) = \sin x_* + \cos x_*(x - x_*)$ satisfait (5.3) en tout point $x_* \in \mathbb{R}$. Dessiner, sur un même dessin, le graphe $y = \sin x$ et le graphe de ce polynôme lorsque $x_* = \pi/4$ (voir aussi la figure 5.5)

Sous quelles conditions une fonction f admet-elle une droite tangente en un point $(x_*, f(x_*))$ de son graphe ? La réponse est donnée dans la proposition suivante.

Proposition 5.13. *Soit $f : D \to \mathbb{R}$ continue et $x_* \in D$. La fonction f est dérivable en x_* si et seulement si il existe $a_0, a_1 \in \mathbb{R}$ tels que $P_1(x) = a_0 + a_1(x - x_*)$ satisfait (5.3). Dans ce cas on a $a_0 = f(x_*), a_1 = f'(x_*)$ et donc*

$$P_1(x) = f(x_*) + f'(x_*)(x - x_*).$$

Démonstration : Supposons d'abord que f soit dérivable en x_*. Il faut alors montrer que $P_1(x) = f(x_*) + f'(x_*)(x - x_*)$ est l'unique polynôme de degré 1

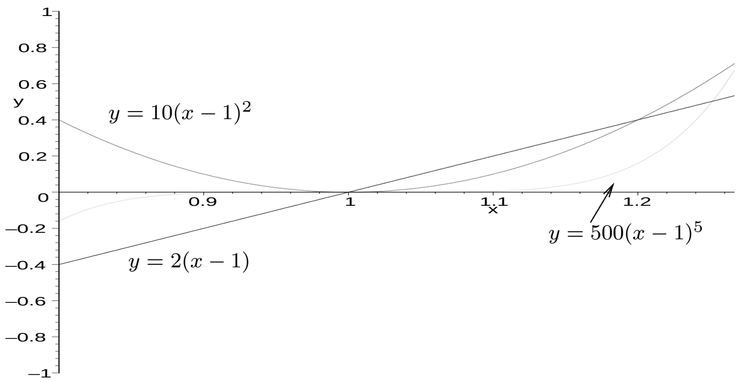

FIG. 5.4 – $500(x-1)^5$ est plus petit que $2(x-1)$ lorsque x est proche de 1.

qui satisfait (5.3). Mais, si f est dérivable en x_*, on voit tout de suite que

$$\lim_{x\to x_*}\frac{f(x)-P_1(x)}{(x-x_*)}=\lim_{x\to x_*}\frac{f(x)-f(x_*)}{(x-x_*)}-f'(x_*)=0.$$

Pour l'unicité, on remarque que, si $Q_1(x)=a_0'+a_1'(x-x_*)$ satisfait (5.3), alors

$$\lim_{x\to x_*}\frac{Q_1(x)-P_1(x)}{(x-x_*)}=0.$$

On en tire facilement la conclusion que $a_0'=f(x_*)$ et $a_1'=f'(x_*)$, c'est à dire que $P_1(x)=Q_1(x)$.

Supposons maintenant qu'il existe $P_1(x)=a_0+a_1(x-x_*)$ tel que (5.3) est satisfait. On voit immédiatement qu'alors

$$0=\lim_{x\to x_*}f(x)-P_1(x)=f(x_*)-a_0.$$

On a également,

$$0=\lim_{x\to x_*}\frac{f(x)-P_1(x)}{(x-x_*)}=\lim_{x\to x_*}\frac{f(x)-f(x_*)}{(x-x_*)}-a_1.$$

On conclut que la limite

$$\lim_{x\to x_*}\frac{f(x)-f(x_*)}{(x-x_*)}$$

existe bel et bien, et donc que f est dérivable en x_*. En plus, $f'(x_*)=a_1$, ce qui conclut la démonstration. $\square$

Une façon de comprendre la dérivabilité est donc de constater que les fonctions

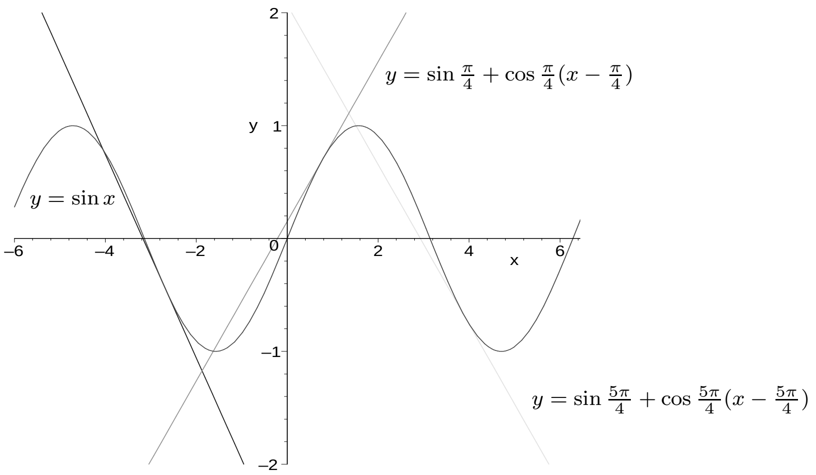

FIG. 5.5 – Le graphe du sinus et quelques-unes de ses tangentes

dérivables sont celles qui peuvent être bien approchées localement autour de chaque point de leur domaine (dans le sens de (5.3)) par une fonction affine. Ce sont donc les fonctions dont le graphe ressemble localement à une droite, que l'on appelle alors la droite tangente.

La fonction valeur absolue, par contre, avec sa forme en V, ne ressemble pas à une droite proche du point $(0, 0)$, et n'est en effet pas dérivable en $x_* = 0$, comme nous l'avons vu dans l'exercice 5.6.

En résumé, j'ai *défini* la droite tangente au graphe de f, au point $(x_*, f(x_*))$, comme étant celle qui "colle le mieux au graphe de f", proche de ce point. J'ai alors *démontré* que cette droite a comme équation

$$y = f(x_*) + f'(x_*)(x - x_*),$$

et qu'elle n'existe que lorsque f est dérivable en x_*. Il ne suffira pas, par la suite, de se souvenir de l'équation de la droite tangente, tout en oubliant son interprétation géométrique.

5.4.2 Les droites du plan

Quand on demande à un jeune bachelier quelle est l'équation d'une droite du plan, il répond :

$$y = ax + b. \tag{5.4}$$

C'est certes correct, mais pas toujours la meilleure façon d'écrire l'équation. Lorsqu'une droite est définie en spécifiant deux de ses points, disons (x_1, y_1) et (x_2, y_2), il est souvent plus commode d'écrire son équation sous la forme

$$\frac{y - y_1}{x - x_1} = \frac{y_2 - y_1}{x_2 - x_1} \quad \text{ou } y = y_1 + \frac{y_2 - y_1}{x_2 - x_1}(x - x_1). \tag{5.5}$$

Comme vous savez, on appelle a dans (5.4) ou $\frac{y_2 - y_1}{x_2 - x_1}$ dans (5.5) la *pente* ou le *coefficient directeur* de la droite. Finalement, parfois une droite est définie en spécifiant un de ses points, disons (x_*, y_*), et sa pente $\alpha \in \mathbb{R}$. Dans ce cas, son équation est

$$y = y_* + \alpha(x - x_*). \tag{5.6}$$

C'est sous cette forme que les droites tangentes se manifestent !

N'oubliez jamais qu'en termes géométriques, la pente d'une droite est égale à $\tan\theta$, où θ est l'angle entre la droite et l'horizontale.

Bien sûr, les droites verticales sont exclues de la discussion ci-dessus, puisqu'elles sont une équation du type $x = x_*$!

5.5 Fonctions composées

5.5.1 Définition

Nous avons montré que les polynômes, ainsi que les fonctions trigonométriques sont dérivables et nous avons établi des formules pour leur dérivée. Mais quelle est la dérivée de $\sin x^2$? J'espère que vous le savez depuis le lycée, mais avec ce que j'ai fait dans ce cours, vous n'êtes pas encore à même de démontrer que la fonction $\sin x^2$ est dérivable et encore moins de calculer sa dérivée. Il serait temps de remédier à cette situation. Pour cela, je dois d'abord rappeler la définition de "fonction composée". Soit $g : y \in D' \mapsto g(y) \in \mathbb{R}$ et $f : x \in D \to \mathbb{R}$ deux fonctions numériques telles que $f(D) \subset D'$. On définit alors une nouvelle fonction $g \circ f : D \to \mathbb{R}$ par $(g \circ f)(x) = g(f(x))$. Par exemple, en posant $D = D' = \mathbb{R}$ et $g(y) = \sin y$, $f(x) = x^2$, on a $(g \circ f)(x) = \sin x^2$. De même, avec $f : x \in]-1, +\infty[\mapsto f(x) = (x + 1)$ et $g : y \in \mathbb{R}_*^+ \mapsto g(y) = \ln y$, on a $(g \circ f)(x) = \ln(x + 1)$. On voit ici la nécessité de restreindre le domaine de f à l'intervalle $]-1, +\infty[$, pour assurer que $f(x) > 0$, puisque la fonction logarithme n'est définie que sur $\mathbb{R}_*^+$. Il faut remarquer que j'ai choisi des noms différents pour la variable de la fonction f et celle de la fonction g. C'est très pratique pour éviter des confusions et en tout cas cela vient automatiquement dans les applications où la notion de fonction composée arrive tout naturellement. Par exemple, si je connais pour le trajet en voiture de Lille à Grenoble, la hauteur $H(x)$ au dessus de la mer en fonction de la distance x parcourue à partir de Lille (C'est marqué sur une bonne carte routière), et si je connais aussi la distance parcourue $d(t)$ en fonction du temps t (Je n'ai qu'à regarder mon odomètre), alors je peux déterminer $H(d(t))$, la hauteur à laquelle je me trouve à l'instant t. Je calcule donc ainsi la fonction composée $H \circ d$.

5.5.2 Continuité des fonctions composées

Proposition 5.14. *Soit $f : D \to \mathbb{R}$ et $g : D' \to \mathbb{R}$ deux fonctions continues telles que $f(D) \subset D'$. Alors $g \circ f$ est continue. Plus généralement, si f est continue en x_* et si g est continue en $y_* = f(x_*)$, alors $g \circ f$ est continue en x_*. En particulier, on a*

$$\lim_{x \to x_*} g(f(x)) = \lim_{y \to y_*} g(y) = g(y_*). \tag{5.7}$$

Démonstration* : Il s'agit d'un bon exercice de manipulation de epsilon-delta. Il faut montrer que, quelque soit $\epsilon > 0$, il existe $\delta > 0$ tel que, pour tout $x \in D$ on a

$$|x - x_*| < \delta \Rightarrow |g(f(x)) - g(f(x_*))| < \epsilon. \tag{5.8}$$

On sait que g est continue en $y_* = f(x_*)$. Donc, on sait que, quelque soit $\epsilon_1 > 0$, il existe $\delta_1 > 0$ tel que, pour tout $y \in D'$ on a

$$|y - y_*| < \delta_1 \Rightarrow |g(y) - g(y_*)| < \epsilon_1. \tag{5.9}$$

On sait aussi que f est continue en x_*. Par conséquent, quelque soit $\epsilon_2 > 0$, il existe $\delta_2 > 0$ tel que, pour chaque $x \in D$ on a

$$|x - x_*| < \delta_2 \Rightarrow |f(x) - f(x_*)| < \epsilon_2. \tag{5.10}$$

Soit donc $\epsilon > 0$ un réel positif quelconque. Posons $\epsilon_1 = \epsilon$ dans (5.9) et $\epsilon_2 = \delta_1$ dans (5.10). On obtient alors, en enchaînant ces implications qu'il existe $\delta_2 > 0$ tel que pour chaque $x \in D$ on a

$$|x - x_*| < \delta_2 \Rightarrow |f(x) - f(x_*)| < \delta_1 \Rightarrow |g(f(x)) - g(f(x_*))| < \epsilon, \tag{5.11}$$

ce qu'il fallait démontrer. □

Exercice 5.15. *Les affirmations suivantes, sont-elles vraies ou fausses ?*

(i) Soient $f, g : \mathbb{R} \to \mathbb{R}$, g étant continue, mais pas f. Alors $(g \circ f)$ n'est pas continue.

(ii) Soient $f, g : \mathbb{R} \to \mathbb{R}$, g étant continue, mais pas f. Alors $(f \circ g)$ n'est pas continue.

Solution : Les deux affirmations sont fausses (contrairement à ce que de nombreux étudiants affirment régulièrement) ! Pour (i), on peut par exemple prendre $g(x) = 3$, $f(x) = H(x)$, où H est la fonction de Heaviside.

5.5.3 Dérivabilité des fonctions composées

Proposition 5.16. *Soit $f : D \to \mathbb{R}$ et $g : D' \to \mathbb{R}$ deux fonctions dérivables telles que $f(D) \subset D'$. Alors $g \circ f$ est dérivable. Plus généralement, si f est dérivable en x_* et si g est dérivable en $y_* = f(x_*)$, alors $g \circ f$ est dérivable en x_* et on a*

$$(g \circ f)'(x_*) = g'(f(x_*))f'(x_*). \tag{5.12}$$

La démonstration de ce résultat est un peu plus délicate que celle de Proposition 5.14, bien qu'elle ne fasse pas intervenir des epsilons ou des deltas. Avant de la donner, je vous propose un argument incomplet qui permet de comprendre d'où sort l'importante et très utile formule (5.12). On a, en effet

$$\begin{aligned}
(g \circ f)'(x_*) &= \lim_{x \to x_*} \frac{g(f(x)) - g(f(x_*))}{x - x_*} \\
&= \lim_{x \to x_*} \frac{g(f(x)) - g(f(x_*))}{f(x) - f(x_*)} \frac{f(x) - f(x_*)}{x - x_*} \\
&= \lim_{x \to x_*} \frac{g(f(x)) - g(y_*)}{f(x) - y_*} \frac{f(x) - f(x_*)}{x - x_*} \\
&= \lim_{x \to x_*} \frac{g(f(x)) - g(y_*)}{f(x) - y_*} \lim_{x \to x_*} \frac{f(x) - f(x_*)}{x - x_*} \\
&= \lim_{y \to y_*} \frac{g(y) - g(y_*)}{y - y_*} \lim_{x \to x_*} \frac{f(x) - f(x_*)}{x - x_*} = g'(y_*) f'(x_*).
\end{aligned}$$

Pourquoi ceci n'est pas une démonstration ? D'abord, j'ai divisé par $f(x) - f(x_*)$, qui pourrait être 0 pour certaines valeurs de $x \in D, x \neq x_*$ et je n'ai pas le droit de diviser par 0. (Penser par exemple au cas où la fonction f est une constante !) Puis, dans la dernière étape de ce calcul, j'ai remplacé $f(x)$ par y comme dans la formule (5.7) ce qui nécessite une justification. Je la donnerai dans la démonstration ci-dessous.

Démonstration* : Pour justifier le calcul ci-dessus, je fais appel au subterfuge suivant. Définissons une fonction $h : D' \to \mathbb{R}$ par

$$\begin{aligned}
h(y) &= \frac{g(y) - g(y_*)}{y - y_*} \quad \text{si } y \in D', y \neq y_* \\
h(y_*) &= g'(y_*)
\end{aligned}$$

Comme g est dérivable en y_*, il résulte que h est continue en y_*. En effet, par la définition même de la dérivée de g, on a

$$\lim_{y \to y_*} h(y) = g'(y_*) = h(y_*),$$

ce qui montre précisément la continuité de h en y_*. On montre alors facilement que, quelque soit $x \in D$, tel que $x \neq x_*$ on a

$$\frac{g(f(x)) - g(f(x_*))}{x - x_*} = h(f(x)) \frac{f(x) - f(x_*)}{x - x_*}. \tag{5.13}$$

En effet, si $x \in D, x \neq x_*$, et $f(x) \neq f(x_*)$, alors

$$\begin{aligned}
\frac{g(f(x)) - g(f(x_*))}{x - x_*} &= \frac{g(f(x)) - g(f(x_*))}{f(x) - f(x_*)} \frac{f(x) - f(x_*)}{x - x_*} \\
&= h(f(x)) \frac{f(x) - f(x_*)}{x - x_*}.
\end{aligned}$$

Si, par contre, $x \in D, x \neq x_*$, mais $f(x) = f(x_*)$, on a bien évidemment

$$\frac{g(f(x)) - g(f(x_*))}{x - x_*} = 0 = h(f(x))\frac{f(x) - f(x_*)}{x - x_*}.$$

Il suffit maintenant d'appliquer à (5.13) la règle pour la limite d'un produit pour obtenir

$$\lim_{x \to x_*} \frac{g(f(x)) - g(f(x_*))}{x - x_*} = \lim_{x \to x_*} h(f(x)) \lim_{x \to x_*} \frac{f(x) - f(x_*)}{x - x_*}.$$

Comme f est continue en x_*, comme $h : D' \to \mathbb{R}$ est continue en $y_* = f(x_*)$ et comme $f(D) \subset D'$, on a finalement, en application de (5.7),

$$\lim_{x \to x_*} \frac{g(f(x)) - g(f(x_*))}{x - x_*} = \left(\lim_{y \to y_*} h(y)\right) f'(x_*) = g'(y_*)f'(x_*),$$

ce qui est le résultat escompté. □

5.5.4 Le nom des variables I

J'ai déjà insisté au début de cette section sur l'importance de donner des noms différents aux variables des fonctions g et f qu'on compose. Je veux développer un peu cette idée. Si x est la variable indépendante de f, on a tout naturellement $y = f(x)$ comme équation du graphe de f, qu'on dessinera donc dans le plan x-y. Si maintenant y est la variable indépendante de g, et que je veux tracer son graphe, il me faut un autre nom pour la variable dépendante, disons z. On aura $z = g(y)$ pour l'équation du graphe de g, que l'on dessinera dans un plan y-z. La fonction composée $g \circ f$ a maintenant x comme variable indépendante et z comme variable dépendante. Son graphe, d'équation $z = (g \circ f)(x)$ se dessine dans le plan x-z ! Pour comprendre tout cela, il suffit de penser à l'exemple $H(d(t))$ au début de la section : les rôles de x, y, z sont joués dans ce cas par t, d et H respectivement. Il est maintenant très naturel d'écrire

$$\frac{dz}{dx} = (g \circ f)'(x) = g'(f(x))f'(x) = \frac{dz}{dy}\frac{dy}{dx},$$

c'est à dire, en bref,

$$\frac{dz}{dx} = \frac{dz}{dy}\frac{dy}{dx}. \tag{5.14}$$

Ici j'ai utilisé (5.12) et les notations

$$\frac{dy}{dx} = f'(x), \quad \frac{dz}{dy} = g'(y),$$

qui sont très fortement suggérées par

$$z = g(y), \quad y = f(x).$$

Pour des raisons mnémotechnique évidentes il est beaucoup plus facile de se souvenir de (5.14) que de (5.12). Ces notations sont en plus très utiles dans les calculs un peu concrets, et utilisées presque exclusivement par les physiciens, chimistes, économistes et autres utilisateurs des mathématiques. Il est donc bon de se familiariser avec elles et de bien comprendre le lien avec les notations un peu plus formelles et précises des livres de mathématiques standards.

Une suite à cette section se trouve dans la section 8.8.7.

Exercice 5.17. *(i) Soient $f, g, h : \mathbb{R} \to \mathbb{R}$ et considérons $k = h \circ g \circ f$. En introduisant $w = h(z)$, $z = g(y)$, $y = f(x)$, montrer avec une application judicieuse et répétée de (5.12) que*

$$\frac{dw}{dx} = \frac{dw}{dz}\frac{dz}{dy}\frac{dy}{dx}.$$

(ii) Calculer la dérivée de la fonction

$$x \in \mathbb{R} \mapsto \sin(\cos(\exp x^2)) \in \mathbb{R}.$$

5.5.5 Le prolongement par continuité*

La fonction $f(x) = \frac{\sin x}{x}$ est définie (et continue) sur $D = \mathbb{R} \setminus \{0\} = \mathbb{R}_*$. En effet, on n'a pas le droit de diviser par 0. Or, nous avons vu que

$$\lim_{x \to 0} \frac{\sin x}{x} = 1,$$

ce qui suggère de définir une fonction $\tilde{f} : \mathbb{R} \to \mathbb{R}$ par $\tilde{f}(x) = f(x)$ lorsque $x \neq 0$ et $\tilde{f}(0) = 1$. De cette façon, la fonction $\tilde{f}$ est continue en 0 (et donc partout). On dit que $\tilde{f}$ est un prolongement de f par continuité. En pratique, quand un mathématicien vous parle de la fonction $\frac{\sin x}{x}$, il entend par cela la fonction $\tilde{f}$, puisqu'il sous-entend toujours le prolongement par continuité. Il s'avère que la fonction $\tilde{f}$ ainsi définie est infiniment dérivable sur $\mathbb{R}$, mais nous ne disposons pas encore des outils nécessaires pour le démontrer.

C'est précisément cette procédure de prolongement par continuité qui est utilisée dans la démonstration précédente ! En effet, la fonction

$$y \in D' \setminus \{y_*\} \mapsto \frac{g(y) - g(y_*)}{y - y_*} \in \mathbb{R}$$

n'est à priori pas définie en $y = y_*$ précisément parce que je n'ai pas le droit de diviser par 0. Or, comme g est dérivable en y_*, on peut prolonger cette fonction en y_* par continuité et c'est précisément ce que j'ai fait dans la démonstration, où j'ai appelé l'extension obtenue h.

5.6 Limites à gauche et à droite

La fonction de Heaviside n'a pas de limite en 0, on l'a vu à plusieurs reprises. Elle a néanmoins une limite à droite et une limite à gauche. Voici les définitions :

Définition 5.18. *(i) On dit que la fonction* $f : D \to \mathbb{R}$ *admet* $\ell \in \mathbb{R}$ *comme limite à droite en un point* $x_* \in \overline{D}$ *si la condition suivante est satisfaite. Pour tout* $\epsilon > 0$*, il existe* $\delta > 0$ *avec la propriété que, pour chaque* $x \in D$ *tel que* $0 < x - x_* < \delta$*, on a* $|f(x) - \ell| < \epsilon$*. On écrit alors* $\lim_{x \downarrow x_*} f(x) = \ell$.

(ii) Pareillement, on dit que la fonction $f : D \to \mathbb{R}$ *admet* $\ell \in \mathbb{R}$ *comme limite à gauche en un point* $x_* \in \overline{D}$ *si la condition suivante est satisfaite. Pour tout* $\epsilon > 0$*, il existe* $\delta > 0$ *avec la propriété que, pour chaque* $x \in D$ *tel que* $0 < x_* - x < \delta$*, on a* $|f(x) - \ell| < \epsilon$*. On écrit alors* $\lim_{x \uparrow x_*} f(x) = \ell$.

En d'autres termes, $\lim_{x \downarrow x_*} f(x) = \ell$ (respectivement $\lim_{x \uparrow x_*} f(x) = \ell$) si $f(x)$ s'approche de ℓ lorsque x s'approche de x_* à droite (respectivement à gauche).

Exercice 5.19. *Montrer que* $\lim_{x \downarrow x_*} H(x) = 1$ *et que* $\lim_{x \uparrow x_*} H(x) = 0$.

La proposition suivante, dont la démonstration est un exercice simple, est parfois utile dans les applications.

Proposition 5.20. *Soit* $f : D \to \mathbb{R}$ *et* $x_* \in \overline{D}$*.* f *admet une limite en* x_* *si et seulement si les limites à gauche et à droite de* f *en* x_* *existent et sont égales.*

On peut aussi définir les notions de dérivée à droite et à gauche, mais cça n'a pas beaucoup d'intérêt pour nous.

Chapitre 6

La fonction exponentielle

Le manque d'imagination ne constitue pas une preuve.
G.G.Emch

6.1 Introduction

Ayant préparé le terrain dans les deux chapitres précédents, nous sommes finalement en position pour faire un peu de mathématiques intéressantes, importantes et belles. Le but principal de ce chapitre est en effet de réaliser une première partie du programme d'analyse esquissé dans l'introduction du Chapitre 3. Spécifiquement, je montrerai dans la Section 6.4 que l'équation $f'(x) = f(x)$ admet une unique solution telle que $f(0) = 1$ et que cette fonction est bien donnée par

$$\lim_{n\to+\infty} P_n(x),\ \ P_n(x) = \sum_{k=0}^{n} \frac{x^k}{k!}, \tag{6.1}$$

comme nous l'avions conjecturé dans le Chapitre 3. Ce résultat n'a rien d'évident et est le premier résultat de ce cours d'analyse qui a un réel intérêt.

Nous aurons, pour arriver à nos fins, besoin des notions, techniques et résultats des deux chapitres précédents, mais cela ne suffira pas. Je me servirai en outre de deux théorèmes capitaux d'analyse : le Théorème 6.1 sur les suites adjacentes et le Théorème 6.6 sur la convergence des suites monotones. Le premier sera admis sans démonstration. Je m'en servirai pour démontrer un troisième théorème très important, le Théorème 6.14 sur la *borne supérieure* qui, à son tour, me permettra de démontrer le second. Tous les trois serviront encore à de maintes reprises dans la suite du cours.

6.2 Les suites adjacentes

Théorème 6.1. *(Théorème des suites adjacentes) Soit* $(a_n), (b_n)$ *deux suites de nombres* réels. *Supposons que, pour tout* $n \in \mathbb{N}$ *à partir d'un certain rang*

$N \in \mathbb{N}$, *on ait*

$$a_n \leq a_{n+1} \leq b_{n+1} \leq b_n.$$

Supposons aussi que $\lim_{n\to+\infty}(b_n - a_n) = 0$. *Alors il existe un nombre* réel ℓ *tel que*

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

Deux suites satisfaisants aux hypothèses du théorème sont appelées *adjacentes* (à partir du rang N). Le théorème dit donc que deux suites adjacentes

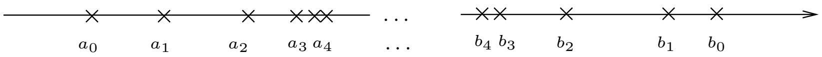

Fig. 6.1 – Deux suites adjacentes

convergent vers la même limite. Je ne le démontrerai pas, bien qu'il constitue la clé de voûte de toute l'analyse. Il est en particulier à la base de tous les théorèmes importants du cours d'analyse de cette première année, comme par exemple le théorème des valeurs intermédiaires et le théorème des accroissements finis. Dans un cours de plus haut niveau, on définit (ou construit) d'abord très soigneusement l'ensemble $\mathbb{R}$, puis on montre le théorème, mais c'est assez difficile. Vous pouvez trouver une présentation claire de tous les détails de cette démarche à laquelle sont associés quelques-uns des plus grands mathématiciens du 19ième siècle (Cauchy-Cantor-Dedekind-Weierstrass) dans le premier chapitre de [LFA]. Je vous recommande l'étude de cette matière, mais je pense que vous la trouverez très difficile tant que vous n'avez pas progressé un peu plus dans ce cours et en particulier bien compris le Chapitre 9.

Comme première illustration de l'utilisation du théorème des suites adjacentes, je vais montrer que la suite de terme général

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

converge, avec $P_n(x)$ défini en (6.1). J'aurai besoin du résultat suivant (dont la démonstration est un exercice instructif sur la définition de suite convergente que je vous invite à faire) :

Lemme 6.2. *Soit* (u_n) *une suite de nombres réels et soit* $\ell \in \mathbb{R}$. *Les deux affirmations suivantes sont équivalentes :*

(i) La suite (u_n) *converge vers* ℓ *;*

(ii) Les suites (u_{2n}) *et* (u_{2n+1}) *convergent vers* ℓ.

En d'autres termes, le lemme affirme qu'une suite converge si et seulement si les deux sous-suites obtenues en considérant uniquement les termes d'indice pair, respectivement impair, convergent et ont la même limite. Considérons alors les suites

$$b_n = P_{2n}(-1),\ a_n = P_{2n+1}(-1) = b_n - \frac{1}{(2n+1)!} \leq b_n\ .$$

Un petit calcul montre qu'elles sont adjacentes. En effet, $(a_n - b_n)$ tend clairement vers 0 et on vient de remarquer que $a_n \leq b_n$. Par ailleurs,

$$a_{n+1} - a_n = \frac{1}{(2n+2)!} - \frac{1}{(2n+3)!} \geq 0,$$

donc la suite (a_n) est croissante. On vérifie de la même façon que (b_n) est décroissante. Le Théorème 6.1 permet donc de conclure qu'elles convergent vers une même limite. Utilisant le lemme on conclut finalement que la suite $P_n(-1)$ converge. Il faut remarquer la puissance du Théorème 6.1. Vérifier que deux suites sont adjacentes est souvent très facile et le théorème permet d'en tirer immédiatement une conclusion forte, à savoir qu'elle converge.

Le Théorème 6.1 peut en outre être utilisé pour obtenir des valeurs approchées de la limite commune des suites adjacentes, via la remarque suivante :

Corollaire 6.3. *Soient (a_n) et (b_n) deux suites adjacentes à partir d'un certain rang $N \in \mathbb{N}$ et de limite commune ℓ. Alors, pour tout $n \geq N$ on a :*

$$a_n \leq \ell \leq b_n \quad \textit{et donc} \quad 0 \leq \ell - a_n \leq (b_n - a_n).$$

Démonstration : On a, pour tout $n \geq N$ et quelque soit $m \in \mathbb{N}$

$$a_n \leq a_{n+m}.$$

Par conséquent, en prenant la limite lorsque m tend vers l'infini (avec n fixé) et en utilisant la Proposition 4.8 (passage à la limite dans les inégalités), on a :

$$a_n = \lim_{m\to+\infty} a_n \leq \lim_{m\to+\infty} a_{n+m} = \ell.$$

On montre l'autre inégalité de la même façon. □

En application du Corollaire on obtient immédiatement le résultat suivant. Soit $\ell = \lim_{n\to+\infty} P_n(-1)$. On a, pour tout $n \in \mathbb{N}$,

$$0 \leq \ell - P_{2n+1}(-1) \leq \frac{1}{(2n+1)!}$$

Exercice 6.4. *Calculer une valeur approchée de ℓ, à $0,01$ près. Même question pour $0,001$ et $0,0001$. Demander à sa calculatrice la valeur de $\exp -1$ et comparer. Relire l'introduction du Chapitre 3 et expliquer ses observations.*

Le lecteur s'entraîne

1. Soient (u_n) et (v_n) deux suites définies par : $u_0 = a \in \mathbb{R}_+^*$, $v_0 = b \in \mathbb{R}_+^*$ et

$$\forall n \in \mathbb{N} \qquad u_{n+1} = \frac{u_n + v_n}{2} \qquad v_{n+1} = \sqrt{u_n \cdot v_n}.$$

Montrer que (u_n) et (v_n) sont deux suites adjacentes, et donc qu'elles convergent vers une même limite (que l'on ne demande pas de calculer).

2. On considère les deux suites réelles définies pour $n \geq 1$ par :

$$u_n = P_n(1) = 1 + \frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{1}{n!}, \qquad v_n = u_n + \frac{1}{n!}.$$

Montrer que ces deux suites sont adjacentes et qu'elles convergent vers un irrationnel ℓ. Calculer une valeur approchée de ℓ avec une précision de 10^{-5}. Le résultat vous dit-il quelque chose ?

6.3 Les suites monotones

Il n'est pas nécessaire, je suppose, de vous rappeler la définition d'une suite croissante ou décroissante mais je le fais tout de même :

Définition 6.5. *Soit une suite réelle (u_n). On dit que (u_n) est*
(i) croissante si et seulement si, quelque soit $n \in \mathbb{N}$, on a : $u_n \leq u_{n+1}$;
(ii) décroissante si et seulement si, quelque soit $n \in \mathbb{N}$, on a : $u_n \geq u_{n+1}$.

Bien évidemment, une suite monotone est une suite qui est soit croissante, soit décroissante. Vous devinez également facilement ce qu'on entend par une suite strictement croissante, strictement décroissante ou strictement monotone. Dans beaucoup d'applications les suites ne sont monotones qu'à partir d'un certain rang.

Le second grand théorème sur la convergence de suites est le suivant :

Théorème 6.6. *(Théorème des suites monotones)*
(i) Une suite croissante est convergente si et seulement elle est majorée ;
(ii) Une suite décroissante est convergente si et seulement si elle est minorée.

Je démontrerai ce résultat dans la Section 6.7, après avoir préparé le terrain dans les Sections 6.5-6.6. La démonstration utilisera le Théorème 6.1 et n'est pas facile. Pourtant, intuitivement, le Théorème 6.6 semble assez évident, comme le dessin ci-dessous le montre, je pense. Je donne tout de suite deux illustrations

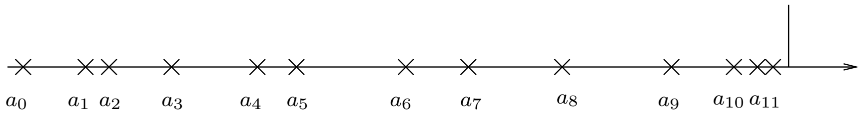

Fig. 6.2 – Une suite croissante majorée converge

de son utilisation. Considérons d'abord la suite

$$u_n = \sum_{k=1}^{n} \frac{1}{k^2} = 1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \cdots + \frac{1}{n^2}.$$

Elle est évidemment croissante. Est-elle convergente ? Pour trancher la question, il suffira de décider si elle est majorée. C'est en effet le cas, comme on peut le voir avec l'astuce suivante. On remarque d'abord que, quelque soit $k \in \mathbb{N}, k \geq 2$, on a :

$$\frac{1}{k^2} < \frac{1}{k(k-1)} = \frac{1}{(k-1)} - \frac{1}{k}.$$

Par conséquent :

$$\begin{aligned} u_n &= \sum_{k=1}^{n} \frac{1}{k^2} < 1 + \sum_{k=2}^{n} \frac{1}{k(k-1)} \\ &< 1 + \sum_{k=2}^{n} (\frac{1}{(k-1)} - \frac{1}{k}) \\ &< 1 + (\frac{1}{1} - \frac{1}{2}) + (\frac{1}{2} - \frac{1}{3}) + \cdots + (\frac{1}{n-1} - \frac{1}{n}) \\ &< 1 + 1 - \frac{1}{n}. \end{aligned}$$

On en conclut que, quelque soit $n \in \mathbb{N}$, $u_n < 2$: (u_n) est majorée. Le Théorème 6.6 (i) implique donc que la suite (s_n) est convergente. Quelle est sa limite ? Cette question est plus difficile ! Le Théorème 6.6 est un théorème d'existence : il affirme l'existence de la limite, mais reste muet lorsqu'il s'agit de savoir où elle se trouve ! Il faut, dans chaque cas, trouver d'autres moyens pour localiser la limite. Pour la suite u_n ci-dessus, je reviendrai sur la question dans la Section **??**.

Exercice 6.7. *Montrer que les affirmations suivantes sont vraies :*
(i) Une suite croissante est majorée si et seulement si elle est bornée.
(ii) Une suite décroissante est minorée si et seulement si elle est bornée.
(iii) Une suite monotone est convergente si et seulement si elle est bornée.
Attention ! Ces affirmations sont dangereuses : elles deviennent fausses quand on oublie le "croissant", le décroissant" ou le "monotone" dans leurs énoncés, ce que les étudiants ont la fâcheuse habitude de faire.

Exercice 6.8. *Soit, pour $p \in \mathbb{N}$, la suite $u_n(p) = \sum_{k=1}^{n} \frac{1}{k^p}$. Montrez que ces suites convergent si $p > 1$.*

6.4 La fonction exponentielle

Nous voici correctement équipés pour attaquer la convergence des suites $P_n(x)$, définies en (6.1) :

Proposition 6.9. *Pour tout $x \in \mathbb{R}$, la suite $(P_n(x))$ converge.*

Afin de montrer la Proposition, nous aurons besoin du lemme suivant :

Lemme 6.10. *Soit $r \in \mathbb{R}$. On a :*
(i) Si $r \neq 1$, alors, pour tout $n \in \mathbb{N}$, $\sum_{k=0}^{n} r^k = \frac{r^{n+1}-1}{r-1}$;
(ii) Si $|r| < 1$, $\sum_{k=0}^{\infty} r^k = \frac{1}{1-r}$

Je vous rappelle la notation introduite au Chapitre 3 :

$$\sum_{k=0}^{\infty} d_k = \lim_{n\to+\infty} \sum_{k=0}^{n} d_k.$$

Démonstration : Le (i) a été démontré dans la Section 2.9.

(ii) En utilisant le (i) on obtient :

$$\begin{aligned}
\sum_{k=0}^{\infty} r^k &= \lim_{n\to+\infty} \sum_{k=0}^{n} x = r^k \\
&= \frac{1}{1-r} + \lim_{n\to+\infty} \frac{r^{n+1}}{r-1} \\
&= \frac{1}{1-r} + \frac{1}{r-1} \lim_{n\to+\infty} r^{n+1},
\end{aligned}$$

ce qui donne le résultat puisque $|r| < 1$. □

On appelle $(\sum_{k=0}^{n} r^k)$ *la série géométrique de raison* r. Le lemme dit donc que la série géométrique de raison r converge vers $1/(1-r)$ pourvu que $|r| < 1$. Ce lemme, qui est très simple, est très important et souvent très utile (A bon entendeur, mi-mot ...) : vous en verrez une première utilisation dans la démonstration suivante.

Démonstration de la Proposition* : Je traiterai séparément les cas $x \geq 0$ et $x < 0$, qui nécessitent des approches différentes. Considérons d'abord le cas où $x \geq 0$. La suite $(P_n(x))$ est alors croissante,

$$P_{n+1}(x) = P_n(x) + \frac{x^{n+1}}{(n+1)!} \geq P_n(x),$$

et il suffira donc de montrer qu'elle est majorée pour conclure en utilisant le Théorème 6.6. Soit donc $x \geq 0$ fixé et choisissons un entier naturel $K \in \mathbb{N}$ tel que $K > 2x$. Etant donné x, un tel entier existe bien évidemment. Par exemple, si $x = \sqrt{2}$, je peux prendre $K = 5$, et si $x = \pi$, je peux prendre $K = 10$. Par la suite, x et K sont fixés. Je vais maintenant réutiliser l'idée de la démonstration du Lemme 4.23 (iii) pour établir que, quelque soit $n \in \mathbb{N}$, on a :

$$P_n(x) \leq P_{K-1}(x) + 2\frac{x^K}{K!}. \tag{6.2}$$

Comme le membre de droite ne dépend pas de n, ceci montrera bien que la suite croissante $(P_n(x))$ est majorée par $P_{K-1}(x) + 2\frac{x^K}{K!}$ et est donc convergente. Remarquons d'abord que, si $n \leq (K-1)$, (6.2) est certainement vérifié puisque la suite $(P_n(x))$ est croissante. Afin de montrer (6.2) lorsque $n \geq K$, j'écris $n = K + m, m \geq 0$ et je fais remarquer que

$$P_{K+m}(x) = P_{K-1}(x) + \sum_{k=K}^{K+m} \frac{x^k}{k!}. \tag{6.3}$$

Pour $k \geq K$ on a

$$\begin{aligned} \frac{x^k}{k!} &= \frac{x}{k}\frac{x^{k-1}}{(k-1)!} \leq \frac{x}{K}\frac{x^{k-1}}{(k-1)!} \\ &\leq \frac{1}{2}\frac{x^{k-1}}{(k-1)!} \leq \frac{1}{2^2}\frac{x^{k-2}}{(k-2)!} \\ &\leq \cdots \leq \frac{1}{2^{k-K}}\frac{x^K}{K!} \end{aligned}$$

On trouve alors, en utilisant le Lemme 6.10 (i),

$$\begin{aligned} \sum_{k=K}^{K+m} \frac{x^k}{k!} &= \sum_{\ell=0}^{m} \frac{x^{K+\ell}}{(K+\ell)!} \\ &< \sum_{\ell=0}^{m} \left(\frac{1}{2}\right)^{\ell} \frac{x^K}{K!} = \frac{(1/2)^{(\ell+1)}-1}{(1/2)-1}\frac{x^K}{K!} = 2\frac{x^K}{K!}\left(1-(1/2)^{(\ell+1)}\right) \\ &< 2\frac{x^K}{K!}. \end{aligned}$$

Insérant cette inégalité en (6.3), on a immédiatement (6.2) pour $n = K+m \geq K$.

Au delà des notations et des calculs, il est important de comprendre le mécanisme de cette démonstration : nous avons montré que la suite $(P_n(x))$ est croissante et que, à partir d'un certain rang, elle est majorée par la série géométrique de raison $1/2$, dont nous avions montré auparavant la convergence. Nous aurons encore l'occasion d'utiliser cette approche à de maintes reprises.

Passons maintenant au cas où $x < 0$. La suite $P_n(x)$ n'est maintenant pas croissante puisque $x^n < 0$ lorsque n est impair. Il nous faut donc une autre stratégie de démonstration. Le cas $x = -1$ a déjà été traité dans la Section 6.2 et la même démonstration fonctionne pour le cas général. On considère les suites

$$a_n(x) = P_{2n+1}(x) \quad \text{et} \quad b_n(x) = P_{2n}(x),$$

dont on montre facilement qu'elles sont adjacentes à partir d'un certain rang. Par exemple, on a ($x < 0$!)

$$a_{n+1}(x) - a_n(x) = \frac{x^{2n+2}}{(2n+2)!}(\frac{x}{2n+3}+1) = \frac{x^{2n+2}}{(2n+2)!}(1-\frac{|x|}{2n+3}).$$

Par conséquent, (a_n) est une suite croissante à partir d'un rang K tel que $2K+3 > |x|$. Les autres calculs pour vérifier que les deux suites sont adjacentes se font pareillement et je vous invite à les faire. On conclut en utilisant le Théorème 6.1 et le Lemme 6.2. □

La Proposition nous permet maintenant de définir une fonction à partir des suites $(P_n(x))$:

Définition 6.11. *La fonction exponentielle (notée* exp*) est la fonction de domaine $\mathbb{R}$ définie pour tout $x \in \mathbb{R}$ par :*

$$\exp x = \lim_{n\to+\infty} P_n(x).$$

Il est vrai, mais pas du tout clair jusqu'ici, que la fonction que je viens de définir est bien celle que vous avez appelée la fonction exponentielle au lycée. Pour cela, il faudra que je montre qu'elle a une fonction réciproque et que celle-ci est une primitive de $1/x$. Je le montrerai plus tard, dans le Chapitre 8. Pour le moment, je me contenterai de montrer les plus importantes de ses propriétés.

Théorème 6.12. *La fonction exponentielle a les propriétés suivantes :*

(i) Elle est dérivable et elle est l'unique solution de $f'(x) = f(x)$ *telle que* $f(0) = 1$ *;*

(ii) Pour tout $x \in \mathbb{R}$, $\exp x > 0$ *;*

(iii) $\forall a, b \in \mathbb{R},\ \exp(a + b) = \exp a \exp b$;

(iv) Pour tout $p \in \mathbb{N}$, $\lim_{x\to+\infty} x^{-p} \exp x = +\infty$ *;*

(v) Pour tout $p \in \mathbb{N}$, $\lim_{x\to+\infty} x^{p} \exp -x = 0$.

Avant de passer à la démonstration, quelques remarques. Le (i) du théorème est riche en informations. Il dit trois choses distinctes : d'abord qu'il existe une fonction f tel que $f'(x) = f(x),\ f(0) = 1$, ensuite qu'elle est donnée par la fonction définie dans la Définition 6.11, et finalement que l'équation en question n'admet pas d'autres solutions. Ce dernier point est particulièrement important et, comme les autres, pas du tout clair à priori.

Si, dans le point (iv), on met $p = 0$, on obtient que la fonction exponentielle tend vers plus l'infini lorsque x tend vers plus l'infini. Or, les fonctions x, ou x^2, x^3 et plus généralement toutes les puissances de x tendent également vers plus l'infini lorsque x tend vers plus l'infini. On sent bien que, plus la puissance est élevée, plus cette convergence est rapide. On peut donner un sens précis à cette idée de la façon suivante. Si f et g sont deux fonctions qui tendent vers $+\infty$ lorsque x tend vers $+\infty$, on dit que "f tend plus vite vers $+\infty$ que g" lorsque

$$\lim_{x\to+\infty} \frac{f(x)}{g(x)} = +\infty.$$

En effet, dans ce cas $f(x)/g(x)$ sera "beaucoup plus grand que 1" lorsque x est suffisamment grand. L'idée est donc parfaitement analogue à celle utilisée dans la discussion sur les développements limités pour étudier la vitesse de convergence vers 0 (voir (5.2) ainsi qu'à celle sur la vitesse de convergence de suites dans la section 4.7. Par exemple, x^2 tend "plus vite" vers plus l'infini que x puisque $x^2/x = x$ tend aussi vers plus l'infini, ce qui signifie en effet que, pour x assez grand, x^2 est "beaucoup plus grand" que x. Dans la même veine, on peut dire que, lorsque $p_1 > p_2$, x^{p_1} tend plus vite vers plus l'infini que x^{p_2}. Ce que le (iv) affirme donc finalement est que la fonction exponentielle tend plus vite vers plus l'infini que n'importe quelle puissance de x et donc plus vite que n'importe quel polynôme. Une "croissance exponentielle" est donc plus rapide que n'importe quelle "croissance polynômiale". Le (iv) est d'ailleurs parfaitement analogue au (iii) du Lemme 4.23. Cette discussion permet de comprendre pourquoi on considère une "croissance exponentielle" comme étant une croissance très rapide. Un discours analogue s'applique au (v) : la fonction $\exp(-x)$ tend vers 0 plus vite que n'importe quelle puissance négative de x, lorsque x tend vers plus l'infini. On peut aussi dire les choses un peu différemment. La fonction $\exp(-x)$ tend vers 0 lorsque x tend vers l'infini. Considérons maintenant $x^{100}\exp -x$. Comme x^{100} tend vers plus l'infini et que $\exp(-x)$ tend vers 0 on peut se demander ce qui se passera avec leur produit : "Est-ce que la croissance de x^{100} réussira à vaincre la décroissance de $\exp(-x)$ de façon à ce que le produit tend encore vers plus l'infini ou est-ce que, au contraire, la décroissance de $\exp(-x)$ est tellement forte qu'elle arrivera à dompter la croissance de x^{100} ?" Le (v) dit que c'est ce dernier cas de figure qui se présente.

Démonstration : La démonstration est relativement longue, mais pas vraiment difficile. Seulement la première partie est un peu fastidieuse. Les autres introduisent de belles idées mathématiques que nous aurons l'occasion de réutiliser dans d'autres contextes.

(i) Il faut montrer que

$$\lim_{h\to 0}\frac{\exp(x+h)-\exp x}{h}=\exp x,$$

ou, ce qui revient au même, que

$$\lim_{h\to 0}\frac{|\exp(x+h)-\exp x-h\exp x|}{|h|}=0.$$

Dans ce but, je vais réécrire $\exp(x+h)-\exp x-h\exp x$ d'une façon un peu spéciale, particulièrement bien adaptée à nos besoins. L'astuce consiste à remarquer que

$$\exp x=\lim_{n\to+\infty}P_n(x)=\lim_{n\to+\infty}P_{n-1}(x)$$

et que

$$P_n'(x)=\sum_{k=0}^{n}\frac{kx^{k-1}}{k!}=P_{n-1}(x),$$

de façon à ce que

$$h\exp x=h\lim_{n\to+\infty}P_{n-1}(x)=\lim_{n\to+\infty}\sum_{k=0}^{n}\frac{hkx^{k-1}}{k!}.$$

On a donc

$$\exp(x+h)-\exp x-h\exp x=\lim_{n\to+\infty}\sum_{k=0}^{n}\frac{1}{k!}[(x+h)^k-x^k-hkx^{k-1}].$$

Ecrite sous cette forme, l'expression $\exp(x+h)-\exp x-h\exp x$ sera relativement facile à étudier. Utilisons d'abord la formule du binôme de Newton pour écrire

$[(x+h)^k - x^k - hkx^{k-1}]$:

$$
\begin{aligned}
[(x+h)^k - x^k - hkx^{k-1}] &= C_k^0 x^k + C_k^1 x^{k-1}h + C_k^2 x^{k-2}h^2 + \cdots + C_k^{k-2}x^2h^{k-2} \\
&\qquad + C_k^{k-1}xh^{k-1} + C_k^k h^k - x^k - hkx^{k-1} \\
&= C_k^2 x^{k-2}h^2 + C_k^3 x^{k-3}h^3 + \cdots + C_k^{k-2}x^2h^{k-2} \\
&\qquad + C_k^{k-1}xh^{k-1} + C_k^k h^k \\
&= \sum_{\ell=2}^{k} C_k^\ell x^{k-\ell}h^\ell \\
&= h^2 \sum_{\ell=2}^{k} C_k^\ell x^{k-\ell}h^{\ell-2},
\end{aligned}
$$

où je me suis servi de $C_k^k = 1, C_k^{k-1} = k$. Dans la dernière ligne, j'ai fait exprès de mettre en facteur h^2, qui est commun à tous les termes. Supposons maintenant que $|h| \leq 1$. Il en résulte alors $|h|^{\ell-2} \leq 1$ et donc

$$
\begin{aligned}
|(x+h)^k - x^k - hkx^{k-1}| &\leq |h|^2 \sum_{\ell=2}^{k} C_k^\ell |x|^{k-\ell} \\
&\leq |h|^2 \sum_{\ell=0}^{k} C_k^\ell |x|^{k-\ell},
\end{aligned}
$$

où j'ai tout simplement ajouté deux termes positifs à la somme en passant de la première ligne à la seconde. Mais la formule du binôme de Newton appliquée à $(|x|+1)^k$ donne

$$\sum_{\ell=0}^{k} C_k^\ell |x|^{k-\ell} = (|x|+1)^k,$$

d'où l'on obtient finalement que

$$|(x+h)^k - x^k - hkx^{k-1}| \leq h^2(|x|+1)^k.$$

On a en fin de compte que

$$
\begin{aligned}
|\exp(x+h) - \exp x - h\exp x| &= \lim_{n\to+\infty} \Big|\sum_{k=0}^{n} \frac{1}{k!}[(x+h)^k - x^k - hkx^{k-1}]\Big| \\
&\leq \lim_{n\to+\infty} \sum_{k=0}^{n} \frac{1}{k!}|(x+h)^k - x^k - hkx^{k-1}| \\
&\leq \lim_{n\to+\infty} \sum_{k=0}^{n} \frac{1}{k!}h^2(|x|+1)^k \\
&\leq h^2 \exp(|x|+1),
\end{aligned}
$$

où j'ai utilisé la définition de la fonction exponentielle dans la dernière ligne. On a donc

$$0 \leq \frac{|\exp(x+h) - \exp x - h \exp x|}{|h|} \leq |h| \exp(|x|+1),$$

ce qui permet de conclure en utilisant le théorème des gendarmes (version Proposition 4.8 (ii)).

Puisque la définition de la fonction exponentielle implique de façon évidente que $\exp 0 = 1$, nous venons donc de montrer que la fonction exponentielle est dérivable et qu'elle satisfait l'équation $f'(x) = f(x), f(0) = 1$. Il me reste à montrer que la fonction exponentielle est l'*unique* fonction telle que $f'(x) = f(x), f(0) = 1$.

Pour cela, j'ai besoin du (ii), que je montre donc d'abord.

(ii) Pour $x \geq 0$ cette affirmation est évidente puisqu'alors, pour tout n, $P_n(x) \geq 1$. Lorsque $x < 0$, les polynômes $P_n(x)$ prennent des valeurs négatives et il n'est donc plus si évident que la limite de $P_n(x)$, lorsque n tend vers l'infini, est positif. La démonstration que je donne du (ii) contourne ce problème en évitant d'utiliser les polynômes dans l'argument. Considérons la fonction $h : x \in \mathbb{R} \to h(x) = (\exp(-x))(\exp x) \in \mathbb{R}$. Utilisant le résultat du (i) et la règle de dérivation d'un produit, on a

$$\begin{aligned} h'(x) &= (\exp(-x))'(\exp x) + (\exp(-x))(\exp x)' \\ &= -(\exp(-x))(\exp x) + (\exp(-x))(\exp x) = 0. \end{aligned}$$

La fonction h est donc dérivable et de dérivée nulle. On en conclut que h est une fonction constante. (J'utilise ici un résultat qui vous est familier depuis l'époque du lycée et que je montrerai plus tard (Théorème 7.8).) Comme $h(0) = 1$, il en résulte que

$$(\exp(-x))(\exp x) = 1, \tag{6.4}$$

pour tout $x \in \mathbb{R}$. Puisque la définition de la fonction exponentielle implique clairement que, pour tout $x \geq 0, \exp x > 1 > 0$, on conclut que $(\exp(-x)) = 1/\exp x > 0$, ce qui démontre le résultat.

Suite de la démonstration du (i) : Il me reste à montrer que la fonction exponentielle est *l'unique* fonction telle que $f'(x) = f(x), f(0) = 1$. Dans ce but, supposons que $f : \mathbb{R} \to \mathbb{R}$ soit une telle fonction et considérons la fonction $k : \mathbb{R} \to \mathbb{R}$:

$$k(x) = \frac{f(x)}{\exp x}.$$

La fonction k est bien définie parce que, selon (ii), $\exp x \neq 0$, pour tout $x \in \mathbb{R}$. Utilisant la règle de dérivation d'un quotient et $f'(x) = f(x)$ on obtient

$$k'(x) = \frac{f'(x)(\exp x) - f(x)(\exp x)'}{(\exp x)^2} = 0.$$

La fonction k est donc constante, et comme $k(0) = 1$, on trouve $k(x) = 1$, pour tout $x \in \mathbb{R}$. On a donc bien

$$f(x) = \exp x,$$

ce qui montre le résultat.

(iii) Comme

$$\exp(a+b) = \lim_{n\to+\infty} P_n(a+b) \quad \text{et} \quad \exp a \exp b = \lim_{n\to+\infty} P_n(a)P_n(b),$$

on pourrait montrer ce résultat en montrant que

$$\lim_{n\to+\infty} P_n(a+b) = \lim_{n\to+\infty} P_n(a)P_n(b),$$

mais cette démonstration nécessite des calculs longs et terriblement fastidieux, provoqués par le fait que bien évidemment $P_n(a+b) \neq P_n(a)P_n(b)$. Je vais donc procéder différemment. Considérons la fonction $t : \mathbb{R} \to \mathbb{R}$ définie par :

$$t(x) = (\exp(-a))(\exp(a+x)).$$

On voit, en utilisant (6.4) que $t(0) = 1$. En utilisant ensuite la première partie du résultat de (i), à savoir que exp est dérivable et égale à sa propre dérivée, on voit également que $t'(x) = t(x)$. Par conséquent, la partie "unicité" de (i) implique que

$$t(x) = \exp x.$$

On trouve donc, en posant $x = b$,

$$\exp(-a)\exp(a+b) = \exp b,$$

d'où le résultat suit en multipliant les deux membres de cette égalité avec $\exp a$ et en utilisant encore une fois (6.4). Il faut remarquer que cette démonstration est très simple, et repose de façon essentielle sur l'unicité de la solution de l'équation $f'(x) = f(x), f(0) = 1$, montrée auparavant.

(iv) Nous avons déjà remarqué à plusieurs reprises que pour tout $x \geq 0$ et pour tout $n \in \mathbb{N}$ on a :

$$P_n(x) \leq \exp x.$$

Par ailleurs on a également

$$\frac{x^n}{n!} \leq P_n(x).$$

Il en résulte donc pour tout $n, p \in \mathbb{N}$ que

$$\frac{x^{n-p}}{n!} \leq x^{-p}\exp x.$$

En prenant $n > p$, le résultat suit immédiatement du Lemme 4.32.

(v) Ceci est une conséquence immédiate du (iv) puisque

$$x^{-p}\exp x = \frac{1}{x^p \exp(-x)}.$$

$\square$

Le lecteur s'entraîne

1. (i) Montrer que si une suite $u_n = \sum_{k=0}^{n} d_k$ converge, alors la suite d_n converge vers 0.

(ii) Montrer que la suite $u_n = \sum_{k=1}^{n} \frac{1}{\sqrt{k}}$ diverge. En conclure que dans (i) l'implication réciproque est fausse.

2. Dans l'Exercice 6.8 nous avons vu que les suites $u_n(p) = \sum_{k=1}^{n} \frac{1}{k^p}$ convergent lorsque $p \geq 2$. Nous venons de voir dans l'exercice précédent que la suite $u_n(p)$ diverge lorsque $p = 1/2$. Montrer que la suite $\sum_{k=1}^{n} \frac{1}{k}$ (appelée série harmonique) diverge également.

3. Le Lemme 6.10 pose une question évidente : “Que fait la série géométrique de raison x quand $|x| \geq 1$?” Montrer qu'elle diverge. **Indication :** penser à utiliser le (i) de l'exercice 1 ci-dessus.

4. Etudier la convergence des suites $P_n(x) = \sum_{k=1}^{n} \frac{x^k}{k^2}$ en fonction de x. Même question pour $P_n(x) = \sum_{k=1}^{n} \frac{x^k}{k^p}$, avec $p \in \mathbb{N}$. **Indication :** Il s'agit d'appliquer les techniques de la démonstration de la Proposition 6.9.

6.5 Max, min, sup, inf et les autres

Le reste de ce chapitre est consacré à la démonstration du théorème des suites croissantes (Théorème 6.6). La démonstration n'est pas facile et nécessite un peu de préparation, qui sera faite dans cette section et la suivante. Nous montrerons en route le très important théorème de la borne supérieure (Théorème 6.14), dont le Théorème 6.6 sera essentiellement un corollaire.

Nous avons besoin des définitions suivantes :

Définition 6.13. *Soit E un sous-ensemble de $\mathbb{R}$.*

(i) Soit $M \in \mathbb{R}$. On dit que M est un majorant de E si et seulement si pour tout $x \in E$ on a $x \leq M$.

(ii) Soit $m \in \mathbb{R}$. On dit que m est un minorant de E si et seulement si pour tout $x \in E$ on a $m \leq x$.

(iii) Soit $M \in E$. On dit que M est un maximum (ou un plus grand élément) de E si et seulement si pour tout $x \in E$ on a $x \leq M$. On écrit alors $M = \max E$.

(iv) Soit $m \in E$. On dit que m est un minimum (ou un plus petit élément) de E si et seulement si pour tout $x \in E$ on a $m \leq x$.On écrit alors $m = \min E$

Un sous-ensemble E de $\mathbb{R}$ est majoré (minoré) s'il admet un majorant (minorant). Il est borné si et seulement si il est majoré et minoré. Tout ceci est très simple, mais marqué du sceau de la pédanterie du langage mathématique et quelques exemples aideront à clarifier les choses. Soit $E =]0, 1]$; π est alors un majorant de E, ainsi que 10^{10} et 1. Il est clair qu'aucun majorant de E n'est plus petit que 1. Comme 1 appartient à E, 1 est un plus grand élément de E. On peut (et on doit) s'étonner de l'utilisation de l'article indéfini “un” dans ce contexte puisqu'il semble clair qu'il ne peut y avoir deux plus grands éléments distincts ! C'est évidemment vrai et se démontre facilement (Faites le !), mais au moment d'écrire la définition nous ne le savions pas encore, et donc il convenait d'écrire "un" plutôt que "le" maximum. A partir de maintenant je dirai "le maximum", lorsqu'il existe. Retournons à $E =]0,1]$. On voit que -1, $-\sqrt{2}$ et 0 sont des minorants de E. Il est clair que 0 est le plus grands des minorants, mais comme 0 n'appartient pas à E, ce n'est pas un plus petit élément. L'intervalle $]0,1]$ n'a pas de plus petit élément. Un sous-ensemble borné de $\mathbb{R}$ peut donc ne pas avoir de maximum ou de minimum. Par contre, il a toujours un plus petit majorant et un plus grand minorant, comme l'affirme le Théorème 6.14 :

Théorème 6.14. *(Théorème de la borne supérieure)*

(i) Soit E un sous-ensemble non-vide et majoré de $\mathbb{R}$. L'ensemble des majorants de E admet un plus petit élément, que l'on appelle la borne supérieure de E (et que l'on désigne par $\sup E$*).*

(ii) Soit E un sous-ensemble non-vide et minoré de $\mathbb{R}$. L'ensemble des minorants de E admet un plus grand élément, que l'on appelle la borne inférieure de E (et que l'on désigne par $\inf E$*).*

Remarque : Notez bien que le minimum et le maximum de E appartiennent toujours à E, mais tel n'est pas le cas de la borne supérieure et inférieure, comme les exemples ci-dessous le montrent.

On a $\sup E = 1, \inf E = 0$ lorsque $E =]0,1]$. Plus généralement, lorsque $a < b$ et E est un des intervalles $[a,b],]a,b],]a,b[, [a,b[$, on a $\inf E = a, \sup E = b$. Pour un intervalle les notions de borne supérieure et borne inférieure ne présentent donc pas un intérêt particulier, puisqu'elles ne sont alors que des façons compliquées de parler des extrémités de l'intervalle. Le théorème ne devient intéressant que lorsqu'on a affaire à des sous-ensembles un peu plus compliqués. Un premier exemple est

$$E = \{u_n \mid n \in \mathbb{N}\},$$

où (u_n) est une suite croissante majorée. Le théorème garantit que E a une borne supérieure, ce qui n'est pas clair à priori. Un autre exemple un peu plus compliqué encore est celui-ci :

$$F = \{x \in [0,1] \mid \forall n \in \mathbb{N}, 10^n x - E(10^n x) > 10^{-1}\},$$

où $E(10^n x)$ désigne la partie entière de $10^n x$. Comme F est un sous-ensemble de l'intervalle $[0,1]$, il est certainement borné, mais il n'est pas tout de suite clair qu'il a une borne supérieure et inférieure. Le théorème affirme que c'est le cas.

Exercice 6.15. *Déterminer la borne supérieure et la borne inférieure de l'ensemble F ci-dessus. F admet-il un maximum et/ou un minimum ? F contient-il un intervalle ?* **Indication :** *Si vous trouvez cet exercice difficile, revenez-y après avoir étudié le Chapitre 9.*

Exercice 6.16. *Montrer qu'une fonction $f : D \to \mathbb{R}$ est minorée (respectivement majorée, bornée) si et seulement si son image $f(D)$ est minorée (respectivement majorée, bornée).*

La définition de la borne supérieure paraît simple : c'est le plus petit majorant. En pratique, elle est rarement utile sous cette forme, et nous nous servirons régulièrement du résultat suivant, qui donne une caractérisation de la borne supérieure qui est plus compliquée, mais plus maniable.

Proposition 6.17. *(Caractérisation de la borne supérieure) Soit E un sous-ensemble non-vide et majoré de $\mathbb{R}$. Soit $M \in \mathbb{R}$. Alors les trois affirmations suivantes sont équivalentes :*

(i) $M = \sup E$;

(ii) M est un majorant de E et, quelque soit $\epsilon > 0$, il existe $x \in E$ tel que $M - \epsilon < x \leq M$;

(iii) M est un majorant de E et il existe une suite $(x_n \in E)$ telle que $\lim_{n\to+\infty} x_n = M$.

Le (ii) exprime tout simplement que, M est un majorant de E, mais que $M - \epsilon$ n'est plus un majorant, quelque soit $\epsilon > 0$, ce qui montre bien que M est le plus petit majorant. L'importance ou l'intérêt de cette proposition ne peut vous devenir clair que lorsque nous nous en servirons (dans les deux sections suivantes). Comme il est difficile de travailler la démonstration d'un résultat dont on ne voit pas très bien l'importance, une bonne stratégie consiste à continuer l'étude des sections suivantes, pour revenir sur la démonstration de la proposition ci-dessus lorsque vous en aurez besoin.

Remarquons encore qu'il existe une proposition analogue pour la borne inférieure, que je vous laisse le soin de rédiger tout seul.

Démonstration : $(i) \Rightarrow (ii)$ Comme $M = \sup E$, M est un majorant. Soit $\epsilon > 0$. Alors $M - \epsilon$ n'est pas un majorant, puisque $M = \sup E$ est le plus petit des majorants. Il existe donc un élément x de E strictement plus grand que $M - \epsilon$, c'est à dire tel que $M - \epsilon < x \leq M$.

$(ii) \Rightarrow (i)$ Il faut montrer qu'un nombre réel M qui a la propriété énoncée dans le (ii) est forcément le plus petit majorant de E. En d'autres termes, il faut montrer que, si N est un réel strictement plus petit que M $(N < M)$, alors N n'est pas un majorant. Or, posant $\epsilon = M - N > 0$, on a $N = M - \epsilon$ et (ii) garantit alors l'existence d'un élément x de E tel que $N = M - \epsilon < x \leq M$. On troueve donc $N < x$, ce qui montre que N n'est pas un majorant de E.

$(ii) \Leftrightarrow (iii)$ Je vous passe la main. □

Le lecteur s'entraîne

1. Déterminer explicitement les sous-ensembles de $\mathbb{R}$ suivants :

a) $A = \{x \in [0,1] \mid \exists n \in \mathbb{N}^*, \frac{1}{n} \leq x \leq 1\}$;

b) $B = \{x \in [0,1] \mid \forall n \in \mathbb{N}^*, \frac{1}{n} \leq x \leq 1\}$.

2. Déterminer les bornes inférieure et supérieure des ensembles $A = \{\frac{3n^2+4}{n^2+1},\ n \in \mathbb{N}\}$ et $B = \{(-1)^n + \frac{1}{n}, n \in \mathbb{N}^*\}$.

3. Soit $E = \{x \in \mathbb{Q} \mid x^2 \leq 2\}$. Montrer que E est un sous-ensemble borné de $\mathbb{Q}$, mais n'admet pas de borne supérieure ou inférieure dans $\mathbb{Q}$. Est-ce que cela contredit le théorème de la borne supérieure ?

4. Soient E_1, E_2 des sous-ensembles non vides et majorés de $\mathbb{R}$. Montrer que

$$\sup(E_1 \cup E_2) = \max\{\sup E_1, \sup E_2\}. \tag{6.5}$$

Montrer que, si $E_1 \subset E_2$, alors $\sup E_1 \leq \sup E_2$.

6.6 Démonstration du théorème de la borne supérieure*

Comme promis, je vais utiliser le théorème des suites adjacentes pour arriver à mes fins. Plus précisément, je vais construire deux suites adjacentes (a_n) et (b_n) dont la limite commune sera la borne supérieure recherchée. La méthode de construction a un joli nom : “par dichotomie”, ce qui veut dire essentiellement, “en coupant (les cheveux) en deux”.

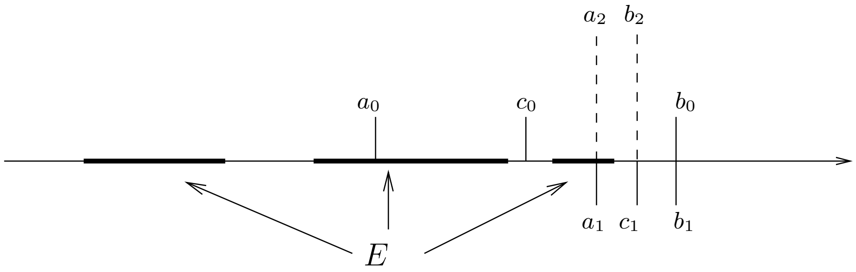

Fig. 6.3 – La construction

Allons-y. Je vous invite à suivre la construction sur la Figure 6.3. Comme E n'est pas vide, il existe a_0 appartenant à E. Comme E est majoré, il existe un majorant b_0 de E. Considérons alors $c_0 = \frac{1}{2}(a_0 + b_0)$, à mi-chemin entre a_0 et b_0. De deux choses l'une :

(i) c_0 est un majorant de E. Je pose alors $b_1 = c_0$ et $a_1 = a_0$;

(ii) c_0 n'est pas un majorant de E. Je pose alors $b_1 = b_0$ et je choisis dans E un élément $a_1 \in E$ tel que $c_0 < a_1$. (C'est ce deuxième cas qui est représenté dans la Figure 6.3.)

Dans les deux cas, j'ai maintenant deux éléments a_0, a_1 de E et deux majorants b_0, b_1 de E tels que

$$a_0 \leq a_1 \leq b_1 \leq b_0,$$

et, de plus

$$(b_1 - a_1) \leq \frac{1}{2}(b_0 - a_0).$$

Cette dernière égalité est obtenue par un simple calcul, mais il est instructif de la voir géométriquement : dans les deux cas, l'intervalle $[a_1, b_1]$ est contenu dans un des intervalles $[a_0, c_0]$ ou $[c_0, b_0]$, qui sont précisément de longueur $\frac{1}{2}(b_0 - a_0)$.

Vous vous imaginez maintenant comment continuer. On considère le point c_1 au milieu entre a_1 et b_1 et on a deux possibilités :

(i) c_1 est un majorant de E. Je pose alors $b_2 = c_1$ et $a_2 = a_1$ (C'est ce premier cas qui est représenté dans la Figure 6.3.) ;

(ii) c_1 n'est pas un majorant de E. Je pose alors $b_2 = b_1$ et je choisis dans E un élément $a_2 \in E$ tel que $c_1 < a_2$. On a

$$a_0 \leq a_1 \leq a_2 \leq b_2 \leq b_1 \leq b_0,$$

et

$$(b_2 - a_2) \leq \frac{1}{2}(b_1 - a_1) \leq \left(\frac{1}{2}\right)^2 (b_0 - a_0).$$

On construit ainsi de fil en aiguille deux suites $(a_n), (b_n)$ tels que les a_n appartiennent à E, les b_n sont des majorants de E et tels que, quelque soit $n \in \mathbb{N}$,

$$a_0 \leq a_1 \leq a_2 \leq \cdots \leq a_n \leq b_n \leq \ldots b_2 \leq b_1 \leq b_0,$$

et

$$(b_n - a_n) \leq \left(\frac{1}{2}\right)^n (b_0 - a_0).$$

Les suites $(a_n), (b_n)$ sont donc adjacentes et ont donc (Théorème des suites adjacentes !) une limite commune que j'appellerai M.

Je vais maintenant finir la démonstration en montrant que M est la borne supérieure de E. J'utilise pour cela le (iii) de la Proposition 6.17. D'abord, quelque soit $x \in E$, on a, pour tout $n \in \mathbb{N}$:

$$x \leq b_n,$$

puisque les b_n sont des majorants de E. On a donc

$$x \leq \lim_{n \to +\infty} b_n = M,$$

ce qui montre que M est un majorant de E. Par ailleurs, les a_n appartiennent à E et $M = \lim_{n \to +\infty} a_n$, donc le (iii) de la Proposition permet de conclure que $M = \sup E$. □

6.7 Démonstration du théorème des suites monotones

Montrons d'abord le (i). Premièrement, si une suite est croissante et convergente, elle est certainement bornée (Lemme 4.6) et donc majorée.

Supposons maintenant que la suite (u_n) soit majorée et croissante. L'ensemble

$$E = \{u_n \mid n \in \mathbb{N}\}$$

est alors majoré et admet donc une borne supérieure $\sup E$ grâce au Théorème 6.14. On a en particulier, quelque soit $n \in \mathbb{N}$

$$u_n \leq \sup E.$$

Je vais montrer que la suite (u_n) est alors convergente et que

$$\lim_{n\to+\infty} u_n = \sup E.$$

Soit $\epsilon > 0$. Il faut montrer qu'il existe $N \in \mathbb{N}$ tel que

$$n > N \Rightarrow |u_n - \sup E| < \epsilon.$$

Or, la Proposition 6.17 (ii) garantit qu'il existe un élément u_N de l'ensemble E ci-dessus tel que

$$\sup E - \epsilon < u_N \leq \sup E.$$

Comme la suite (u_n) est croissante, on en conclut que, quelque soit $n \geq N$, on a

$$\sup E - \epsilon < u_n \leq \sup E,$$

et donc

$$|u_n - \sup E| < \epsilon,$$

ce qui conclut la démonstration.

Pour montrer le (ii), on peut adapter l'argument ci-dessus, en argumentant que cette fois-ci l'ensemble E a une borne inférieure, ce qui constitue un bon exercice. Alternativement, on peut observer que, si la suite u_n est minorée et décroissante, alors la suite $(-u_n)$ est majorée et croissante, et appliquer la partie (i). Je vous laisse le soin de compléter ces raisonnements.

6.8 Fonctions monotones

Il y a un théorème des fonctions monotones tout à fait analogue au théorème des suites monotones. Le voici :

Théorème 6.18. *(Théorème des fonctions monotones) Soit* $f :]a, b[\to \mathbb{R}$ *une fonction monotone, avec* $a \in \mathbb{R}$ *ou* $a = -\infty$ *et* $b \in \mathbb{R}$ *ou* $b = +\infty$. *Alors* $\lim_{x\to a} f(x)$ *et* $\lim_{x\to b} f(x)$ *existent.*

(i) Si f *est croissante et majorée, on a* $\lim_{x\to b} f(x) \in \mathbb{R}$. *Si* f *est croissante, mais n'est pas majorée, on a* $\lim_{x\to b} f(x) = +\infty$.

(ii) Si f *est décroissante et minorée, alors* $\lim_{x\to b} f(x) \in \mathbb{R}$. *Si* f *est décroissante mais n'est pas minorée, on a* $\lim_{x\to b} f(x) = -\infty$.

(iii) Si f *est croissante et minorée, on a* $\lim_{x\to a} f(x) \in \mathbb{R}$. *Si* f *est croissante, mais n'est pas minorée, on a* $\lim_{x\to a} f(x) = -\infty$.

(iv) Si f *est décroissante et majorée, alors* $\lim_{x\to a} f(x) \in \mathbb{R}$. *Si* f *est décroissante mais n'est pas majorée, on a* $\lim_{x\to a} f(x) = +\infty$.

La démonstration de ce théorème se fait de façon tout à fait analogue à celle du théorème des suites monotones, et comme j'ai la flemme de la rédiger, je vous la laisse en exercice. Je vous invite par ailleurs à faire quelques dessins pour illustrer les différentes parties du théorème.

Le lecteur teste ses connaissances
Les barêmes sur 15 sont donnés à titre indicatif

Interrogation Ecrite Limites 1 – durée 1h30

I Questions de cours
(i) [1pt] Enoncer le théorème des suites adjacentes.
(ii) [3pts] Soit $f : \mathbb{R} \to \mathbb{R}$ croissante et non-majorée. Rappeler la définition de "f est non-majorée" et de "f tend vers $+\infty$ lorsque x tend vers $+\infty$". Montrer que $\lim_{x\to+\infty} f(x) = +\infty$.

II Soit, pour tout $x \in \mathbb{R}^+$, $P_n(x) = \sum_{k=1}^n \frac{x^k}{k^2}$.
(i) [2pts] Montrer que la suite $P_n(1)$ converge.
(ii) [1pt] Montrer que, si $0 < x < 1$, $P_n(x)$ converge.
(iii) [2pts] Montrer que $P_n(2)$ diverge.

III On considère les suites

$$u_0 \in \mathbb{R}^+, \qquad u_{n+1} = \frac{1+u_n^2}{2}.$$

(i) [1pt] Montrer que la suite (u_n) est croissante.
(ii) [1pt] Dans le cas où (u_n) converge, montrer que

$$\lim_{n\to+\infty} u_n = 1.$$

(iii) [2pts] On suppose que $u_0 \in [0,1]$. Montrer que (u_n) converge.
(iv) [2pts] On suppose que $u_0 > 1$. Que se passe-t-il ?

Interrogation Ecrite Limites 2 – durée 1h30

I Questions de cours
(i) [2pts] Soient $f : \mathbb{R} \to \mathbb{R}$ et $\ell \in \mathbb{R}$. Donner la définition de $\lim_{x\to\infty} f(x) = \ell$.
(ii) [1pt] Enoncer le théorème de la borne supérieure.
(iii) [3pts] Soit $f : \mathbb{R} \to \mathbb{R}$ croissante et bornée. Montrer que $\lim_{x\to\infty} f(x) = \sup f(\mathbb{R})$.

II [6pts] Soit, pour tout $x \in \mathbb{R}$, $P_n(x) = \sum_{k=1}^n \frac{x^k}{k^k}$. Etudier la convergence des suites $(P_n(x))$ en fonction de x.
Indication : Etudier séparément les cas $x > 0$ et $x < 0$. Considérer éventuellement des cas particuliers comme $x = 1$ ou $x = -1$ si vous ne voyez pas tout de suite comment attaquer le cas général.

III [3pts] Etudier la convergence de la suite $(u_n = \frac{2^{(n+1)!}}{(n!)^n})$.

Interrogation Ecrite Limites 3 – durée 1h30

I Question de cours

(i) [2pt] Donner la définition de “borne supérieure” et énoncer le théorème de la borne supérieure.

(ii) [2pt] Donner la définition de la fonction exponentielle. L’utiliser pour montrer que

$$\lim_{x\to+\infty} \frac{e^x}{x^2} = +\infty.$$

II [4pts] Etudier la convergence de la suite de terme général

$$u_n = \sum_{k=0}^{n} (-1)^k e^{-k^2}.$$

On pensera à étudier les suites de terme général $a_n = u_{2n+1}$ et $b_n = u_{2n}$.

III [2pt] Calculer la dérivée de $\cos(\exp(x^2))$, puis de $\sin(\cos(\exp(x^2)))$.

IV [3pts] On considère l’ensemble

$$E = \{x \in \mathbb{R} \mid \exists n \in \mathbb{N}^*, 1 - \frac{1}{n} < x\}.$$

Est-il minoré, majoré ? Admet-il une borne supérieure, inférieure ? Admet-il un minimum, un maximum ?

V [2pts] Etudier la dérivabilité en 0 de la fonction $f : \mathbb{R} \to \mathbb{R}$ telle que $f(x) = |x|$.

Chapitre 7

Le théorème des accroissements finis

Si vous pensez que vos profs sont difficiles,
attendez de voir votre patron.
Bill Gates

7.1 Introduction

Dans le Chapitre 6 nous avons réussi à démontrer que l'équation différentielle

$$f'(x) - f(x) = 0, \quad f(0) = 1$$

a une unique solution. A partir de là, il n'est pas difficile de montrer que, quelque soient $a, b, c, d \in \mathbb{R}$, $a \neq 0$, il existe une unique solution de l'équation différentielle

$$af'(x) + bf(x) = c, \quad f(0) = d.$$

Exercice 7.1. *Montrer ceci.*
Indication : *On peut commencer par remarquer que*

$$f(x) = (d - \frac{c}{b})e^{-\frac{b}{a}x} + \frac{c}{b}$$

est une solution du problème. Reste à établir l'unicité.

Mais le but affiché au début du Chapitre 3 est de résoudre les équations

$$a(x)f'(x) + b(x)f(x) = c(x),$$

où cette fois-ci $a(x), b(x)$ et $c(x)$ ne sont plus des constantes. Je m'attaquerai d'abord à l'équation

$$f'(x) = c(x),$$

c'est à dire à la question de savoir si une fonction c (continue) quelconque a une primitive. La réponse, affirmative, ne viendra que dans le Chapitre 11. Dans le présent chapitre, je vous présente d'abord un dernier outil mathématique indispensable, le théorème des accroissements finis – TAF pour les amis – que voici :

Théorème 7.2. *(Théorème des accroissements finis)*
Soit $f : [a, b] \to \mathbb{R}$ $(-\infty < a < b < +\infty)$ *une fonction continue sur* $[a, b]$ *et dérivable sur* $]a, b[$. *Alors il existe* $c \in]a, b[$ *tel que*

$$\frac{f(b) - f(a)}{b - a} = f'(c). \tag{7.1}$$

Plusieurs remarques s'imposent. D'abord, ce théorème a une interprétation géométrique évidente que l'on peut admirer dans la figure 7.1

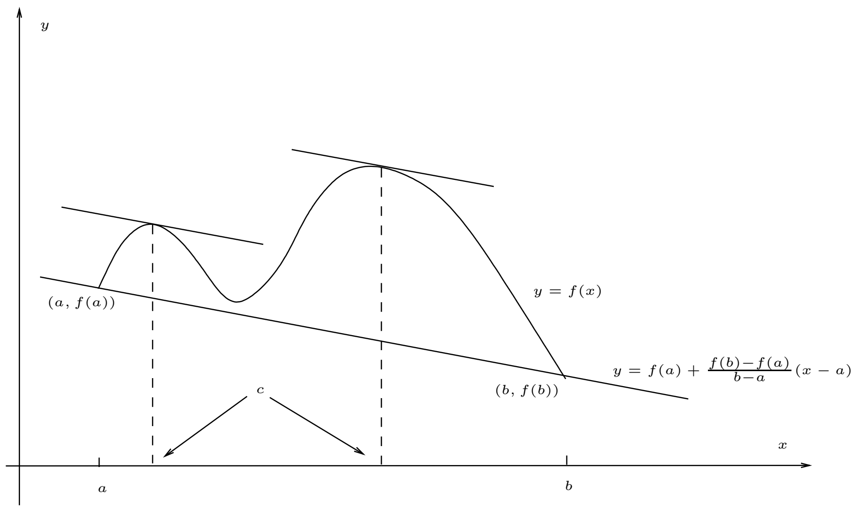

Fig. 7.1 – Le TAF en images. Y a-t-il un autre point c où (7.1) est satisfaite ?

Comme $\frac{f(b)-f(a)}{b-a}$ est la pente de la droite D passant par les points $(a, f(a))$ et $(b, f(b))$, le TAF dit en effet qu'il existe (au moins) un c entre a et b tel que la droite tangente au graphe $y = f(x)$ au point $(c, f(c))$ est parallèle à D. Je vous invite à tracer plusieurs graphes de fonctions satisfaisant aux hypothèses du théorème et de vérifier à chaque fois graphiquement qu'une telle valeur c existe en effet. Le plus souvent, plusieurs tels points existent : dans la figure 7.1, il y en a 3, même si je n'en ai indiqué que deux.

La deuxième remarque que je veux faire est que le TAF est un résultat extrêmement puissant : pour vous en convaincre, et avant même de le démontrer, j'en donnerai quelques premières applications dans la section suivante. Nous l'utiliserons encore plusieurs fois par la suite.

Dans les applications, deux variantes du TAF sont souvent utiles. Les voici.

D'abord, il faut remarquer qu'on peut appliquer le TAF à un sous-intervalle de l'intervalle de définition de f de la façon suivante :

Soit $f : [a, b] \to \mathbb{R}$ $(-\infty < a < b < +\infty)$ une fonction continue sur $[a, b]$ et dérivable sur $]a, b[$. Soient $x, x' \in [a, b], x < x'$. Alors il existe $c \in]x, x'[$ tel que

$$\frac{f(x') - f(x)}{x' - x} = f'(c). \tag{7.2}$$

Il est en effet clair que si f satisfait les hypothèses du TAF sur $[a, b]$, elle les satisfait aussi sur tout sous-intervalle $[x, x']$ de $[a, b]$. Attention ! Le c dont il est question ici dépend de x et de x' (Voir l'exercice 4 après la Section 7.3).

Exercice 7.3. *Dessiner sur la figure 7.1 quelques couples de points x, x' et identifier à chaque fois une valeur de c correspondante.*

L'autre variante du TAF qu'il faut maîtriser est :

Théorème 7.4. *(Inégalité des accroissements finis)*
Soit $f : [a, b] \to \mathbb{R}$ $(-\infty < a < b < +\infty)$ une fonction continue sur $[a, b]$ et dérivable sur $]a, b[$. Supposons que

$$\sup_{x \in]a,b[} |f'(x)| = M < +\infty.$$

Alors, quelques soient $x, x' \in [a, b]$, on a

$$|f(x') - f(x)| \leq M|x' - x|. \tag{7.3}$$

Ce résultat aussi est un corollaire immédiat du TAF et je vous invite à le démontrer.

A partir de dessins comme celui de la figure 7.1 on se convainc facilement que le TAF *doit* être vrai. Le démontrer ne sera pourtant pas facile, je m'y attaquerai dans les Sections 7.3 et 7.4. Je démontrerai le TAF comme corollaire du théorème de Rolle, souvent utile lui-même et dont il est une simple généralisation.

Théorème 7.5. *(Théorème de Rolle)*
Soit $f : [a, b] \to \mathbb{R}(-\infty < a < b < +\infty)$ une fonction continue sur $[a, b]$ et dérivable sur $]a, b[$ telle que $f(a) = f(b)$. Alors il existe $c \in]a, b[$ tel que

$$f'(c) = 0. \tag{7.4}$$

La figure qui vient avec le théorème de Rolle (Fig. 7.2) montre très clairement en quel sens le TAF en est une généralisation. Pour compléter la chaîne logique, le théorème de Rolle est un corollaire du théorème suivant qui est lui-même très important en soi :

Théorème 7.6. *(Théorème du maximum)*
Soit $f : [a, b] \to \mathbb{R}$ $(-\infty < a < b < +\infty)$ une fonction continue. Alors

(i) f est bornée ;

(ii) f atteint un maximum global et un minimum global sur $[a, b]$.

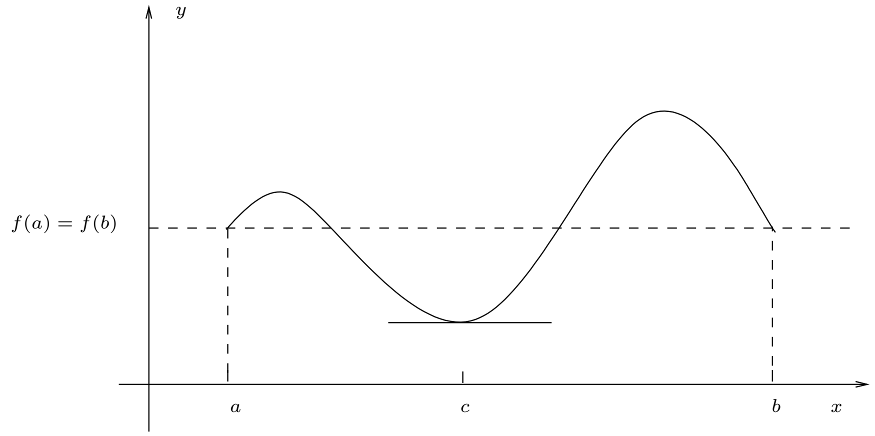

FIG. 7.2 – Le théorème de Rolle en images. Y a-t-il un autre point c où (7.1) est satisfaite ?

Ce résultat dit que si on trace un graphe quelconque entre $(a, f(a))$ et $(b, f(b)$, *sans lever le crayon*, alors on passe par un minimum et un maximum. J'expliquerai sa signification plus en détail dans la Section 7.4. Bien qu'il vous paraît sans doute évident, vous constaterez que sa démonstration (Section 7.4) est difficile. Par contre, une fois le théorème du maximum établi, le théorème de Rolle et le TAF se démontrent facilement (Section 7.3).

Indépendamment des difficultés des démonstrations, ce qu'il faut surtout retenir est que vous voyez réunis dans cette introduction trois théorèmes très importants d'analyse, avec lesquels il conviendra de vous familiariser à fond.

7.2 Monotonie et signe de la dérivée

Comme promis, voici d'abord quelques conséquences relativement immédiates mais importantes du TAF. Le résultat suivant vous est familier :

Théorème 7.7. *Soit* $f : [a, b] \to \mathbb{R}$ $(-\infty < a < b < +\infty)$ *une fonction continue sur* $[a, b]$ *et dérivable sur* $]a, b[$.

(i) Si $f'(x) \geq 0$ *(respectivement* $f'(x) > 0$*) pour tout* $x \in]a, b[$*, alors* f *est croissante (respectivement strictement croissante) sur* $[a, b]$ *;*

(ii) Si $f'(x) \leq 0$ *(respectivement* $f'(x) < 0$*) pour tout* $x \in]a, b[$*, alors* f *est décroissante (respectivement strictement décroissante) sur* $[a, b]$.

Ce résultat vous est bien évidemment connu depuis le lycée et vous l'avez utilisé *ad nauseam* dans les innombrables "tableaux de variation" que vous avez construits en préparation du bac. Qui plus est, on a bien l'impression, en regardant quelques graphes et en se souvenant de l'interprétation géométrique de la dérivée, qu'il est évident et devrait donc être facile à démontrer. Eh bien non ! Je

vous invite à essayer de trouver un argument simple de ce résultat, sans utiliser le TAF : ce ne sera pas facile.... Par contre, une fois qu'on dispose du TAF, la démonstration est en effet simple.
Démonstration : Il est commode d'utiliser la variante du TAF ci-dessus. Soit $x, y \in [a, b]$, avec $x < y$. Il existe alors $c \in]x, y[$ tel que

$$f(y) - f(x) = f'(c)(y - x).$$

Si $f'(c) \geq 0$, on en conclut que $f(y) \geq f(x)$ et si $f'(c) \leq 0$, on a $f(y) \leq f(x)$.

Théorème 7.8. *Soit $f : [a, b] \to \mathbb{R}$ $(-\infty < a < b < +\infty)$ une fonction continue sur $[a, b]$ et dérivable sur $]a, b[$. Si $f'(x) = 0$ pour tout $x \in]a, b[$, f est une constante.*

Les mêmes remarques que ci-dessus s'appliquent.
Démonstration : Soit $x \in]a, b]$. On sait grâce au Théorème 7.2 qu'il existe $c \in]a, x[$ tel que

$$f(x) - f(a) = f'(c)(x - a) = 0.$$

Donc $f(x) = f(a)$ pour tout $x \in]a, b]$ ce qui montre bien que la fonction est constante.

Attention ! Piège à éviter : Une fonction $f : D \to \mathbb{R}$ peut être dérivable sur D, de dérivée nulle partout, mais pas constante ! Par exemple, si $D = \mathbb{R}^*$, et $f(x) = x/|x|$, c'est le cas ! La raison est que le domaine D n'est pas un intervalle, mais l'union de deux intervalles disjoints. La fonction f est bien constante sur chacun de ces intervalles, mais la valeur de cette constante est différente sur les deux intervalles.

7.3 Démonstration du théorème de Rolle et du TAF

7.3.1 Les hypothèses du TAF

L'hypothèse "dérivable sur $]a, b[$ et continue sur $[a, b]$" peut paraître un peu bizarre. D'abord, si la fonction est dérivable sur $]a, b[$, elle y est automatiquement continue. L'hypothèse supplémentaire ne joue donc qu'aux extrémités de l'intervalle. Deuxièmement, la plupart des fonctions que vous manipulez sont tout simplement dérivables sur $[a, b]$ (fermée !) et donc automatiquement continues sur $[a, b]$. Néanmoins, des exceptions existent, et ne sont pas si exotiques que ça :

Exercice 7.9. *Montrer que la fonction $f(x) = \sqrt{1 - x^2}$ satisfait aux hypothèses du TAF sur $[-1, 1]$, et n'est pas dérivable en -1 et 1. Peut-on voir cela sur le graphe ? Montrer qu'elle ne satisfait pas aux hypothèses du Théorème 7.4.*

Dans de nombreuses applications, les fonctions $f : [a, b] \to \mathbb{R}$ que nous rencontrerons seront dérivables sur $[a, b]$ et leur dérivée sera continue sur $[a, b]$.

Dans ce cas, les hypothèses du Théorème 7.4 sont satisfaites grâce au théorème du maximum, qui garantit que f' atteint un maximum global sur $[a, b]$. On appelle de telles fonctions continûment dérivables.

Définition 7.10. *Soit $f : D \to \mathbb{R}$. On dit que f est continûment dérivable si et seulement si f est dérivable sur D et f' est continue sur D. L'ensemble des fonctions continûment dérivables sur D est désigné par $C^1(D)$.*

Il est légitime de se demander si une fonction $f : [a, b] \to \mathbb{R}$ qui est dérivable sur tout l'intervalle $[a, b]$ (extrémités comprises) n'a pas automatiquement une dérivée continue ? Si vous tracez quelques graphes, vous verrez que le contraire est un peu difficile à imaginer. Ça existe pourtant :

Exercice 7.11. *Montrer que la fonction $f : [-1, 1] \to \mathbb{R}$ définie par $f(x) = x^2 \sin \frac{1}{x}$ lorsque $x \neq 0$ et $f(0) = 0$ est dérivable, mais que f' n'est pas continue en 0.* **Indication :** *Consulter l'exercice 2 de la Section 5.3.*

7.3.2 Extrema

Rappelons d'abord quelques définitions :

Définition 7.12. *Soit $f : D \subset \mathbb{R} \to \mathbb{R}$.*

(i) On dit que f atteint un maximum (respectivement minimum) en un point $x_* \in D$ si et seulement si il existe un intervalle $I \subset D$ contenant x_* tel que, quelque soit $x \in I$, $f(x) \leq f(x_*)$ (respectivement $f(x) \geq f(x_*)$).

(ii) On dit que f atteint un maximum global (respectivement minimum global) en un point $x_* \in D$ si et seulement si, quelque soit $x \in D$, $f(x) \leq f(x_*)$ (respectivement $f(x) \geq f(x_*)$).

Développons encore un peu notre vocabulaire. On dit que f atteint un extremum (global) si elle atteint un minimum ou un maximum (global). Dire que f atteint un minimum ou un maximum global est de toute évidence équivalent à dire que l'image $f(D)$ de f a, en tant que sous-ensemble de $\mathbb{R}$, un minimum ou un maximum (Voir Section 6.5). On écrit donc indifféremment

$$\min f = \min f(D) = \min_{x \in D} f(x),$$

et

$$\max f = \max f(D) = \max_{x \in D} f(x).$$

On se rappellera aussi qu'une fonction est majorée si et seulement si $f(D)$ l'est, au quel cas $\sup f(D)$ existe (Théorème de la borne supérieure). On écrit souvent

$$\sup f(D) = \sup_{x \in D} f(x).$$

Un même discours est valable pour les fonctions minorées et on écrit

$$\inf f(D) = \inf_{x \in D} f(x).$$

Dans le cas de (i) de la définition ci-dessus, on parle parfois d'extremum local, pour insister sur la différence avec le (ii). Par abus de langage, on dit souvent que "x_* est un extremum de f" plutôt que "f atteint un extremum en x_*". En particulier, lorsqu'on cherche les extrema d'une fonction, on s'intéresse le plus souvent autant à savoir en quels points x_* ces extrema sont atteints, qu'aux valeurs $f(x_*)$ de ces extrema elles-mêmes. On dira par exemple que les maxima de la fonction cos sont $2\pi n,\ n \in \mathbb{Z}$, plutôt que de dire que le maximum global de la fonction cos est 1, et que ce maximum global est atteint en $2\pi n,\ n \in \mathbb{Z}$. Je ne me priverai pas de ces glissements de langage...

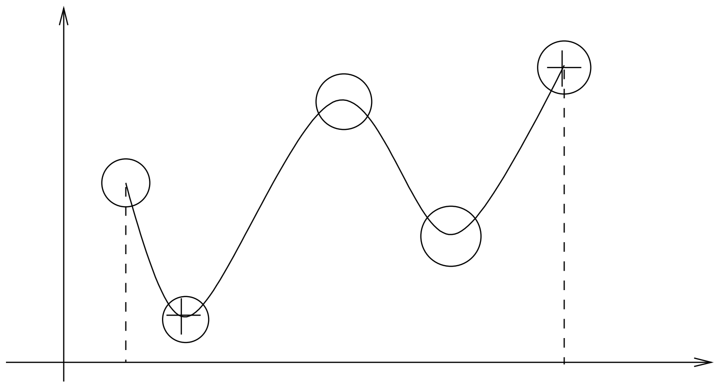

FIG. 7.3 – Les extremas sont encerclés, les extremas globaux indiqués par une croix.

Exercice 7.13. *(i) Montrer que la fonction $f(x) = |x-1||x-2|$, définie sur $D = [0, +\infty[$ a des extrema locaux en $0, 1, 3/2$, et 2. S'agit-il d'extrema locaux ou globaux, de minima ou de maxima ?*

(ii) Cherchez dans le [LM] la définition de maximum/minimum local et comparez à la définition ci-dessus. En quoi est-elle différente ? Consultez d'autres livres de DEUG sur ce point. Laquelle des définitions utilisées vous préférez ? Interrogez vos profs de mathématiques. Qu'en pensent-ils ? Est-il préjudiciable que différents livres de mathématiques utilisent les mêmes mots pour désigner des notions différentes ? Cela arrive-t-il souvent ?

Un résultat simple mais crucial pour la démonstration du TAF et souvent très utile par ailleurs est le suivant :

Théorème 7.14. *Soit $f :]a, b[\to \mathbb{R}$ $(-\infty \leq a < b \leq +\infty)$ une fonction dérivable. Supposons que f atteint un extremum en $c \in]a, b[$. Alors $f'(c) = 0$.*

Attention ! Piège à éviter : Si $f : [a, b] \to \mathbb{R}$ $(-\infty < a < b < +\infty)$ est une fonction dérivable qui atteint un extremum en a, alors rien ne garantit que $f'(a) = 0$. Par exemple, considérons $f(x) = x$ sur $[0, 1]$. Elle atteint son maximum global en 1 et son minimum global en 0, mais de toute évidence $f'(0) = 1 = f'(1)$ (Voir aussi la figure 7.3).

Attention ! Deuxième piège à éviter : Ce n'est pas parce que la dérivée s'annule que la fonction atteint un extremum. L'exemple type est la fonction $f(x) = x^3$ pour laquelle $f'(0) = 0$ sans qu'elle atteint un extremum en $x = 0$.

7.3.3 Les démonstrations

Démonstration du Théorème de Rolle : Tout d'abord, si $f(x) = f(a)$ pour tout $a \in [a, b]$, le résultat est vrai. Plaçons-nous donc dans le cas où il existe $x \in]a, b[$ tel que $f(x) \neq f(a)$. On a alors $f(x) > f(a)$ ou $f(x) < f(a)$. Supposons que le premier cas se présente. Alors le maximum global M de f, qui existe grâce au théorème du maximum, est strictement plus grand que $f(a)$ et est donc atteint en un point c de l'intervalle ouvert $]a, b[$. Le Théorème 7.14 permet de conclure que $f'(c) = 0$. Si maintenant il existe $x \in]a, b[$ tel que $f(x) < f(a)$, le même raisonnement s'applique avec le minimum de f sur $[a, b]$.
Démonstration du TAF : Introduisons la fonction

$$h(x) = f(x) - \left[f(a) + \frac{f(b) - f(a)}{b - a}(x - a)\right]$$

qui représente la hauteur entre le point $(x, f(x))$ du graphe de f et la droite passant par $(a, f(a))$ et $(b, f(b))$ (Fig. 7.1). De toute évidence, h est une fonction continue sur $[a, b]$ et dérivable sur $]a, b[$ et $h(a) = h(b) = 0$. Le théorème de Rolle garantit donc l'existence d'un $c \in]a, b[$ tel que $h'(c) = 0$. Mais, comme

$$h'(x) = f'(x) - \frac{f(b) - f(a)}{b - a},$$

on obtient

$$0 = f'(c) - \frac{f(b) - f(a)}{b - a},$$

ce qui est le résultat recherché !

Le lecteur s'entraîne

1. Soit f une fonction dérivable sur $\mathbb{R}$, telle que f' est une fonction continue et telle que $f'(x) \neq 1$ pour tout x réel.
Montrer alors que l'équation

$$f(x) = f(0) + x$$

n'admet pas d'autre racine que $x = 0$ (On pourra considérer la fonction $g(x) = f(x) - x$).

2. a) Soit f deux fois continûment dérivable sur $[a, b]$ et s'annulant en trois points distincts sur $[a, b]$. Montrer qu'il existe $c \in]a, b[$ tel que $f^{(2)}(c) = 0$.
b) Soit $g(x) = x^2(x - 1)^2(x + 113)^{152}$. Montrer qu'il existe $c \in]0, 1[$ tel que $g^{(3)}(c) = 0$.

3. Soit f une fonction dérivable sur $\mathbb{R}$, telle que $f(0) = 1$ et pour tout $x \in \mathbb{R}$, $|f'(x)| < 2$. Montrer que l'on a

$$\forall x \geq 0, \;\; 1 - 2x \leq f(x) \leq 1 + 2x.$$

4. Soit $P(x) = \alpha x^2 + \beta x + \gamma$. Quelle est la valeur de c dans la formule des accroissements finis :

$$P(x) - P(y) = P'(c)(x - y).$$

Dépend-elle de x et de y ?

5. Soit f la fonction définie sur $[0, \pi/2]$ par $f(x) = 1 + \frac{1}{3} \sin x$. On considère la suite (u_n) définie par $u_{n+1} = f(u_n)$ et $u_0 \in [0, \pi/2]$.
a) Montrer que léquation $f(x) = x$ admet une unique racine sur $[0, \pi/2]$, que l'on notera α.
b) Montrer que $\forall\, n \geq 0$, $u_n \in [0, \pi/2]$.
c) Montrer que $\forall\, x \in [0, \pi/2]$, $|f'(x)| \leq 1/3$.
d) En utilisant le théorème des accroissements finis, montrer que $\forall\, n \geq 0$,

$$|u_{n+1} - \alpha| \leq \frac{1}{3}|u_n - \alpha|.$$

d) En déduire que la suite (u_n) converge vers α, et fournir une valeur approchée de cette racine à 10^{-2} près.

6. On note α_n l'unique racine positive du polynôme $P_n(x) = x^n + 2x^2 + x - 1$.
a) Montrer que la suite (α_n) est bien définie, et que l'on a $\alpha_n \in [0, \frac{1}{2}]$ pour tout $n \geq 3$.
b) Montrer que la suite (α_n) est croissante, puis convergente.
c) Déterminer la limite de (α_n).

7.4 Démonstration du théorème du maximum

Commençons par analyser un peu le théorème en question (Théorème 7.6). Etudions en particulier la possibilité d'affaiblir ses hypothèses sans affecter le résultat. Par exemple, que se passe-t-il lorsque la fonction est continue mais l'intervalle de définition n'est pas fermé ? Ou lorsque f est définie sur un intervalle $[a, b]$ fermé, mais n'est pas continue ? Les réponses se trouvent dans l'exercice suivant.

Exercice 7.15. *(i) Trouver une fonction sur $[0, 1]$ qui n'est pas bornée.*

(ii) Trouver une fonction continue sur $[0, 1[$ qui n'est pas minorée/majorée.

(iii) Trouver une fonction bornée sur $[0, 1]$ qui n'a pas de maximum ni de minimum global.

(iv) Trouver une fonction continue et bornée sur $\mathbb{R}$ qui n'atteint ni maximum, ni minimum global.

Solution : Regarder la figure 7.4 et réfléchir un peu.

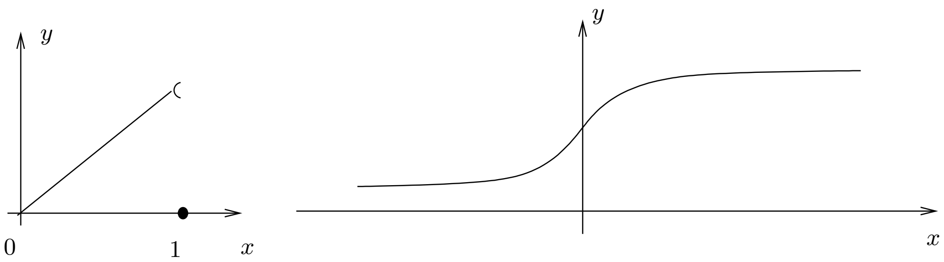

FIG. 7.4 – Autour du théorème du maximum

Tournons-nous maintenant vers la démonstration du théorème du maximum, qui n'est vraiment pas facile, même si elle ne fait appel à aucune technique que je n'ai pas déjà utilisée. Pour préparer le terrain, je démontre le petit lemme technique suivant :

Lemme 7.16. *Soit $f : [a, b] \to \mathbb{R}$ une fonction. Soit*

$$E = \{x \in [a, b] | \exists M \in \mathbb{R}, \forall x' \in \mathbb{R}, (a \leq x' \leq x \Rightarrow |f(x')| \leq M)\}.$$

On a (i) E est borné et non-vide et $E = [a, \sup E[$ ou $E = [a, \sup E]$.
(ii) Si, de plus, f est continue, $E = [a, \sup E]$.

Je vous fais remarquer que la première partie du lemme n'impose aucune condition sur la fonction f ! La définition de l'ensemble E vous paraît sans doute un peu compliquée. Si vous décodez correctement les $\forall, \exists$, vous constaterez que l'ensemble E n'est rien que l'ensemble des x appartenant à $[a, b]$ tels que f est bornée sur $[a, x]$. Pour mieux comprendre, considérons un exemple.

Exercice 7.17. *(i) Considérer la fonction $f : [-1, 1] \to \mathbb{R}$ définie par $f(x) = 1/x$ lorsque $x \neq 0$ et $f(0) = 0$. Identifier E.*
(ii) Considérer la même fonction que ci-dessus, mais définie exclusivement sur $[0, 1]$.
Je vous invite à tracer le graphe de ces fonctions, afin de mieux voir ce qu'il se passe. Remarquez en particulier que f n'est pas une fonction continue.

Solution : (i) Ici $E = [-1, 0[$ parce que f est bornée sur chaque intervalle $[-1, -\epsilon]$ $(0 < \epsilon < 1)$, mais pas sur $[-1, 0]$. En effet,

$$\max_{x \in [-1, -\epsilon]} |f(x)| = \max_{x \in [-1, -\epsilon]} |1/x| = \frac{1}{\epsilon} < +\infty,$$

mais bien évidemment f n'est pas bornée sur $[-1, 0]$ et donc $0 \notin E$.
(ii) Ici $E = \{0\} = [0, 0]$ parce que f n'est pas bornée sur $[0, \epsilon]$, quelque soit $\epsilon > 0$.
Nous voilà prêts pour attaquer la démonstration du lemme.

Démonstration* : (i) On remarque d'abord que la définition même de E implique immédiatement que, si $x_1 \in E$, et si $a \leq x_2 \leq x_1$, alors $x_2 \in E$. Par ailleurs, comme E est borné ($E \subset [a,b]$!) et comme E n'est pas vide ($a \in E$!), on sait, par le théorème de la borne supérieure que E a une borne supérieure $\sup E \in [a,b]$. On en conclut que, quelque soit $x_2 < \sup E$, $x_2 \in E$. En effet, on sait, par la caractérisation de la borne supérieure, qu'il existe $x_1 \in E$, $x_2 \leq x_1 \leq \sup E$ et donc, par la remarque ci-dessus, que $x_2 \in E$. On a donc montré que $[a, \sup E[\subset E$. Comme, par ailleurs, $E \subset [a, \sup E]$, la première partie du lemme est démontrée.

(ii) Si $\sup E = a$, le résultat est vrai. Supposons donc que $a < \sup E \leq b$ et posons $c = \sup E$. Comme f est continue, f a comme limite $f(c)$ en c. Le Lemme 4.6 implique alors qu'il existe $\delta > 0$ tel que, quelque soit $x \in [c-\delta, c+\delta] \cap [a,b]$, $f(x) \leq |f(c)| + 1$. En prenant δ assez petit pour que $a \leq c - \delta < c$, on peut conclure que f est bornée sur $[c-\delta, c] \subset [a,b]$. Comme par ailleurs la partie (i) implique que $c - \delta \in E$ (puisque $c = \sup E$!), on a que f est bornée sur $[a, c-\delta]$ et donc f est bornée sur $[a,c] = [a, c-\delta] \cup [c-\delta, c]$ (Ici, j'ai utilisé (6.5)) . Ceci montre que $c \in E$: ouf ! □

Ça vous a peut-être semblé un peu douloureux, mais c'est comme chez le dentiste : c'est presque fini. En effet, avec le lemme en poche, la démonstration du théorème n'est plus très difficile :

Démonstration : (i) Etant donné le lemme, il suffit de montrer que $\sup E = b$. Je vais procéder par l'absurde. Supposons donc que $\sup E = c < b$. Comme f est continue en c, le Lemme 4.6 implique qu'il existe $\delta > 0$ tel que $|f(x)| \leq |f(c)| + 1$ pour tout $x \in [a,b] \cap [c-\delta, c+\delta]$. Comme c est strictement inférieur à b, nous pouvons alors choisir δ assez petit pour que $[c, c+\delta] \subset [a,b]$, et nous avons alors f bornée sur $[c, c+\delta]$. Par ailleurs, comme $c \in E$, on a f bornée sur $[a,c]$. Par conséquent, f est bornée sur $[a, c+\delta]$, ce qui montre que $c + \delta \in E$. Comme $c = \sup E$, ceci est une contradiction et on conclut que $\sup E = b$.

(ii) Posons maintenant

$$M = \sup f([a,b]) = \sup_{x \in [a,b]} f(x).$$

La partie (i) nous garantit l'existence de $M \in \mathbb{R}$. Il reste à montrer que M est bien le maximum de la fonction f, c'est à dire qu'il existe $x_* \in [a,b]$ tel que $f(x_*) = M$. Mais où trouver x_* ? Il nous faut un algorithme permettant de construire un tel x_*, étant donné une quelconque fonction f continue sur $[a,b]$. Je vais encore une fois me servir d'une démonstration par dichotomie pour construire deux suites adjacentes $(a_n), (b_n)$ dont la limite commune sera le x_* recherché : ce ne sera pas tout à fait simple. Vous avez intérêt de suivre la construction sur la figure 7.5.

Posons, pour démarrer, $a_0 = a, b_0 = b$ et $c_0 = (a_0 + b_0)/2$ et remarquons que (Voir 6.5 !)

$$M = \sup f([a,b]) = \max \{\sup f([a_0, c_0]), \sup f([c_0, b_0])\},$$

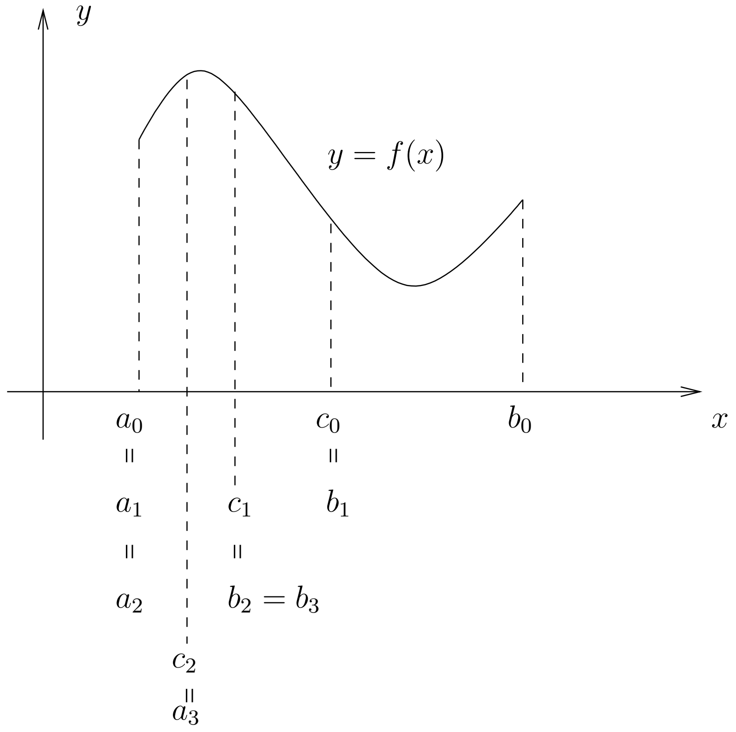

Fig. 7.5 – Encore une dichotomie

donc

$$M = \sup f([a_0, c_0]) \quad \text{ou} \quad M = \sup f([c_0, b_0]).$$

On a donc de deux choses l'une :

(i) Si $M = \sup f([a_0, c_0])$, on pose $a_1 = a_0$ et $b_1 = c_0$;

(ii) Si non, on a $M = \sup f([c_0, b_0])$ et on pose $a_1 = c_0$ et $b_1 = b_0$.

Dans les deux cas on a

$$a_0 \leq a_1 \leq b_1 \leq b_0 \text{ et } (b_1 - a_1) = \frac{1}{2}(b_0 - a_0),$$

et, de façon tout à fait cruciale,

$$M = \sup\{f(x) | x \in [a_1, b_1]\}.$$

On recommence alors la procédure en introduisant $c_1 = \frac{1}{2}(a_1 + b_1)$. On a de nouveau deux cas de figure :

(i) Si $M = \sup f([a_1, c_1])$, on pose $a_2 = a_1$ et $b_2 = c_1$;

(ii) Si non, on a $M = \sup f([c_1, b_1])$ et on pose $a_2 = c_1$ et $b_2 = b_1$.

Dans les deux cas on a

$$a_0 \leq a_1 \leq a_2 \leq b_2 \leq b_1 \leq b_0 \text{ et } (b_2 - a_2) = \frac{1}{2^2}(b_0 - a_0),$$

et, de façon tout à fait cruciale,

$$M = \sup\{f(x)|x \in [a_2, b_2]\}.$$

On construit ainsi par récurrence (Faites-le !) deux suites adjacentes (a_n) et (b_n) telles que, quelque soit $n \in \mathbb{N}$, on ait

$$M = \sup\{f(x)|x \in [a_n, b_n]\}, \quad (b_n - a_n) = \frac{1}{2^n}(b_0 - a_0).$$

Soit alors x_* la limite commune de (a_n) et de (b_n) :

$$\lim_{n\to+\infty} a_n = x_* = \lim_{n\to+\infty} b_n \text{ et } a_n \leq x_* \leq b_n.$$

Il nous reste à montrer que $M = f(x_*)$. Pour cela, je montrerai que, quelque soit $\epsilon > 0$, on a

$$M - \epsilon \leq f(x_*) \leq M,$$

ce qui implique en effet le résultat ! C'est une façon bien étonnante pour montrer que deux nombres sont égaux, mais ça marche très bien, vous allez voir (Comparez ceci avec l'Exercice 4.2 (ii) du Chapitre 4). Puisque $M = \sup\{f(x)|x \in [a_n, b_n]\}$, la caractérisation de la borne supérieure garantit l'existence de $x_n \in [a_n, b_n]$ tel que

$$M - \epsilon \leq f(x_n) \leq M.$$

Comme, de toute évidence (Gendarmes !) (x_n) converge vers x_*, la continuité de f garantit que $(f(x_n))$ converge vers $f(x_*)$ (Théorème 4.26) et on obtient, en prenant la limite de n vers $+\infty$ dans l'inégalité précédente

$$M - \epsilon \leq f(x_*) \leq M.$$

Comme vous avez pu constater, c'était bien comme chez le dentiste : ce n'était pas fini du tout, mais maintenant ça l'est.

Exercice 7.18. *Où dans la démonstration avons-nous utilisé que l'intervalle de définition de la fonction était fermé ?*

Le lecteur teste ses connaissances

Les barêmes sur 15 sont donnés à titre indicatif

Interrogation Ecrite TAF – durée 1h30

I Question de cours :

(i) [2pt] Enoncer le théorème des accroissements finis.

(ii) [3pt] Montrer que, si $f : [a, b] \to \mathbb{R}$ est continue sur [a,b] et dérivable sur $]a, b[$, et si $f'(x) > 0$ pour tout $x \in]a, b[$, alors $f(b) > f(a)$.

II [3pt] Les affirmations suivantes sont-elles vraies ou fausses ?

(i) Toute fonction $f : \mathbb{R} \to \mathbb{R}$ croissante et non-bornée est surjective.

(ii) Si $f, g : \mathbb{R} \to \mathbb{R}$ sont décroissantes, alors fg est monotone.

(iii) Si $f : D \to \mathbb{R}$ est dérivable et si f atteint un maximum en un point x_* de D, alors $f'(x_*) = 0$.

III [3pt] Montrer que la fonction $f : \mathbb{R} \to \mathbb{R}$, définie par $f(x) = x^{68^{69}} + 7^7 x - 10^{10}$ a exactement deux zéros.

IV [1pt] Montrer que, quelque soit $x \geq 0$, $\sin x \leq x$.

V [3pt] Soit $f : [0, 2] \to \mathbb{R}$ la fonction définie par $f(1) = 0$,

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

Calculer la dérivée de f en 1, si elle existe.

Chapitre 8

Les fonctions réciproques

Soit dit en passant, c'est une chose assez hideuse que le succès.
Sa fausse ressemblance avec le mérite trompe les hommes.
V.Hugo – Les Misérables.

8.1 Introduction

Il y a beaucoup de problèmes dans les mathématiques et dans ses applications qui peuvent être réduits en dernière analyse à la question de trouver toutes les solutions de l'équation

$$f(x) = d. \tag{8.1}$$

Ici $f : D \to \mathbb{R}$ est une fonction et $d \in \mathbb{R}$. L'exemple qui vous est le plus familier est celui de la recherche des racines d'un polynôme de degré 2 :

$$ax^2 + bx + c = 0,$$

que vous avez rencontré dans plusieurs problèmes de physique, par exemple.

Je vous ai donné un autre exemple dans le Chapitre 3, où il s'agissait de trouver l'instant T où votre dette serait amortie. Admettons que vous souhaitez acheter une mobilette pour faciliter vos déplacements à l'université et ainsi libérer plus de temps pour l'étude des mathématiques. Vous disposez de revenus de babysitting et d'autres menus travaux qui vous permettent de rembourser $2000FF$ par an. Vous souhaitez savoir pendant combien de temps vous devrez payer de mensualités, sachant que vous empruntez un capital initial C_0 (dont le montant déterminera la qualité de la mobilette) et sachant que le banquier vous charge un taux d'intérêt I de 7%. Comme nous l'avons vu au Chapitre 3, ce temps T est la solution de l'équation $C(T) = 0$ qui peut être réécrite de la façon suivante :

$$\frac{2000}{0,07}(1 - \exp -(0,07)T) = C_0 \tag{8.2}$$

où T est l'inconnue et qui est en effet du type (8.1). Une telle solution existe-t-elle ? Pas pour n'importe quelle valeur de C_0, bien évidemment. En effet, si vous souhaitez emprunter $40.000FF$, par exemple, le banquier ne sera pas d'accord : dans ce cas l'intérêt sur votre dette est plus élevé que vos remboursements annuels ! Pas besoin de connaître beaucoup de mathématiques pour comprendre cela. Quelle est la somme maximale que vous pouvez espérer emprunter ? Pour le comprendre, on peut remarquer que (8.2) répond à une autre question également : "Etant donné que je souhaite rembourser pendant un temps T, quel est le capital que je peux emprunter ?" Dans cette façon de voir, c'est T qui joue le rôle de la variable indépendante et C_0 celui de l'inconnue ! Bien sûr, ce capital est une fonction croissante de T, comme on peut confirmer en calculant la dérivée par rapport à T du membre de gauche de (8.2). Elle tend vers $\frac{2000}{0{,}07}$ lorsque T tend vers $+\infty$ (Tracer son graphe !) et vous ne pouvez donc certainement pas emprunter plus que $\frac{2000}{0{,}07} = 28.571$FF. Je ne pense tout de même pas que le banquier vous les donnera.

Exercice 8.1. *Pourquoi ?*

En tout cas, il est maintenant clair que, si j'emprunte une somme initiale C_0 strictement inférieure à 28.571, il existe une solution T à (8.2) et qu'elle est unique (Regardez votre graphe !). Dans cet exemple très simple, les mathématiques de lycée vous permettent bien évidemment d'exprimer explicitement ce temps nécessaire au remboursement en fonction de C_0. On trouve après un petit calcul à partir de (8.2) :

$$T = \frac{1}{0,07}|\ln(1 - \frac{0,07}{2000}C_0)|. \tag{8.3}$$

Par exemple, pour $C_0 = 10.000$FF, on trouve $T = 6,15$, c'est à dire 6 ans et deux mois et pour $C_0 = 20.000$ $T = 17,14$, c'est à dire 17 ans et 2 mois. On peut donc dire que le temps T pendant lequel vous devrez rembourser dépend (est fonction) du capital initial C_0 emprunté, ce qui est tout à fait logique. Mais on peut tout aussi bien dire de façon *réciproque* que le capital initial C_0 que vous *pouvez* emprunter dépend (est fonction) du temps T pendant lequel vous *souhaitez* payer des remboursements, comme dans l'équation (8.2). Les deux variables C_0 et T se déterminent donc mutuellement l'une l'autre de façon unique. Cet exemple simple illustre la base de la notion de "fonction réciproque" qui est le sujet de ce chapitre. Dans ce cas très simple il était facile d'exprimer la variable T en fonction de la variable C_0 (voir (8.3)), une fois qu'on connaissait la variable C_0 en fonction de la variable T (comme dans (8.2)). En général, les choses ne sont pas si simples.

Considérons en effet une situation un peu plus complexe. Vous disposez de très peu de revenus en tant qu'étudiant et vous essayez de convaincre le banquier de vous permettre de rembourser très peu d'argent pendant vos années d'études, et plus après, lorsque vous travaillerez. Ce n'est pas complètement fou, de tels prêts existent ! Pour modéliser la chose, posons $R(t) = 500t$ dans l'équation différentielle

$$C'(t) - IC(t) = -R(t)$$

qui gouverne l'évolution de votre dette. Je vous rappelle de la Section 3.1 que $R(t)\Delta t$ représente la somme que vous remboursez dans un lapse de temps Δt

autour de l'instant t. Comme le temps est mesuré en années (puisque I est un taux d'intérêt annuel), vous rembourserez par exemple pendant le premier mois ($t = 1/12, \Delta t = 1/12$) à peu près $R(1/12)1/12 = 3,47$FF et pendant le douzième mois ($t = 1, \Delta t = 1/12$) $R(1)1/12 = 42$FF. Vous pouvez très facilement vérifier que la solution de cette équation différentielle est donnée par :

$$C(t) = (C_0 - \frac{500}{I^2})e^{It} + \frac{500}{I^2}(1 + It). \tag{8.4}$$

Comme pour le cas précédent, le temps de remboursement T satisfait à l'équation $C(T) = 0$ qui peut être réécrite de la façon suivante :

$$\frac{500}{I^2}(1 - (1 + IT)e^{-IT}) = C_0 \tag{8.5}$$

Cette équation a-t-elle une solution ? A nouveau, le membre de gauche représente le capital que vous pouvez emprunter, si vous êtes prêt à rembourser pendant un temps T et doit donc être une fonction strictement croissante de T (Figure 8.1). Elle tend cette fois-ci vers $\frac{500}{(0,07)^2} = 102.041$FF !

Exercice 8.2. *(i) Montrer ces deux dernières affirmations.*

(ii) Pourquoi cette fois-ci le banquier semble à priori prêt à vous prêter nettement plus que la dernière fois ?

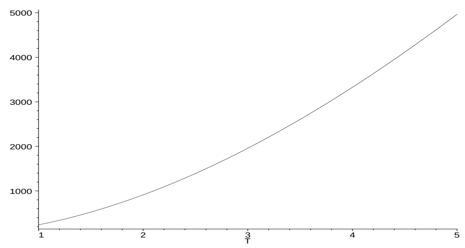

FIG. 8.1 – Le capital C_0 que je peux emprunter exprimé en fonction du temps T pendant lequel je souhaite rembourser. Ici $I = 0.07$ et T est exprimé en années.

Donc, si $C_0 < 102.041$FF, il existe une unique solution T de (8.5) et dans ce sens, il est clair que T est une fonction de C_0. Mais, contrairement à ce qui se passait dans l'exemple précédent, il n'est plus possible de trouver une formule simple, en termes de fonctions connues, qui permet d'exprimer T en fonction de C_0. Si vous souhaitez néanmoins savoir combien de temps vous devrez rembourser, si vous empruntez 3.000FF, 10.000FF ou 20.000FF, vous pouvez tracer le graphe du membre de gauche de (8.5) et vérifier visuellement pour quelle valeur de T il coupe la droite horizontale correspondant à ces trois sommes.

Exercice 8.3. *Quelles valeurs de T trouvez-vous ? Sont elles plus longues ou plus courtes que précédemment ? Pouvez-vous comprendre cela intuitivement ?*

Comme les exemples ci-dessus l'illustrent, et comme tous les problèmes de solution d'équations en mathématiques, le problème (8.1) peut être coupé en trois. D'abord on peut se poser la question de l'existence d'une solution :

"Pour quelles valeurs de d l'équation a-t-elle une solution ?"

On peut la reformuler en un langage plus savant de la façon suivante :

"Quelle est l'image $f(D)$ de f ?"

En effet, dire que d appartient à l'image de f (ou que f prend la valeur d) est précisément la même chose (Voir Section 3.3) que de dire que l'équation (8.1) a une solution ! Ceci explique d'ailleurs en partie l'intérêt de la notion de l'image d'une fonction. Nous verrons dans les Sections 8.2 et 8.3 comment identifier l'image d'un intervalle par une fonction continue. Le théorème des valeurs intermédiaires jouera un rôle essentiel ici. Une fois qu'on sait que l'équation a des solutions, la deuxième question est :

"La solution est-elle unique ? Si non, combien y en a-t-il ?"

Ici, je m'intéresserai surtout au cas où la solution est unique. Ce sera le cas lorsque la fonction f dans (8.1) est injective (Section 8.4), ce qui est en particulier le cas lorsqu'elle est strictement monotone. Ceci est souvent relativement facile à décider en utilisant la dérivée (Voir Section 7.2). La dernière question qui se pose est finalement :

"Comment peut-on calculer de façon efficace (une valeur approchée)
de la solution ?"

Cette question, pourtant intéressante et importante, relève de ce qu'on appelle l'analyse numérique, et je n'en parlerai pas ici.

On est souvent intéressé à résoudre une équation comme (8.1) non pour une seule valeur d, mais plutôt, comme dans l'exemple avec le banquier, pour plusieurs valeurs. On considère alors d dans l'équation comme une variable, et non comme une constante, tel que je l'ai fait jusqu'ici. Ce changement de point de vue ressort très clairement dans l'exemple avec T et C_0 ci-dessus. On écrit alors volontiers l'équation sous la forme $y = f(x)$. Lorsque la solution x est unique pour chacun des $y \in f(D)$, on peut dire que x est fonction de y. L'équation $y = f(x)$ peut alors être réécrite dans la forme $x = g(y)$, pour un choix convenable de g. On obtient ainsi la notion de fonction réciproque qu'on étudiera en détail dans les Sections 8.5 - 8.6 - 8.7. Je donne un exemple simple. Considérons l'équation

$$y = \frac{x}{x+1}.$$

C'est l'équation du graphe de $f(x) = x/(x+1)$, dont on vérifie facilement que c'est une fonction strictement croissante. On peut réecrire cette équation de la façon suivante :

$$y(x+1) = x \text{ ou encore } \frac{y}{1-y} = x.$$

Dans cette dernière relation, qui est de la forme $x = g(y)$, on voit bien que j'ai exprimé x comme fonction de y (Figure 8.2).

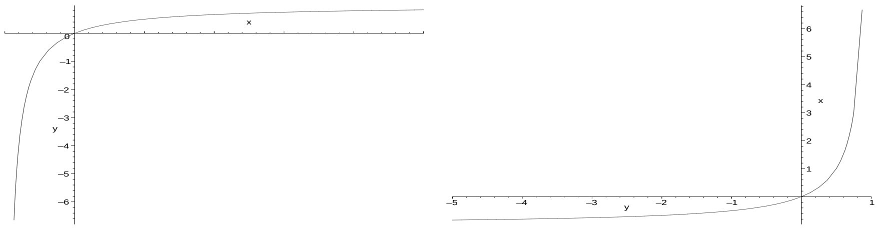

FIG. 8.2 – Les graphes de $y = x/(1+x)$ et de $x = y/(1-y)$. Remarquer que dans le premier cas l'axe horizontal est l'axe des x, tandis que dans le deuxième, c'est l'axe des y : dans les deux cas, j'ai choisi de mettre sur l'axe horizontal la variable indépendante.

La relation $y = f(x)$ acquiert ainsi une nouvelle vie. A l'origine, ce n'était rien d'autre que l'équation du graphe de f et elle exprimait donc dans un premier temps comment la variable y dépend de la variable x. C'est comme ça que vous avez passé vos années de lycée à voir les choses. Mais, si chaque valeur de la variable y n'est atteinte que pour une unique valeur de x, on peut tout aussi bien changer de point de vue – et c'est le programme de ce chapitre – pour dire que la variable x dépend de (est fonction de) la variable y. Ce changement de point de vue a tendance à perturber les étudiants pour qui – par habitude – une fonction d'un cours de mathématiques doit dépendre de x, et pas d'autre chose. Si vous avez ce problème, je vous invite à relire le passage sur le remboursement de votre prêt, jusqu'à ce que cela vous paraît naturel. Ce qui marche avec T et C_0, ne devrait-il pas marcher aussi avec x et y ? Le cours de physique regorge par ailleurs d'exemples de ce type.

Un autre exemple, un peu plus compliqué, est

$$y = \frac{x}{x^2+1}.$$

C'est aussi le graphe d'une fonction (que je vous invite à tracer), mais elle n'est pas injective. En effet, elle est strictement croissante pour $x \in [-1, 1]$ et strictement décroissante sinon. Elle atteint son maximum global, qui vaut $1/2$, en $x = 1$ et son minimum global, qui vaut $-1/2$, en $x = -1$. Peut-on résoudre cette équation pour trouver x en fonction de $y \in [-1/2, 1/2]$? On s'attend à trouver, pour chaque valeur de y, deux valeurs de x. En effet, l'équation peut se réécrire

$$yx^2 - x + y = 0,$$

qui (lorsque $y \neq 0$) est une équation quadratique dans l'inconnue x, et dont les solutions sont

$$x = \frac{1 - \sqrt{1-4y^2}}{2y} \text{ et } x = \frac{1 + \sqrt{1-4y^2}}{2y}.$$

La première solution correspond à la partie du graphe de $\frac{x}{x^2+1}$ avec $x \in [-1, 1]$, et la deuxième à la partie avec $|x| \geq 1$.

Exercice 8.4. *(i) Pourquoi ? (ii) Montrer que*

$$\lim_{y \to 0} \frac{1 - \sqrt{1 - 4y^2}}{2y} = 0.$$

Expliquer ce résultat.

Je termine par une remarque. Les équations du type $y = f(x)$ peuvent être considérées comme des cas spéciaux des équations plus générales

$$G(x, y) = 0,$$

où $G : \mathbb{R}^2 \to \mathbb{R}$ est une fonction de 2 variables. Par exemple

$$x^2 + y^2 - 1 = 0$$

est de ce type. C'est, comme vous savez, l'équation du cercle de rayon 1, centré à l'origine. Un autre exemple est

$$x^2 - y^2 = 1.$$

Toutes ces équations ne font qu'exprimer une relation entre les variables x et y. Dans les deux derniers exemples ci-dessus, la donnée de x ne détermine pas de façon unique y, et la donnée de y ne détermine pas x : ce ne sont donc pas des équations du graphe d'une fonction de x, ni celles du graphe d'une fonction de y. L'étude systématique de ces équations plus générales fait partie du programme de deuxième année.

8.2 Le théorème des valeurs intermédiaires

L'outil principal introduit dans ce chapitre est le théorème suivant.

Théorème 8.5. *(Le théorème des valeurs intermédiaires–TVI) Soit $f\colon I \to \mathbb{R}$ une fonction continue définie sur un intervalle I. Soient $x_1, x_2 \in I$ tels que $f(x_1) \leq f(x_2)$. Alors f prend toutes les valeurs comprises entre $f(x_1)$ et $f(x_2)$. Plus précisément, quelque soit le nombre y_* compris entre $f(x_1)$ et $f(x_2)$, (*i. e. *$f(x_1) \leq y_* \leq f(x_2)$), il existe x_* compris entre x_1 et x_2 tel que $f(x_*) = y_*$. En particulier,*

$$[f(x_1), f(x_2)] \subset f(I).$$

On peut dire aussi que l'image de f n'a pas de trous, ce qui est à rapprocher de la notion de “continu” dans le sens de “faite d'une seule partie” (Voir Section 5.1) et de l'idée que le graphe d'une fonction continue se trace “sans lever le crayon”. Je donnerai des informations plus précises encore sur $f(I)$ lorsque f est continue dans la section suivante, mais remarquons tout de suite que l'hypothèse

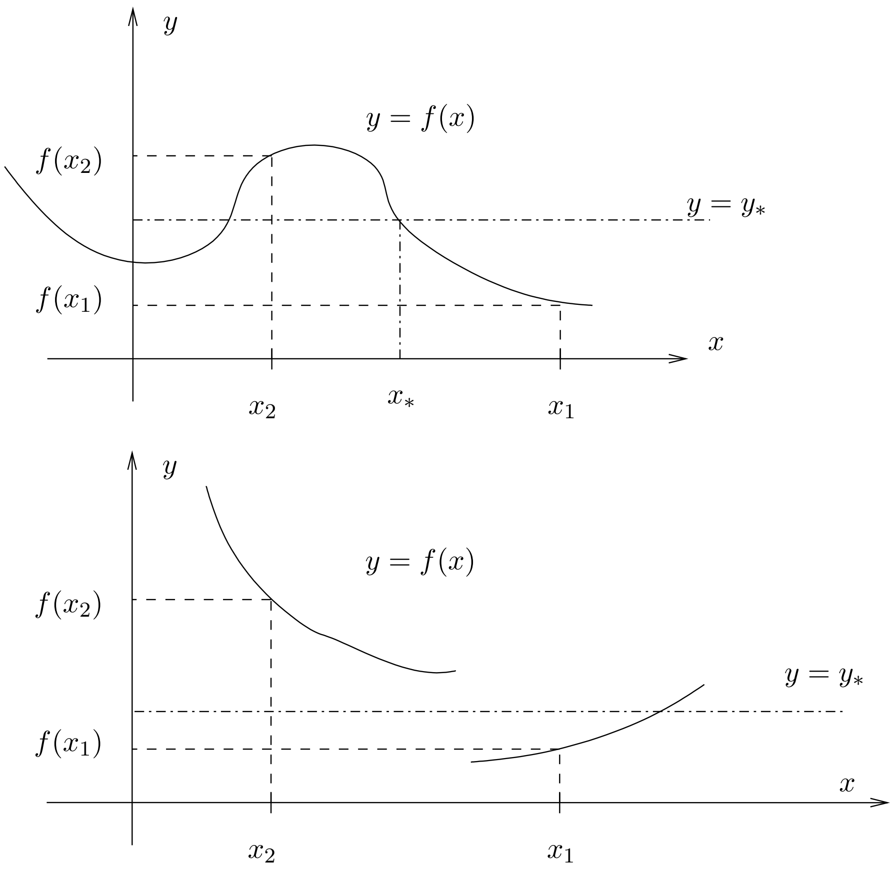

FIG. 8.3 – En haut, une fonction continue. En bas, une fonction discontinue : on remarque que la valeur y_* indiquée n'est pas atteinte par f entre x_1 et x_2. Elle est néanmoins atteinte plus loin !

que le domaine de f est un intervalle est cruciale ici. En effet, la fonction $f : \mathbb{R}^* \to \mathbb{R}$, définie par $f(x) = x/|x|$ est bel et bien continue en chaque point de son domaine. Néanmoins, bien qu'elle vaille 1 en $x = 2$ et -1 en $x = -2$, elle ne prend la valeur intermédiaire 0 nullepart ! Son image est l'ensemble $\{-1, 1\}$, qui n'est bien sûr pas fait "d'une seule partie". La raison se trouve dans le fait que $\mathbb{R}^*$ n'est pas un intervalle.

Le TVI et le théorème du maximum sont les deux théorèmes les plus importants que nous verrons concernant les fonctions continues. Tous les autres théorèmes sur les fonctions continues en sont des conséquences plus ou moins directes.

La démonstration du TVI n'est pas tout à fait simple, même si je n'utiliserai que des techniques de démonstration dont je me suis déjà servi. Je la remets à la Section 8.10 et je me tourne d'abord vers quelques-unes des applications du

TVI.

8.3 Identifier l'image de f

J'ai indiqué dans l'introduction que, dans le contexte de la résolution de l'équation (8.1), il est important d'identifier l'image de la fonction f. Je me concentrerai ici sur le cas le plus souvent utile où la fonction f est continue et où le domaine de f est un intervalle I d'extrémités a et b avec $-\infty \leq a < b \leq +\infty$. Le résultat central est alors le suivant.

Théorème 8.6. *Soit $f : I \to \mathbb{R}$ une fonction continue. Alors $f(I)$ est un intervalle d'extrémités $\inf f(I)$ et $\sup f(I)$. Si $I = [a, b]$ avec $-\infty < a < b < +\infty$, alors $f(I) = [\inf f(I), \sup f(I)] = [\min f(I), \max f(I)]$.*

On résume parfois brièvement ce résultat en disant que l'image d'un intervalle par une fonction continue est encore un intervalle (Fig. 8.4).

Rappelez-vous que nous avons vu que, si E est un sous-ensemble non-vide de $\mathbb{R}$, il admet une borne supérieure que nous avons désigné par $\sup E$. Si E n'est pas majoré, on définit tout simplement (et très naturellement) $\sup E = +\infty$. De cette façon, le théorème de la borne supérieure peut être reformulé en disant que tout sous-ensemble non-vide de $\mathbb{R}$ (majoré ou non) admet une borne supérieure (qui est égale à $+\infty$ si jamais E n'est pas majoré). De la même façon, on pose $\inf E = -\infty$ lorsque E n'est pas minorée. J'ai utilisé cette convention dans l'énoncé ci-dessus, ce qui le simplifie considérablement. Remarquons encore que, avec cette convention toujours, on a, comme dans la Proposition 6.17 (ii)

$$\forall x < \sup E, \exists x' \in E, x < x' \leq \sup E.$$

même dans le cas où $\sup E = +\infty$.

Démonstration : Clairement, quelque soit $x \in I$ (voir Fig. 8.4),

$$\inf f(I) \leq f(x) \leq \sup f(I). \tag{8.6}$$

En d'autres termes, l'image $f(I)$ de f est un sous-*ensemble* de l'intervalle fermé d'extrémités $\inf f(I)$, $\sup f(I)$. Ça n'a bien évidemment rien à voir avec la continuité de f, et est vrai pour toute fonction, continue ou pas ! Je vais montrer par ailleurs que *pour une fonction continue*

$$]\inf f(I), \sup f(I)[\subset f(I), \tag{8.7}$$

ou, ce qui revient au même, que quelque soit $y \in \mathbb{R}$

$$\inf f(I) < y < \sup f(I) \Rightarrow y \in f(I). \tag{8.8}$$

Cela signifie très exactement que $f(I)$ est un intervalle d'extrémités $\inf f(I)$ et $\sup f(I)$ et est une conséquence du théorème des valeurs intermédiaires et de la caractérisation de la borne supérieure. En effet, puisque $y < \sup f(I)$, il existe $y \leq y_1 \leq \sup f(I)$ tel que $y_1 \in f(I)$. De même, il existe $\inf f(I) < y_0 < y$

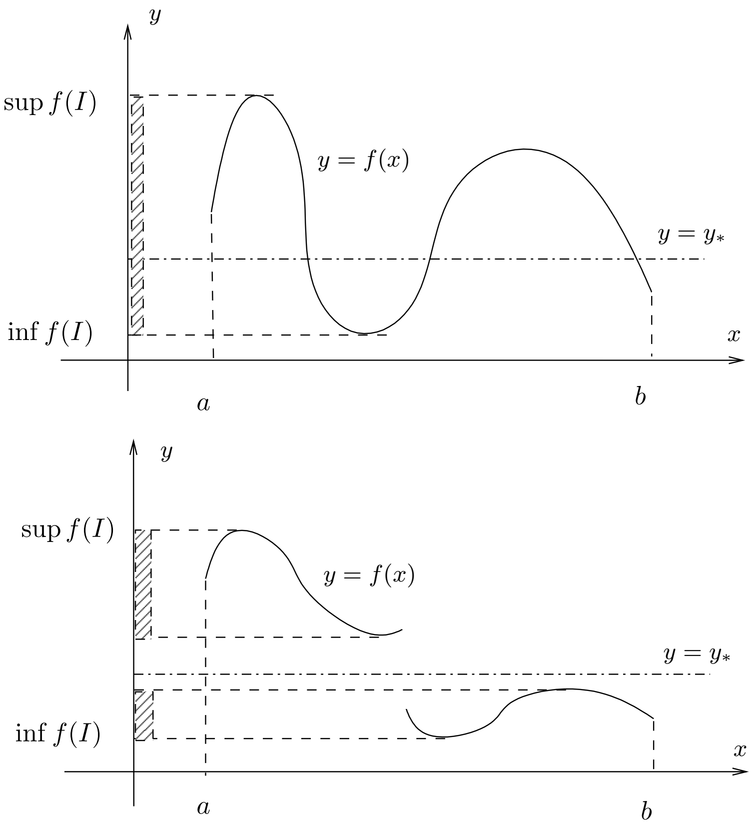

FIG. 8.4 – En haut, une fonction continue. En bas, une fonction discontinue. J'ai indiqué, dans les deux cas, par une boîte hachurée l'image $f(I)$ de $I = [a, b]$ par f. Remarquer que dans le deuxième cas, ce n'est pas un intervalle.

tel que $y_0 \in f(I)$. Par le théorème des valeurs intermédiaires on en conclut que $[y_0, y_1] \subset f(I)$ et donc en particulier $y \in f(I)$. Bien sûr, (8.6) et (8.7) impliquent que $f(I)$ est un intervalle d'extrémités $\inf f(I), \sup f(I)$. Si maintenant f est définie sur un intervalle borné et fermé $[a, b]$, le théorème du maximum dit que $\inf f(I) = \min f(I) \in f(I)$, et $\sup f(I) = \max f(I) \in f(I)$ ce qui implique le résultat.

J'espère que cette démonstration ne vous a paru trop difficile. Il faut tout de même remarquer qu'elle utilise de façon essentielle les deux grands théorèmes sur les fonctions continues que nous avons vus : le théorème du maximum et le TVI. Le corollaire suivant est parfois utile dans les applications.

Corollaire 8.7. *(i) Si $f : I \to \mathbb{R}$ est continue et monotone, alors $f(I)$ est un intervalle d'extrémités $\lim_{x\to a} f(x)$ et $\lim_{x\to b} f(x)$.*

(ii) Si f est continue et strictement monotone, alors

$$a \in I \Leftrightarrow \lim_{x \to a} f(x) \in f(I)$$

et

$$b \in I \Leftrightarrow \lim_{x \to b} f(x) \in f(I).$$

On voit ainsi par exemple que, si f est strictement croissante et continue sur un intervalle *borné* I d'extrémités $-\infty < a < b < +\infty$,

$$f([a,b]) = [f(a), f(b)], f(]a,b]) =]\lim_{x \to a} f(x), f(b)], \ etc.$$

et si f est continue et strictement décroissante,

$$f([a,b]) = [f(b), f(a)], f(]a,b]) = [f(b), \lim_{x \to a} f(x)[, \ etc.$$

Il faut faire quelques dessins (C'est un ordre !) pour explorer les différentes possibilités et se convaincre que le corollaire permet d'identifier $f(I)$ si f est monotone et continue. Quelques exemples sont donnés dans la figure 8.5.

Exercice 8.8. *Considérer la fonction $f(x) = x/(x+1)$ sur $D_1 =]-1, +\infty[$. Montrer qu'elle est strictement croissante et établir que $f(D_1) =]-\infty, 1[$. Même question pour $f(x) = x/(x+1)$ sur $D_2 =]-\infty, -1[$. Que vaut $f(D_2)$? Faites le graphe.*

Démonstration du corollaire : C'est un peu subtil (surtout le (ii)) , mais je vais être bref, à vous de compléter les raisonnements.

(i) Je vous rappelle d'abord que nous savons déjà que les limites de f en a et b existent, grâce au théorème des fonctions monotones (Théorème 6.18). Ces limites étant par ailleurs de toute évidence égales au $\sup f(I), \inf f(I)$ (Pourquoi ?), on peut conclure en invoquant le théorème précédent.

(ii) Supposons que f soit strictement croissante et démontrons la première affirmation. Pour l'implication directe, on remarque que, comme $a \in I$ et comme f est continue, on a $\lim_{x \to a} f(x) = f(a) \in f(I)$. C'est donc simple. Supposons maintenant que $\lim_{x \to a} f(x) \in f(I)$. Nous savons par ailleurs que $\lim_{x \to a} f(x) = \inf f(I)$ et donc que $\inf f(I) \in f(I)$. Mais si la borne inférieure appartient à $f(I)$, c'est un minimum. Il existe donc $x_* \in I$ tel que $f(x_*) = \lim_{x \to a} f(x) = \min f(I) = \inf f(I)$. Je vais montrer par l'absurde que x_* doit être égal à a. Supposons au contraire que $x_* > a$. Alors, il existe $x \in I$ tel que $x_* > x > a$, et donc $f(x_*) > f(x)$ (Faites un dessin !) ce qui est en évidente contradiction avec le fait que $\min f(I) = f(x_*)$. On conclut donc que $a = x_*$ et donc que $a \in I$.

Exercice 8.9. ** Quelles affirmations du corollaire restent valables si je remplace l'hypothèse "strictement monotone" par "monotone" ?* **Indication :** *Fouillez dans la démonstration du corollaire (ii) pour voir où j'ai utilisé la stricte monotonie.*

Exercice 8.10. *L'affirmation suivante, est-elle vraie ou fausse ? "Si $f : I \to \mathbb{R}$ est une fonction et si $f(I)$ est un intervalle, alors f est continue."*

Solution : C'est faux ! Un exemple est donné dans la figure 8.6.

8.4 Injectivité, surjectivité et bijectivité

8.4.1 Définitions

Dire que (8.1) a au moins une solution, on l'a vu, c'est dire que d appartient à l'image de f. Dire que cette solution est unique, c'est dire que la fonction f ne prend la valeur d qu'une seule fois, ou encore,dans le langage de la Section 3.3, que d a exactement un antécédent. On appelle une fonction qui, pour chaque point de son image, n'a qu'un seul antécédent, *injective*. C'est pour les fonctions injectives que nous pourrons définir une fonction réciproque.

Plus généralement, les notions de fonction injective, surjective et bijective sont importantes aussi bien dans l'étude des fonctions numériques d'une variable qu'en algèbre linéaire (et ailleurs) : je les introduis brièvement ici pour une fonction quelconque, dans le cadre de la définition générale de fonction (Définition 3.6) :

Définition 8.11. *Soit $f : D \to E$.*

(i) f est injective si tout point de E a au plus un antécédent.

(ii) f est surjective si tout point de E a au moins un antécédent. En d'autres termes, f est surjective si et seulement si $f(D) = E$ (Comparer ceci avec la discussion dans la Section 3.3).

(iii) f est bijective si f est à la fois injective et surjective, c'est à dire si et seulement si tout point de E a exactement un antécédent.

Lorsque f est une fonction numérique, on peut visualiser les notions d'injectivité/surjectivité/bijectivité graphiquement.

Exercice 8.12. *Montrer que, si $f : D \to \mathbb{R}$ est une fonction numérique, alors*

(i) f est injective si et seulement si le graphe de f coupe toute droite horizontale au plus une seule fois.

(ii) f est surjective si et seulement si le graphe de f coupe toute droite horizontale au moins une fois.

(iii) f est bijective si et seulement si le graphe de f coupe toute droite horizontale exactement une fois.

Il sera important de décider si telle ou telle fonction est injective, surjective, ou bijective, mais les définitions données ci-dessus ne sont pas toujours utiles dans des cas concrets. Les réformulations suivantes servent parfois :

Lemme 8.13. *Soit $f : D \to E$.*

(i) f est injective si et seulement si $f(x_1) = f(x_2)$ implique $x_1 = x_2$ ($x_1, x_2 \in D$).

(ii) f est injective si et seulement si : $x_1 \neq x_2$ implique $f(x_1) \neq f(x_2)$ ($x_1, x_2 \in D$). En d'autres termes, f est injective si et seulement si elle prend des valeurs différentes en des points différents de son domaine.

(iii) f est surjective si et seulement si, quelque soit y en E, il existe au moins un x appartenant à D tel que $y = f(x)$.

(iv) f est bijective si et seulement si, quelque soit y appartenant à E, il existe exactement un élément x de D tel que $y = f(x)$.

Démonstration : (i) Supposons f injective. Soient $x_1, x_2 \in D$ tels que $f(x_1) = f(x_2) \in f(D)$. Comme chaque élément de E a au plus un antécédent, on conclut que $x_1 = x_2$.

(ii) C'est une reformulation du (i) ! Pensez contraposée...

(iii)-(iv) Débrouillez-vous.

Exercice 8.14. *L'affirmation suivante, est-elle vraie ou fausse ? "$f : D \to \mathbb{R}$ est injective si, quelque soit $x_1, x_2 \in D$,*

$$f(x_1) \neq f(x_2) \Rightarrow x_1 \neq x_2.''$$

Indication : *C'est un piège de mauvais goût.*

8.4.2 Critères d'injectivité

Pour les fonctions numériques continues ou dérivables, vers lesquelles nous tournons à nouveau notre attention maintenant, il existe des liens étroits entre les propriétés de monotonie et d'injectivité et bien évidemment, le signe de leur dérivée. En effet, nous avons déjà vu qu'une fonction dérivable, de dérivée strictement positive sur un intervalle, est strictement croissante sur cet intervalle (Section 7.2). Or, le lemme (très simple) suivant affirme qu'une telle fonction est injective :

Lemme 8.15. *Soit $f : D \to \mathbb{R}$ strictement monotone. Alors f est injective.*

Démonstration : Supposons que f soit strictement décroissante. Soient $x_1 \neq x_2$, avec $x_1, x_2 \in D$. Alors $x_1 < x_2$ ou $x_2 < x_1$. Dans le premier cas $f(x_1) > f(x_2)$ et dans le deuxième $f(x_1) < f(x_2)$. Donc $f(x_1) \neq f(x_2)$ et le Lemme 8.13 (ii) permet de conclure

Il est légitime de se demander si une fonction injective est forcément strictement monotone. Il n'en est rien !

Exercice 8.16. *Montrer que la réciproque du lemme est fausse en donnant un exemple de fonction injective qui n'est pas strictement monotone, d'abord dans le cas où $D = [0, 1] \cup [2, 3]$, puis dans le cas où $D = [0, 1]$. Pouvez-vous trouver des exemples où la fonction est continue ?*

Indication : Regarder la figure 8.7 et lire la suite.

Si vous avez trouvé le deuxième exemple recherché dans l'exercice (partie gauche de la figure 8.7), vous constaterez que la fonction n'est pas continue. En effet, pour les fonctions continues sur un intervalle, la réciproque du lemme précédent est bien vrai :

Lemme 8.17. *Soit $f : I \to \mathbb{R}$ une fonction continue sur un intervalle I d'extrémités $-\infty \leq a < b \leq +\infty$. Alors f est injective si et seulement si f est strictement monotone.*

Attention : ce lemme devient faux si je remplace I par un domaine quelconque. Par exemple, il est facile de trouver une fonction continue et injective sur $D = [0, 1] \cup [2, 3]$ qui n'est pas monotone (Figure 8.7, partie droite).

La démonstration du lemme n'est pas vraiment difficile, mais un peu fastidieuse. Il s'agit d'appliquer le TVI de façon répétée (et judicieuse) et c'est donc un bon exercice. On peut tout de même ne pas l'étudier lors d'un premier passage, sans grand dommage pour la suite du voyage.

Démonstration* : Etant donné le lemme précédent, il suffira de montrer que, si f est continue et injective, alors f est strictement monotone.

(i) Montrons le résultat d'abord dans le cas où $I = [a, b], -\infty < a < b < +\infty$. Puisque f est injective, on a $f(a) < f(b)$ ou $f(a) > f(b)$. Plaçons-nous dans le premier cas. Je montrerai que f est alors strictement croissante sur $[a, b]$. Je montre d'abord par l'absurde que, quelque soit $x \in]a, b[$, $f(a) < f(x) < f(b)$. En effet, supposons qu'il existe $x \in]a, b[$ tel que $f(x) \leq f(a)$. Comme $f(a) < f(b)$, on voit alors que $f(a)$ est une valeur comprise entre $f(x)$ et $f(b)$ (Fig, 8.8). Alors, le TVI appliqué à la fonction f sur l'intervalle $[x, b]$ garantit l'existence, dans l'intervalle $[x, b]$, d'un point x' tel que $f(x') = f(a)$; mais, comme $x' \neq a$, ceci est en contradiction avec l'hypothèse que f est injective sur $[a, b]$. On montre de même que $f(x) \geq f(b)$ est impossible. En d'autres termes, si $f(a) < f(b)$, alors le graphe de f doit être situé entre les deux droites horizontales $y = f(a)$ et $y = f(b)$.

Soient maintenant x, x' tels que $a < x < x' < b$. Par ce qui précède, on sait que $f(a) < f(x) < f(b)$. Par ailleurs, comme $x' \in]x, b[$, on peut cette fois-ci appliquer le raisonnement précédent sur l'intervalle $]x, b[$ pour conclure que $f(x) < f(x') < f(b)$. On a donc bien que $a < x < x' < b$ implique $f(x) < f(x')$, ce qui montre (avec ce qui précède) que f est strictement croissante sur $[a, b]$.

On montre de la même façon que f est strictement décroissante si $f(b) < f(a)$.

(ii) Traitons maintenant le cas général d'un intervalle I d'extrémités $-\infty \leq a < b \leq +\infty$: I peut être ouvert, demi-ouvert, borné ou non. Le fait que les extrémités n'appartiennent plus nécessairement à l'intervalle compliquera un peu la démonstration, sans pour autant en changer l'idée de base. Considérons deux points $x_1, x_2 \in I$ tels que $x_1 < x_2$. Comme f est injective, on a soit $f(x_1) < f(x_2)$, soit $f(x_2) < f(x_1)$. Plaçons-nous dans le premier cas. On sait alors par le (i) que f est strictement croissante sur $[x_1, x_2]$. Je vais montrer que ceci force f à être strictement croissante sur tout l'intervalle I. Pour cela, considérons deux points $x < x'$ quelconques de I et définissons $\alpha = \min\{x, x_1\}, \beta = \max\{x_2, x'\}$. L'intervalle $[\alpha, \beta]$ est donc le plus petit intervalle qui contient les quatre points x, x', x_1, x_2. Un cas possible, à savoir $x < x_1 < x' < x_2$, est représenté dans la figure 8.9. Je vous invite à dessiner les autres cas (par exemple $x_1 < x < x_2 < x'$) vous-même. Je commence par montrer par l'absurde que $f(\alpha) < f(\beta)$. En effet, dans le cas contraire, la partie (i) de la démonstration, appliquée à l'intervalle $[\alpha, \beta]$ permettrait de conclure que f est strictement décroissante sur $[\alpha, \beta]$ et cela contredit le fait que $f(x_1) < f(x_2)$. On peut donc conclure que $f(\alpha) < f(\beta)$ et donc, grâce à (i) que f est strictement croissante sur $[\alpha, \beta]$. Comme $x, x' \in [\alpha, \beta]$, il en résulte que $f(x) < f(x')$, ce qu'il fallait démontrer.

Comme je l'ai déjà fait remarquer, l'utilité de ces deux lemmes provient du fait que pour les fonctions dérivables, définies sur un intervalle, il est facile de décider si elles sont strictement monotones, en étudiant le signe de leur dérivée

(Voir Section 7.2).

8.5 Définition de la fonction réciproque

8.5.1 La définition

Nous voilà finalement correctement équipés pour aborder le véritable sujet de ce chapitre. Si vous avez oublié de quoi il s'agit, je vous recommande vivement de relire l'introduction.

Définition 8.18. *Soit $f : D \to E$ une fonction injective. La fonction réciproque de f, notée f^{-1}, est la fonction de domaine $f(D)$ définie pour tout $y \in f(D)$ par $f^{-1}(y) = x$ pourvu que $f(x) = y$. En d'autres termes, $f^{-1}(y)$ est par définition l'unique antécédent de y.*

Cette définition cache plusieurs subtilités et il faut un peu de temps pour bien l'assimiler. Reprenons l'exemple de la fonction $f(x) = x/(x+1)$, de domaine $D_1 =]-1, +\infty[$, traité dans l'Exercice 8.8 et dont j'ai déjà parlé dans l'introduction aussi (Voir également la Figure 8.2). Soit $y \in f(D_1) =]-\infty, 1[$. Que vaut $f^{-1}(y)$? Par exemple, prenons $y = -2$. Selon la définition ci-dessus, $f^{-1}(-2) = x$ si $f(x) = -2$. En d'autres termes, la valeur de la fonction réciproque au point -2 est la solution de l'équation $f(x) = -2$, c'est à dire $x = -2/3$. Plus généralement, si $y \in f(D_1) =]-\infty, 1[$, $f^{-1}(y)$ est la solution de l'équation $f(x) = y$, c'est à dire $x = y/(1-y)$. On a donc

$$f^{-1}(y) = y/(1-y).$$

On remarquera que, en toute généralité, *le domaine de f^{-1} est donné par l'image de f et que l'image de la fonction réciproque f^{-1} est le domaine de f*. Ceci est très important et montre aussi l'importance de savoir bien identifier l'image d'une fonction injective : on comprendra mieux pourquoi j'y ai consacré toute une section. Finalement, la définition de f^{-1} est résumée dans

$$\forall x \in D, \forall y \in f(D), y = f(x) \Leftrightarrow x = f^{-1}(y). \tag{8.9}$$

Exercice 8.19. *Etudier la fonction réciproque de la fonction $f(x) = x/(x+1)$, de domaine $D_2 =]-1, +\infty[$. Quel est son domaine ? Et son image ? Tracer son graphe.*

La définition implique bien évidemment que

$$\forall x \in D, (f^{-1} \circ f)(x) = x, \quad \text{et} \quad \forall y \in f(D), (f \circ f^{-1})(y) = y. \tag{8.10}$$

Attention ! La notation f^{-1} peut prêter à confusion. En effet, ne confondez pas la fonction réciproque avec la fonction $1/f$! Aussi, nous avons vu dans la Section 3.3 que l'image réciproque ou le pré-image d'un ensemble C, notée $f^{-1}(C)$ est définie pour n'importe quelle fonction f, même si elle n'est pas injective ! On utilise donc la notation $f^{-1}(C)$, même si la fonction réciproque de f n'existe pas ! ! Confus ? Allez donc retravailler le Chapitre 3. . . . En tout cas, vous avez le droit de trouver tout ceci difficile à la première lecture (mais plus dans quelques semaines. . .).

8.5.2 Le graphe de la fonction réciproque

Je commence par une remarque. Soit (α, β) un point du plan $\mathbb{R}^2$. On sait que (β, α) est alors le point du plan obtenu par symétrie par rapport à la première bissectrice. Supposons maintenant que le point de coordonnées (α, β) appartient au graphe de f, c'est à dire que $\beta = f(\alpha)$. Alors $\alpha = f^{-1}(\beta)$ et donc le point (β, α) appartient au graphe de f^{-1}. En d'autres termes, on obtient le graphe de f^{-1} à partir de celui de f en effectuant une symétrie par rapport à la première bissectrice. Vous pouvez vérifier ceci sur le graphe de la fonction réciproque de $f(x) = x/(x+1)$, étudié précédemment (Fig. 8.2), ainsi que sur les exemples de la Section 8.8 ci-dessous et sur la figure 8.10.

Une autre façon, plus intuitive, de comprendre le résultat ci-dessus, est la suivante. Si f est une fonction injective et $y = f(x)$ l'équation de son graphe, alors la fonction réciproque exprime simplement la variable x en fonction de la variable y via la relation équivalente $x = f^{-1}(y)$. Or, dans cette relation, y est maintenant la variable *indépendante* et x la variable *dépendante* (Voir le Chapitre 3), et dans un graphe, nous avons l'habitude de mettre la variable indépendante sur l'axe horizontal, et la variable dépendante sur l'axe vertical. Or, si vous dessinez le graphe de f sur une feuille transparente, et que vous faites tourner cette feuille dans l'espace de 180 degrés autour de la première bissectrice, vous aurez aligné l'axe des y horizontalement (et orienté vers la droite), et l'axe des x verticalement (orienté vers le haut) et vous verrez le graphe de f^{-1} ! Mais, comme la rotation effectuée a précisément le même effet sur le plan $x-y$ qu'une symétrie par rapport à la bissectrice, ceci montre que le graphe de f^{-1} est en effet obtenu à partir de celui de f en effectuant une symétrie par rapport à la première bissectrice. Vous pouvez suivre tout cela sur la figure 8.10.

Maintenant que nous savons ce qu'est la fonction réciproque d'une fonction, nous pouvons commencer à étudier ses propriétés. Deux questions s'imposent : si f est continue, que dire de f^{-1}, et si f est dérivable, *quid* de f^{-1} ? Elles sont traitées dans les sections suivantes.

8.6 Continuité d'une fonction réciproque

Théorème 8.20. *Soit $f : I \to \mathbb{R}$ une fonction continue et injective sur un intervalle I. Alors,*

(i) f est strictement croissante (décroissante) si et seulement si f^{-1} l'est ;

(ii) La fonction réciproque f^{-1} est continue.

En bref, la fonction réciproque d'une fonction continue sur un intervalle est continue. La démonstration constitue un excellent exercice sur la notion de limite. Elle a l'air simple, mais est assez subtile.

Démonstration : Nous avons vu (Lemme 8.17) qu'une fonction f, continue et injective sur un intervalle I, est strictement monotone. Supposons qu'elle est strictement décroissante (La preuve lorsqu'elle est strictement croissante est analogue à celle-ci, bien évidemment). Montrons d'abord que f^{-1} est strictement décroissante également. Soient donc $y_1, y_2 \in f(I)$, $y_1 < y_2$. Il existe alors $x_1, x_2 \in$

I tels que $y_1 = f(x_1), y_2 = f(x_2)$. Clairement $x_1 \neq x_2$. Supposons que $x_1 < x_2$, alors $f(x_1) > f(x_2)$, ce qui contredit $y_1 < y_2$. On conclut donc que $x_1 > x_2$. Comme $x_1 = f^{-1}(y_1), x_2 = f^{-1}(y_2)$, ceci montre que f^{-1} est strictement décroissante (Fig. 8.11).

Montrons maintenant la continuité de f^{-1}. Soit $y_* \in J = f(I)$. Rappelons que J est un intervalle. Il faut que je montre que, quelque soit $\epsilon > 0$, il existe $\delta > 0$ tel que, quelque soit $y \in J$,

$$|y - y_*| < \delta \Rightarrow |f^{-1}(y) - f^{-1}(y_*)| \leq \epsilon.$$

Introduisons $x_* = f^{-1}(y_*) \in I$. Traitons d'abord le cas où x_* est distinct des deux extrémités de I. En prenant ϵ assez petit (c'est à dire plus petit que la distance entre x_* et les extrémités de I), on a $x_* - \epsilon \in I$ et $x_* + \epsilon \in I$. On pose alors $y_1 = f(x_* + \epsilon)$ et $y_2 = f(x_* - \epsilon)$. Comme f est décroissante, on a $y_1 \leq y_* \leq y_2$ (Fig. 8.11). Comme par ailleurs f^{-1} est également décroissante, on voit que

$$y_1 \leq y \leq y_2 \Rightarrow f^{-1}(y_2) = x_* - \epsilon \leq f^{-1}(y) \leq f^{-1}(y_1) = x_* + \epsilon,$$

ce qui montre le résultat désiré si l'on prend $\delta = \min\{y_* - y_1, y_2 - y_*\}$.

Supposons maintenant que, par exemple, $x_* = a$. Alors $y_* = f(a)$. Pour tout $\epsilon > 0$ on définit $y_1 = f(x_* + \epsilon) < y_*$ et on voit que

$$y_1 \leq y \leq y_* \Rightarrow f^{-1}(y_*) = x_* \leq f^{-1}(y) \leq f^{-1}(y_1) = x_* + \epsilon$$

ce qui permet de conclure comme avant.

Exercice 8.21. ** *(i) Où la continuité de f a-t-elle été utilisée dans la démonstration de la deuxième partie du théorème ? (ii) L'affirmation suivante est-elle vraie ou fausse :*

"Soit $f : I \to \mathbb{R}$ strictement croissante. Alors f^{-1} est continue."

Indication de solution : (i) Nullepart. La seule chose qui est importante est que la fonction f est définie sur un intervalle. (ii) C'est vrai.

8.7 Dérivabilité d'une fonction réciproque

8.7.1 La dérivée de f^{-1}

Le théorème suivant dit essentiellement que la fonction réciproque d'une fonction dérivable est dérivable et donne une formule *très importante* pour sa dérivée :

Théorème 8.22. *Soit $f : [a, b] \to \mathbb{R}, (a, b \in \mathbb{R}, a < b)$ une fonction continue sur $[a, b]$, dérivable sur $]a, b[$ et telle que $\forall x \in]a, b[, f'(x) > 0$ (respectivement $\forall x \in]a, b[, f'(x) < 0$). Alors f est strictement croissante (respectivement décroissante) et $f([a, b]) = [f(a), f(b)]$ (respectivement $f([a, b]) = [f(b), f(a)]$). La fonction réciproque $f^{-1} : f([a, b]) \to \mathbb{R}$ est continue sur $f([a, b])$ et dérivable sur*

$]f(a), f(b)[$ (respectivement $]f(b), f(a)[$). Finalement, pour tout y strictement compris entre $f(a)$ et $f(b)$ on a

$$(f^{-1})'(y) = \frac{1}{f'(f^{-1}(y))}. \tag{8.11}$$

Ce théorème est un outil : je l'utiliserai pour construire les fonctions réciproques d'un certain nombre de fonctions que nous connaissons déjà, comme x^2 ou $\exp x$ et pour calculer leur dérivée. La plupart des affirmations du théorème ont déjà été démontrées. La nouveauté est la formule (8.11) pour la dérivée d'une fonction réciproque. Elle a tendance de faire un peu peur aux novices. Avant d'en donner une démonstration complète, je voudrais pour l'instant déjà expliquer d'où elle vient, et l'illustrer sur un premier exemple.

On a, avec des notations évidentes, claires, fort utiles, très répandues parmi les physiciens et autres consommateurs de mathématiques, mais honnies par bien des mathématiciens :

$$y = f(x), \text{ donc } \frac{dy}{dx} = f'(x),$$

et

$$x = f^{-1}(y), \text{ donc } \frac{dx}{dy} = (f^{-1})'(y).$$

Par ailleurs, *de toute évidence*,

$$(f^{-1})'(y) = \frac{dx}{dy} = \frac{1}{\frac{dy}{dx}} = \frac{1}{f'(x)} = \frac{1}{f'(f^{-1}(y))}.$$

Au fait, ceci n'a rien d'évident. En effet, la notation $\frac{dy}{dx}$ invite bien à penser que, “de toute évidence”, $\frac{dx}{dy} = \frac{1}{\frac{dy}{dx}}$, mais ceci n'est pas évident parce que $\frac{dy}{dx}$ n'est pas le quotient de dy par dx, ces deux objets n'ayant pas été définis ! C'est pour cela que les mathématiciens purs et durs préfèrent éviter ces notations : elles ne sont en effet pas très pratique pour écrire des démonstrations.

En conclusion, les lignes ci-dessus sont correctes, mais ne constituent pas une preuve. Par contre, elles sont très utiles et une fois la preuve du théorème sera donnée, vous pouvez vous en servir librement, à votre plus grand bénéfice. En effet, elles permettent d'abord de retrouver facilement la formule (8.11) si jamais l'aurait-on oubliée. Puis, elles sont fort utiles lorsqu'il s'agit de faire des calculs explicites. Regardons comment ça marche dans un cas très simple. D'autres exemples, beaucoup plus intéressants, seront étudiés dans la section suivante.

Soit $y = f(x) = (x+1)/(x+2)$ et donc, après calcul $x = f^{-1}(y) = (1-2y)/(y-1)$. Dans ce cas, on peut bien sûr directement calculer $(f^{-1})'(y) = \frac{1}{(y-1)^2}$, mais essayons d'obtenir ce résultat avec le calcul ci-dessus. On a

$$\frac{dy}{dx} = 1/(x+2)^2$$

et donc

$$(f^{-1})'(y) = \frac{dx}{dy} = \frac{1}{\frac{dy}{dx}} = \frac{1}{f'(x)} = (x+2)^2.$$

Remplaçant dans le membre de droite x par son expression en termes de y, on trouve en effet

$$(f^{-1})'(y) = (x+2)^2 = (\frac{1-2y}{y-1}+2)^2 = \frac{1}{(y-1)^2}.$$

Exercice 8.23. *Calculer, de deux façons différentes, comme ci-dessus, la dérivée de la fonction réciproque de $f(x) = x/(x+1)$.*

Démonstration du Théorème 8.22 : Toutes les affirmations du théorème ont déjà été démontrées, sauf la dérivabilité de la fonction réciproque. Je me placerai dans le cas où $f'(x) > 0$ pour tout $x \in]a,b[$. f est donc strictement croissante (Section 7.2). Soit $f^{-1}(a) < y_* < f^{-1}(b)$ et soit x_* l'antécédent de y_*, c'est à dire $x_* = f^{-1}(y_*)$ et $f(x_*) = y_*$. Il faut montrer que

$$\lim_{y \to y_*} \frac{f^{-1}(y) - f^{-1}(y_*)}{y - y_*} = \frac{1}{f'(f^{-1}(y_*))}.$$

Je vais utiliser un procédé très analogue à celui utilisé pour montrer la Proposition 5.16 sur la dérivabilité de fonctions composées. J'introduis la fonction $k :]a,b[\to \mathbb{R}$, définie par

$$k(x_*) = \frac{1}{f'(x_*)}$$

et

$$k(x) = \frac{x - x_*}{f(x) - f(x_*)}, \text{ lorsque } x \neq x_*.$$

Cette fonction est de toute évidence continue ! Par ailleurs,

$$\lim_{y \to y_*} \frac{f^{-1}(y) - f^{-1}(y_*)}{y - y_*} = \lim_{y \to y_*} (k \circ f^{-1})(y).$$

Finalement, puisque k et f^{-1} sont toutes les deux continues, $k \circ f^{-1}$ est continue et donc

$$\lim_{y \to y_*} (k \circ f^{-1})(y) = k(f^{-1}(y_*)) = k(x_*) = \frac{1}{f'(x_*)} = \frac{1}{f'(f^{-1}(y_*)},$$

ce qui termine la démonstration.

Cette démonstration rend précis l'idée un peu vague que $dx/dy = (dy/dx)^{-1}$. Elle est relativement simple mais un peu subtile et l'introduction de la fonction k laisse le sentiment désagréable que c'est une arnaque. En fait, j'ai utilisé que la composée de deux fonctions continues est continue, ce qui n'est pas si simple à démontrer, comme vous vous en souvenez peut-être.

J'en profite pour vous présenter encore quelques autres notations qui ont disparu des livres de mathématiques, mais qui peuplent avec bonheur les livres de science où les mathématiques sont utilisées. On sait que

$$\frac{df}{dx}(x) = \lim_{h \to 0} \frac{f(x+h) - f(x)}{h}.$$

Comme $f(x+h)-f(x)$ représente la variation de la grandeur f lorsque x varie de la quantité h, on écrit souvent $\Delta f = f(x+h) - f(x)$. C'est une notation suggestive, donc utile, mais peu précise (puisque le membre de gauche, Δf n'indique pas sa dépendance en x et en h), et donc (considérée comme) dangereuse.... Introduisant aussi le suggestif $\Delta x = h$, on réécrit

$$\frac{df}{dx} = \lim_{\Delta x \to 0} \frac{\Delta f}{\Delta x}.$$

Se rappelant $y = f(x)$, on n'a pas peur non plus d'écrire $\Delta y = \Delta f$ et donc

$$\frac{df}{dx} = \lim_{\Delta x \to 0} \frac{\Delta y}{\Delta x} = \frac{dy}{dx}.$$

De là, il n'y a qu'un pas à

$$\begin{aligned} \frac{dx}{dy} &= \lim_{\Delta y \to 0} \frac{\Delta x}{\Delta y} \\ &= \lim_{\Delta y \to 0} \frac{1}{\frac{\Delta y}{\Delta x}} = \frac{1}{\frac{dy}{dx}}. \end{aligned}$$

Encore une fois, ces notations sont trop imprécises pour permettre d'affirmer que ces calculs constituent des démonstrations. Néanmoins, ces calculs permettent de se souvenir des formules, de comprendre l'intuition derrière les résultats et sont très utiles dans les applications.

8.7.2 Une interprétation géométrique

La formule (8.11) a une interprétation géométrique intéressante, que je vous invite à suivre sur la figure 8.12. Comme le graphe de f^{-1} est obtenu de celui de f en exécutant une symétrie par rapport à la bissectrice, on voit immédiatement que l'angle θ que fait la tangente au graphe de f en (α, β) avec *l'horizontale* est égal à l'angle θ' que fait la tangente au graphe de f^{-1} en (β, α) avec la *verticale*. Il en résulte que

$$(f^{-1})'(\beta) = \cot \theta' = 1/\tan \theta = 1/f'(\alpha).$$

Mais c'est exactement la formule (8.11) !

8.8 Fonctions réciproques célèbres

Je considère qu'une fonction est célèbre si il y a une touche correspondante sur chaque calculatrice scientifique respectable. Je vous donnerai dans cette section rapidement la liste des fonction réciproques célèbres. Je n'ai pas dessiné leurs graphes, vous avez justement votre calculatrice pour cela ! Je ne donne pas non plus de démonstrations détaillées des affirmations que je fais, et je vous invite à les fournir, vous assurant de bien identifier les théorèmes que vous utilisez.

8.8.1 Les fonctions racines–les puissances rationnelles

Soit $q \in \mathbb{N}^*$. Considérons l'équation

$$x^q = y.$$

Appliquons le résultat de ce chapitre pour décider si elle a une solution. Si q est impair, la fonction $x \to x^q$ est strictement croissante, de domaine $\mathbb{R}$ et d'image $\mathbb{R}$. L'équation en question a donc une unique solution pour chaque $y \in \mathbb{R}$. On la désigne par $\sqrt[q]{y}$ ou $y^{1/q}$. La fonction $y \in \mathbb{R} \to \sqrt[q]{y} \in \mathbb{R}$ est la fonction réciproque de la fonction $x \to x^q$. Elle est donc strictement croissante, et dérivable, sauf en $y = 0$. Je calculerai sa dérivée ci-dessous. Si q est pair, l'équation n'a de solutions que si $y \geq 0$. Comme la fonction $x \in \mathbb{R}^+ \mapsto x^q \in \mathbb{R}$ est strictement croissante et d'image $\mathbb{R}^+$, il y a une unique solution positive, qu'on désigne également par $\sqrt[q]{y}$ ou $y^{1/q}$. *A partir de ces définitions*, on vérifie facilement les égalités suivantes,

$$y^{1/q}{y'}^{1/q} = (yy')^{1/q}, \quad y^{1/q}y^{1/q'} = y^{(q+q')/qq'},$$

la difficulté pour vous étant de comprendre qu'il y a vraiment quelque chose à démontrer. On a également, pour tout $p \in \mathbb{N}$ $(y \geq 0)$

$$(y^{1/q})^p = (y^p)^{1/q},$$

ce qui permet de *définir* $y^{p/q} = (y^p)^{1/q}$. Par conséquent, le calcul avec les puissances fractionnaires se fait comme avec les puissances entières.
Pour ceux qui ont vraiment compris : Il est bon de se rappeler que l'existence de $\sqrt[q]{y}$ pour tout $y \geq 0$ est une conséquence ici du théorème des valeurs intermédiaires. En particulier, nous avions insisté dans le cours d'arithmétique que l'équation $x^2 = 2$ n'avait pas de solution rationnelle et *admis* qu'elle avait une solution réelle. C'est maintenant démontré ! En dernière analyse, c'est une conséquence du théorème des suites adjacentes, qui exprime une propriété des réels, qui n'est pas partagée par les rationnels !

Calculons la dérivée de $\sqrt[q]{y}$ avec la formule (8.11) :

$$\frac{d}{dy}\sqrt[q]{y} = \frac{1}{q(\sqrt[q]{y})^{q-1}} = \frac{1}{qy}\sqrt[q]{y} = \frac{1}{q}y^{\frac{1}{q}-1}.$$

Tout ceci rend donc rigoureux les propriétés énoncées dans la Section 4.4.

Exercice 8.24. *(i) Montrer que, pour tout $r \in \mathbb{Q}$, $y > 0$,*

$$\frac{d}{dy}y^r = ry^{r-1}.$$

(ii) Tracer le graphe de x^2 et de sa fonction réciproque et vérifier qu'ils sont bien l'image miroir l'un de l'autre par rapport à la première bissectrice.

8.8.2 La fonction logarithme

Nous avons défini et étudié la fonction exponentielle dans le chapitre 6. Elle est définie sur $\mathbb{R}$, et son image est $\mathbb{R}_*^+$. Sa fonction réciproque s'appelle "la fonction logarithme", notée ln : elle est définie sur $\mathbb{R}_*^+$, a $\mathbb{R}$ comme image et

$$\forall x \in \mathbb{R}, \forall y \in \mathbb{R}_*^+,\ y = \exp x \Leftrightarrow \ln y = x.$$

Ses propriétés essentielles (que vous connaissez), se déduisent immédiatement de sa définition et des propriétés essentielles de la fonction exp. Ainsi, par exemple, si $a = \exp\alpha$, et $b = \exp\beta$, on a

$$\ln ab = \ln(\exp\alpha \times \exp\beta) = \ln(\exp(\alpha+\beta)) = \alpha+\beta = \ln a + \ln b.$$

On en déduit facilement que $\ln a^{-1} = -\ln a$ et que $\ln a^n = n \ln a$, pour tout $n \in \mathbb{Z}$.

Exercice 8.25. *Démontrer cela !*

Par ailleurs, avec la formule (8.11), on trouve

$$\frac{d}{dy}\ln y = \frac{1}{\exp x} = \frac{1}{y}.$$

Bien évidemment, si l'utilisation de la variable y comme argument d'une fonction vous gêne, vous pouvez écrire

$$\frac{d}{dt}\ln t = \frac{1}{t} \quad \text{ou} \quad \frac{d}{ds}\ln s = \frac{1}{s} \quad \text{ou même} \quad \frac{d}{dx}\ln x = \frac{1}{x}.$$

En tout cas, on voit bien que la fonction logarithme est une primitive de $1/x$, ce qui est une de ses propriétés les plus importantes. On a également,

$$\lim_{y\to 0^+} y\ln y = \lim_{x\to+\infty} \exp -x(\ln\exp(-x)) = \lim_{x\to+\infty} -x\exp(-x) = 0,$$

où j'ai utilisé le théorème 6.12 (iv). On peut de la même façon étudier le comportement du logarithme lorsque $y \to +\infty$.

8.8.3 Puissances réelles

On a déjà défini, ci-dessus, y^r, pour tout $y \in \mathbb{R}^+$ et $r \in \mathbb{Q}$. Si $\frac{p}{q} = r \in \mathbb{Q}$, on a

$$\ln y^r = p\ln y^{1/q} = \frac{p}{q} q \ln y^{1/q} = \frac{p}{q}\ln y = r\ln y,$$

d'où l'on conclut que

$$y^r = \exp(r\ln y).$$

En d'autres termes, j'ai réussi à exprimer les puissances rationnelles d'un nombre réel (positif) en termes des fonctions exponentielle et logarithme. Mais le membre de droite de la dernière expression ci-dessus a un sens même si $r \in \mathbb{R}$ est un nombre irrationnel ! Cela m'incite à introduire la définition suivante :

Définition 8.26. *Quelque soit $y \in \mathbb{R}_*^+$, $r \in \mathbb{R}$,*

$$y^r = \exp(r \ln y).$$

Par exemple on a ainsi $2^\pi = \exp(\pi \ln 2)$. Bien évidemment, 2^5 est 2 multiplié cinq fois avec lui-même, mais on ne peut pas paraphraser 2^π de cette façon. Le seul sens qu'on peut donner à cette expression est bien que c'est l'exponentielle de π fois $\ln 2$.

La notation y^r invite à penser que, quelque soit $y, y_1, y_2 \in \mathbb{R}_*^+$, $r, r_1, r_2 \in \mathbb{R}$, on a

$$y_1^r, y_2^r = (y_1 y_2)^r, \text{ et } y^{r_1} y^{r_2} = y^{r_1 + r_2}.$$

Exercice 8.27. *Montrer ceci en utilisant la définition de y^r et les propriétés des fonctions* exp *et* ln.

Tout ceci me permet d'introduire deux nouveaux types de fonctions. D'abord, pour $r \in \mathbb{R}$ quelconque, "la puissance r-ième" :

$$x \in \mathbb{R}_*^+ \to x^r \in \mathbb{R}.$$

Puis, pour $b \in \mathbb{R}_*^+$, "l'exponentielle de base b" :

$$x \in \mathbb{R} \to b^x \in \mathbb{R}_*^+.$$

Exercice 8.28. *(i) Montrer que*

$$\frac{d}{dx} x^r = r x^{r-1} \text{ et } \frac{d}{dx} b^x = (\ln b) b^x.$$

(ii) Tracer, à l'aide de votre calculatrice, le graphe de x^r et de b^x pour quelques valeurs de r et de b.

8.8.4 Les fonctions arcsin et arctan

La fonction sinus est une fonction périodique : elle n'est donc certainement pas injective. Néanmoins, si on la restreint à l'intervalle $[-\frac{\pi}{2}, \frac{\pi}{2}]$, elle est strictement croissante et donc injective ! En effet, sa dérivée étant le cosinus, elle est strictement positive sur $]-\frac{\pi}{2}, \frac{\pi}{2}[$. Sur l'intervalle $[-\frac{\pi}{2}, \frac{\pi}{2}]$ le sinus admet donc une fonction réciproque, que l'on appelle "l'arcsinus" (abrégée comme arcsin ou parfois $\sin^{-1}$) :

$$\forall x \in [-\frac{\pi}{2}, \frac{\pi}{2}], \forall y \in [-1, 1], y = \sin x \Leftrightarrow \arcsin y = x.$$

On a ainsi $\arcsin \frac{1}{\sqrt{2}} = \frac{\pi}{4}$ et $\arcsin 0 = 0$, $\arcsin 1 = \frac{\pi}{2}$, pour donner quelques exemples. L'arcsinus est une fonction de domaine $[-1, 1]$ qui prend comme valeur un angle entre $-\pi/2$ et $\pi/2$. D'ailleurs, on peut utilement lire l'équation $x = \arcsin y$ comme ceci : "y est l'angle (entre $-\pi/2$ et $\pi/2$) dont le sinus vaut x." On comprend ainsi mieux le nom "arcsinus" : après tout à chaque arc de cercle est associé un angle. Ainsi, l'angle dont le sinus vaut $1/\sqrt{2}$ est bien $\pi/4$.

Exercice 8.29. *Faire tracer par sa calculatrice les graphes des fonctions sinus et arcsinus et constater que l'un est bien l'image miroir de l'autre par rapport à la première bissectrice.*

Calculons la dérivée de la fonction arcsinus :

$$x = \arcsin y, \text{ donc } \frac{dx}{dy} = \frac{1}{\frac{dy}{dx}} = \frac{1}{\cos x} = \frac{1}{\sqrt{1-\sin^2 x}} = \frac{1}{\sqrt{1-y^2}}.$$

J'ai utilisé ici le fait que $\cos x > 0$ lorsque $x \in]-\pi/2, \pi/2[$: c'est pour cela que la racine carré *positive* apparaît dans le calcul. Finalement, nous avons trouvé,

$$\frac{d}{dy}\arcsin y = \frac{1}{\sqrt{1-y^2}}.$$

Exercice 8.30. *Obtenir ce même résultat à partir de la formule (8.11), sans utiliser les notations abrégées que j'ai utilisées ci-dessus.*

On constate ainsi que la fonction arcsinus est une primitive d'une fonction pas trigonométrique du tout : la fonction $\frac{1}{\sqrt{1-y^2}}$! L'intérêt de la fonction arcsinus vient principalement de là et nous en parlerons de nouveau dans les chapitres sur l'intégration.

On peut étudier de la même façon la fonction arccosinus, définie sur $[-1, 1]$ et à valeurs dans $[0, \pi]$. On trouve facilement

$$\frac{d}{dy}\arccos y = -\frac{1}{\sqrt{1-y^2}}.$$

On remarque que $-\arccos$ est, comme arcsin, une primitive de $1/\sqrt{1-y^2}$, ce qui implique qu'ils ne doivent différer que d'une constante. C'est en effet le cas : consultez votre calculatrice pour le constater sur leurs graphes et faites le premier exercice dans “Le lecteur s'entraîne” à la fin du chapitre pour mieux le comprendre.

Exercice 8.31. *(i) Etudier la fonction*

$$y \in [-1, 1] \mapsto \sin(\arcsin y) \in \mathbb{R}.$$

Tracer son graphe.

(ii) (i) Etudier la fonction

$$x \in \mathbb{R} \mapsto \arcsin(\sin x) \in \mathbb{R}.$$

Tracer son graphe.

Solution : (i) L'équation (8.10) implique immédiatement que $\sin(\arcsin y) = y$ quelque soit $y \in [-1, 1]$.

(ii) C'est plus délicat ! En effet, (8.10) implique immédiatement que $\arcsin(\sin x) = x$, quelque soit $x \in [-\frac{\pi}{2}, \frac{\pi}{2}]$, mais lorsque $x \notin [-\frac{\pi}{2}, \frac{\pi}{2}]$, ceci n'est plus vrai ! Par exemple, on voit facilement que $\arcsin(\sin\pi) = 0$! Plus généralement, pour $x \in [\frac{\pi}{2}, \frac{3\pi}{2}]$, $\sin x = -\sin(x-\pi)$ et $x - \pi \in [-\frac{\pi}{2}, \frac{\pi}{2}]$. Par conséquent, pour $x \in [\frac{\pi}{2}, \frac{3\pi}{2}]$,

$$\arcsin(\sin x) = \arcsin(-\sin(x-\pi)) = -\arcsin(\sin(x-\pi)) = -(x-\pi) = \pi - x.$$

Ceci permet de tracer la fonction $\arcsin(\sin x)$ pour $x \in [-\frac{\pi}{2}, \frac{3\pi}{2}]$. Comme par ailleurs la fonction $\arcsin(\sin x)$ est clairement périodique de période 2π, il est maintenant facile de tracer son graphe.
Remarque : Cette exercice montre que les relations (8.10) doivent être manipulées avec soin : il ne faut en particulier pas oublier qu'elles ne sont valables que sur les domaines de f et de f^{-1} respectivement.

La fonction tangente est strictement croissante, donc injective, sur $]-\frac{\pi}{2}, \frac{\pi}{2}[$ et son image est $\mathbb{R}$. Elle admet donc une fonction réciproque, strictement croissante, elle aussi, qu'on appelle la fonction arctangente :

$$\forall y \in \mathbb{R}, \forall x \in]-\frac{\pi}{2}, \frac{\pi}{2}[,\ y = \tan x \Leftrightarrow \arctan y = x.$$

Pour la dérivée, on calcule sans détour :

$$\frac{d}{dy}\arctan y = \frac{1}{dx/dy} = \frac{1}{1+\tan^2 x} = \frac{1}{1+y^2}.$$

On a donc trouvé une primitive pour la fonction $y \to 1/(1+y^2)$!

8.8.5 Les fonctions hyperboliques (réciproques)

On définit le sinus hyperbolique (sh ou sinh) et le cosinus hyperbolique (ch ou cosh) par

$$\sinh x = \frac{1}{2}(\exp x - \exp(-x)) \text{ et } \cosh x = \frac{1}{2}(\exp x + \exp(-x)).$$

Ce sont des fonctions très simples – la somme de deux exponentielles – et on peut, on doit, se demander pourquoi on leur a donné un nom, et pourquoi ce nom-là. Il suffit de regarder les propriétés suivantes, conséquences directes de leur définition, pour commencer à comprendre. On a, en effet,

$$\cosh^2 x - \sinh^2 x = 1, \quad \frac{d}{dx}\cosh x = \sinh x, \quad \frac{d}{dx}\sinh x = \cosh x.$$

Cela ressemble beaucoup, à quelques différences de signe près, à des propriétés analogues pour le sinus et le cosinus. Il y a aussi ceci. Considérons un point mobile, dont les coordonnées sont $(x(t), y(t))$, avec $x(t) = \cosh t, y(t) = \sinh t$. On a alors

$$x^2(t) - y^2(t) = 1,$$

ce qui signifie que le mobile se déplace sur une branche de *l'hyperbole* $x^2 - y^2 = 1$! C'est l'analogue de ce qui se passe lorsque $x(t) = \cos t, y(t) = \sin t$: alors

$x^2(t)+y^2(t) = 1$, et le point mobile se déplace sur le cercle $x^2+y^2 = 1$! D'autres choses encore se cachent derrière les noms poétiques "cosinus hyperbolique" et "sinus hyperbolique" (on en reparlera), mais au moins on voit à partir de ce qui précède qu'ils ne sont pas tout à fait farfelus.

Votre calculatrice a une touche "cosh" (ou ch) et une autre "sinh" (ou sh). Utilisez-la pour tracer les graphes. Vous constaterez que $\cosh 0 = 1$ et que $\cosh x \geq 1$ pour tout x, que $\sinh 0 = 0$, et que sinh est une fonction strictement croissante. Toutes ces propriétés et bien d'autres se déduisent facilement à partir de la définition et je vous invite à le faire.

On définit aussi $\tanh x = \sinh x/ \cosh x$, et ainsi de suite, on peut établir des formules pour $\sinh(a+b)$, analogues (à quelques signes près) aux formules trigonométriques correspondantes. Vous trouverez tout ça dans n'importe quel (autre) livre de DEUG, et je n'ai pas envie de le détailler pour vous.

Comme la fonction sinus hyperbolique est strictement croissante, de domaine $\mathbb{R}$ et d'image $\mathbb{R}$, elle admet une fonction réciproque, appelée "argument sinus hyperbolique" ($\mathrm{argsinh}, \sinh^{-1}$, argsh, ou sh^{-1}), de domaine et d'image $\mathbb{R}$ également :

$$\forall x \in \mathbb{R}, \forall y \in \mathbb{R}, \mathrm{argsinh} y = x \Leftrightarrow y = \sinh x.$$

On a

$$\frac{d}{dy}\mathrm{argsinh} y = \frac{1}{\frac{dx}{dy}} = \frac{1}{\cosh x} = \frac{1}{\sqrt{1+(\sinh x)^2}} = \frac{1}{\sqrt{1+y^2}},$$

où je me suis servi de la relation $\cosh^2 x = 1 + \sinh^2 x$ et du fait que le cosinus hyperbolique est toujours positif. On remarquera l'analogie avec (le calcul de) la dérivée de l'arcsinus !

On peut aussi remarquer que la fonction *cosh* est strictement croissante sur $[0, 1[$, d'image $[1, +\infty[$ et donc définir argcosh par

$$\forall x \in [0, +\infty[, \forall y \in [1, +\infty[,\ \mathrm{argcosh} y = x \Leftrightarrow y = \cosh x.$$

On a, pour $y > 1$,

$$\frac{d}{dy}\mathrm{argcosh} y = \frac{1}{\frac{dx}{dy}} = \frac{1}{\sinh x} = \frac{1}{\sqrt{(\cosh x)^2 - 1}} = \frac{1}{\sqrt{y^2-1}},$$

où je me suis encore servi de la relation $\cosh^2 x = 1 + \sinh^2 x$ et du fait que le sinus hyperbolique est positif lorsque $x > 0$.

On voit ainsi que, tandis que la fonction $\arcsin y$ nous fournissait une primitive de $1/\sqrt{1-y^2}$ (pour $|y| < 1$, bien évidemment), les fonctions hyperboliques inverses nous fournissent des primitives de $1/\sqrt{1+y^2}$ (avec $y \in \mathbb{R}$) et de $1/\sqrt{y^2-1}$ (avec $y > 1$). Nous verrons dans le Chapitre **??** qu'a partir de là on peut trouver une primitive pour toute fonction de la forme $1/\sqrt{P(x)}$, où $P(x)$ est un polynôme de degré 2.

Pour conclure, ceci. J'ai fait remarquer que les fonctions hyperboliques sont définies très simplement en termes d'une somme d'exponentielles. On peut se demander si on ne peut pas calculer les fonctions hyperboliques réciproques très simplement aussi en termes de la fonction logarithme ? C'est en effet le cas. De

$$y = \frac{1}{2}(\exp x - \exp(-x)),$$

on obtient, en multipliant l'expression par $\exp x$, et en la remaniant un peu :

$$\exp(2x) - 2y \exp x - 1 = 0.$$

Mais cette égalité peut être vue comme une équation quadratique pour l'inconnue $X = \exp x$. Comme $x \geq 0$, on trouve

$$\exp x = X = \frac{1}{2}(2y - \sqrt{4y^2 + 4}) = y + \sqrt{y^2 + 1},$$

et donc

$$x = \ln(y + \sqrt{y^2 + 1}).$$

On en conclut que

$$\text{argsinh} y = \ln(y + \sqrt{y^2 + 1}),$$

d'où il est instructif de retrouver la formule pour la dérivée.

Exercice 8.32. *La fonction sinh étant impaire, la même chose est vraie pour la fonction* argsinh. *Par conséquent la fonction* $y \in \mathbb{R} \mapsto \ln(y + \sqrt{y^2 + 1})$ *est impaire aussi. Donner une démonstration directe de cette dernière propriété, sans passer par la fonction argsinh.*

Des formules semblables peuvent être établies pour les fonctions argtanh et argcosh.

8.8.6 Les autres

Quelle est l'utilité des touches de calculatrice donnant $\ln x$, $\arcsin x$, *etc.* ? Essentiellement, qu'on peut trouver rapidement et sans trop réfléchir une solution numérique d'équations comme

$$\exp x = 25 \quad \sin x = 0,9,$$

en écrivant $x = \ln 25, x = \arcsin 0,9$ et en sortant sa calculatrice. Une question reste néanmoins en suspens : comment la calculatrice "sait-elle" évaluer ces fonctions ? Nous y reviendrons dans le Chapitre **??**. Il faut aussi remarquer qu'il y a beaucoup de fonctions injectives très simples, comme $f(x) = x + \exp x$, dont la fonction réciproque n'est pourtant pas célèbre : elles n'ont pas de nom, et elles ne sont pas honorées par une touche de calculatrice. Si vous avez besoin de déterminer $f^{-1}(2)$, par exemple, vous devez développer une méthode pour résoudre l'équation

$$x + \exp x = 2.$$

C'est un des sujets qui est abordé dans les cours d'analyse numérique, en deuxième ou troisième année.

8.8.7 Le nom des variables II

Ceci est une petite suite à la section 5.5.4. J'ai, presque systématiquement dans tout ce chapitre, utilisé x comme nom de la variable indépendante des fonctions f, et y comme nom de la variable indépendante des fonctions réciproques. Cela vient très naturellement, c'est très commode dans les calculs, et aussi d'un point de vue conceptuel. Bien évidemment, j'aurais pu utiliser d'autres noms que x et y, mais il est important, surtout au début, d'utiliser un symbol différent pour désigner la variable indépendante de f et celle de f^{-1}. J'ai déjà souligné que dans les applications cela se fait quasi-automatiquement : pensez à l'exemple du capital initial C_0 et du temps de remboursement T. Bien évidemment, on vous demandera peut-être à un moment ou un autre de calculer la dérivée de $\arcsin x$, plutôt que la dérivée de $\arcsin y$. Si vous connaissez la formule par coeur, vous n'avez qu'à remplacer y par x. Si non, il convient de procéder ainsi. Puisque le prof veut que j'utilise x comme variable de arcsinus, je donnerai un autre nom à la variable du sinus, par exemple θ (ou t, ou s, ou n'importe quoi d'autre). Alors

$$x = \sin\theta \Leftrightarrow \arcsin x = \theta$$

et donc, avec le même calcul que ci-dessus,

$$\frac{d\theta}{dx} = \frac{1}{\frac{dx}{d\theta}} = \frac{1}{\cos\theta} = \frac{1}{\sqrt{1-\sin^2\theta}} = \frac{1}{\sqrt{1-x^2}}.$$

Je vous conseille de vous entrainer à faire de tels calculs, c'est très utile.

8.9 Primitives

J'ai expliqué, dans l'introduction du Chapitre 3 que le but principal de ce cours est de résoudre les équations différentielles du type $a(x)f'(x)+b(x)f(x) = c(x)$. Nous avons fait un premier bout de chemin dans le Chapitre 6, où nous avons construit la fonction exponentielle, solution de $f'(x) = f(x)$. J'avais signalé aussi qu'il n'est pas du tout évident que l'équation $f'(x) = c(x)$ a toujours une solution, même si $c(x)$ est une fonction simple, comme une fraction rationnelle par exemple. Mais maintenant, nous avons progressé un peu, grâce à la notion de fonction réciproque. En effet, on a constaté que la fonction $\ln x$, réciproque de la fonction exponentielle, est une primitive de $1/x$, c'est à dire, est une solution de $f'(x) = 1/x$. Nous avons donc établi *l'existence* d'une telle primitive. De même, nous avons établi l'existence d'une primitive de $1/(1 + x^2)$, à savoir la fonction arctangente. Nous verrons dans le Chapitre **??** qu'on peut exprimer les primitives de toute fraction rationnelle comme une somme de fractions rationnelles, de logarithmes et d'arctangentes. Cela résoudra alors complètement le problème d'existence de solutions à $f'(x) = c(x)$, avec $c(x)$ une fraction rationnelle.

Bien évidemment, un problème reste toujours en suspens. Nous n'avons pas encore développé des méthodes pour calculer de façon efficace la fonction logarithme ou l'arctangente : pour le moment, nous savons seulement que la calculatrice, apparemment, dispose d'une telle méthode, parce qu'elle nous donne une valeur approchée (avec 13 chiffres) de ces fonctions, pour n'importe quelle valeur de x dans leur domaine. On verra plus loin (Chapitre **??**) comment on peut en effet les calculer en les approchant par des polynômes.

8.10 Démonstration du TVI*

Soit $f : I \to \mathbb{R}$ continue, $x_1, x_2 \in I$ tels que $f(x_1) \leq f(x_2)$. Soit $f(x_1) \leq y_* \leq f(x_2)$. Il faut montrer qu'il existe $x_* \in I$ tel que $f(x) = y$. Supposons $x_1 \leq x_2$, l'autre cas se traite de façon similaire. J'utiliserai encore une fois un argument par dichotomie. Pour suivre un tel argument, il faut faire un dessin. Je l'ai fait pour vous lorsque j'ai démontré le théorème de la borne supérieure et le théorème du maximum en utilisant une dichotomie. Cette fois-ci, je vous invite à le faire vous-même. D'ailleurs, je n'écrirai pas tous les détails du raisonnement, que vous devrez fournir par vous-même aussi. Soit donc $a_0 = x_1, b_0 = x_2$ et $c_0 = \frac{1}{2}(a_0 + b_0)$. Si $y \leq f(c_0)$, et donc $f(a_0) \leq y \leq f(c_0)$, c'est à dire si y est compris entre $f(a_0)$ et $f(c_0)$, on pose $a_1 = a_0, b_1 = c_0$. Si non, on a $f(c_0) < y \leq f(b_0)$ et on pose $a_1 = c_0, b_1 = b_0$. Dans les deux cas, on a (et c'est crucial) $f(a_1) \leq y \leq f(b_1)$. Aussi,

$$a_0 \leq a_1 \leq b_1 \leq b_0 \quad \text{et} \quad b_1 - a_1 = \frac{b_0 - a_0}{2}.$$

On peut maintenant itérer la procédure (récurrence !) pour obtenir deux suites adjacentes $(a_n), (b_n)$ ayant (donc) une limite commune x_* et telles que

$$f(a_n) \leq y \leq f(b_n).$$

Comme la fonction f est continue, on a

$$f(x_*) = \lim_{n\to\infty} f(a_n) \leq y \leq \lim_{n\to\infty} f(b_n) = f(x_*).$$

Et bingo ! On conclut que $f(x_*) = y_*$. □

Le lecteur s'entraîne :

1. a) Montrer que l'on a $\arccos(-x) + \arccos(x) = \pi$. Puis comparer les fonctions $\arcsin\sqrt{1-x^2}$ et $\arccos(x)$.

b) Montrer que l'on a $\arccos(x) + \arcsin(x) = \frac{\pi}{2}$

c) Simplifier $\arcsin\left(2x\sqrt{1-x^2}\right)$.

2. a) Montrer que l'on a, pour $x > 0$, $\arctan(x) + \arctan\left(\frac{1}{x}\right) = \frac{\pi}{2}$.

b) Exprimer $\tan 2\theta$ en fonction de $\tan\theta$. En déduire, à l'aide de la question précédente, la formule suivante : pour $x > 0$

$$2\arctan\left(\sqrt{1+x^2} - x\right) + \arctan(x) = \frac{\pi}{2}.$$

3. En étudiant la fonction définie sur $]-\infty, 1/a[$ (avec $a > 0$) par $f(x) = \arctan\left(\frac{a+x}{1-ax}\right)$, montrer que

$$\arctan x + \arctan y = \arctan\left(\frac{x+y}{1-xy}\right).$$

Application : montrer que

$$\arctan\frac{1}{2} + \arctan\frac{1}{3} = \frac{\pi}{4} \quad \text{et} \quad \arctan\frac{1}{7} + 2\arctan\frac{1}{3} = \frac{\pi}{4}$$

4. Exprimer, à l'aide de fonctions connues ($\ln x$, $\sqrt{x}$, x^2 ...), les fonctions argsh$y$, argch$y$ et argth$y$.

5. Etudier, en fonction du paramètre b, les limites en $+\infty$ des fonctions suivantes

$$\frac{(\ln x)^b}{x}, \qquad \frac{e^x}{x^b},$$

et la limite en 0 de la fonction $(\ln x)^b x$.

6. Déterminer le domaine de définition, la dérivée, le sens de variation et la limite en 0 des fonctions suivantes :

$$f(x) = x^{-\ln x}, \quad g(x) = \left(\frac{1}{\sqrt{x}}\right)^{\sqrt{x}}, \quad h(x) = e^{-x^2/2}|x|^x.$$

7. Calculer les dérivées des fonctions arctan(th x) et arctan(sh $2x$). En déduire que l'on a pour tout réel

$$2\arctan(\text{th}x) = \arctan(\text{sh}2x).$$

Le lecteur teste ses connaissances

Les barêmes sur 15 sont donnés à titre indicatif

Interrogation Ecrite TAF et Fonctions réciproques 1 – durée 1h30

I (i) [1pt] Montrer qu'il n'existe pas de fonction dérivable et strictement croissante $f : \mathbb{R} \to \mathbb{R}$ telle que $f^{-1}(x) = f(-x)$. **Indication :** Penser à dériver.

(ii) [3pt] Rappeler la définition de la fonction argsh et calculer sa dérivée. Exprimer la fonction argsh en termes de la fonction ln et de la fonction racine carrée.

(iii) [2pt] Soit $f : [1, +\infty[\to \mathbb{R}$ définie par $f(x) = x^2 \ln x$. Identifier l'image de f. Montrer que f admet une fonction réciproque dont on donnera le domaine et l'image. Tracer (qualitativement) le graphe de la fonction réciproque. Calculer

$$\lim_{y\to+\infty} (f^{-1})'(y).$$

II On veut montrer qu'il existe exactement une solution à l'équation

$$(E) \qquad \text{arctg } (2 + \cos x) = x.$$

(i) [2pt] On considére la fonction $f(x) =$ arctg $(2 + \cos x) - x$. Montrer qu'il existe $b > \pi/2$ tel que $f(b) < 0$ et qu'il existe $a < -\pi/2$ tel que $f(a) > 0$. Montrer que (E) a une solution.

(ii) [2pt] Soit $g(x) =$ arctg $(2 + \cos x)$. Montrer que

$$\forall x \in \mathbb{R}, \quad |g'(x)| \leq \frac{1}{2}.$$

(iii) [2pt] Enoncer le théorème des accroissements finis. Montrer que, quelque soit $a, b \in \mathbb{R}$, on a

$$|g(b) - g(a)| \leq \frac{1}{2}|b - a|.$$

où g est définie dans la question précédente.

(iv) [1pt] Déduire du (iii) que la solution de (E) est unique.

III Les affirmations suivantes, sont-elles vraies ou fausses ? Justifier votre réponse.

(i) [1pt] Une fonction $f : \mathbb{R} \to \mathbb{R}$ qui est injective est monotone.

(ii) [1pt] Quelque soit $x \in \mathbb{R}$, $\arcsin(\sin x) = x$.

Interrogation Ecrite TAF et Fonctions réciproques 2 – durée 1h30

I (i) [1pt] Enoncer le théorème des valeurs intermédiaires.

(ii) [1pt] L'affirmation suivante, est-elle vraie ou fausse ?

“Si une fonction continue $f : D \to \mathbb{R}$ est injective, alors elle est strictement monotone.”

II Soit $f(x) = \frac{x-2}{x^2-1}$ sur le domaine $D = \mathbb{R}^+ \setminus \{1\}$.

(i) [3pts] Calculer f'. Trouver les points où f a un extremum local. Calculer les extremas et les mettres sous la forme $a + b\sqrt{3}$, avec $a, b \in \mathbb{Q}$.

(ii) [1pt] Tracer l'allure du graphe de f.

(iii) [2pts] Montrer que, si l'on restreint x à l'intervalle $[0, 2 - \sqrt{3}]$, l'équation

$$y = \frac{x-2}{x^2-1}$$

définit x comme fonction de y. Trouver l'expression explicite de x en fonction de y.

(iv) [2pt] Sans autre calcul, répondre à la question suivante : "L'équation

$$1 = \frac{x-2}{x^2-1}$$

a-t-elle une solution ? Et l'équation

$$10 = \frac{x-2}{x^2-1}?"$$

III [3pts] Calculer la dérivée de la fonction

$$f(x) = \arctan(\sqrt{1+x^2} - x).$$

Indication : La dérivée s'exprime très simplement en termes de $1/(1+x^2)$.

Calculer la valeur de f en 0, puis tracer son graphe.

IV [2pts] Montrer que, pour tout $a \leq b$,

$$\arctan b - \arctan a \leq b - a.$$

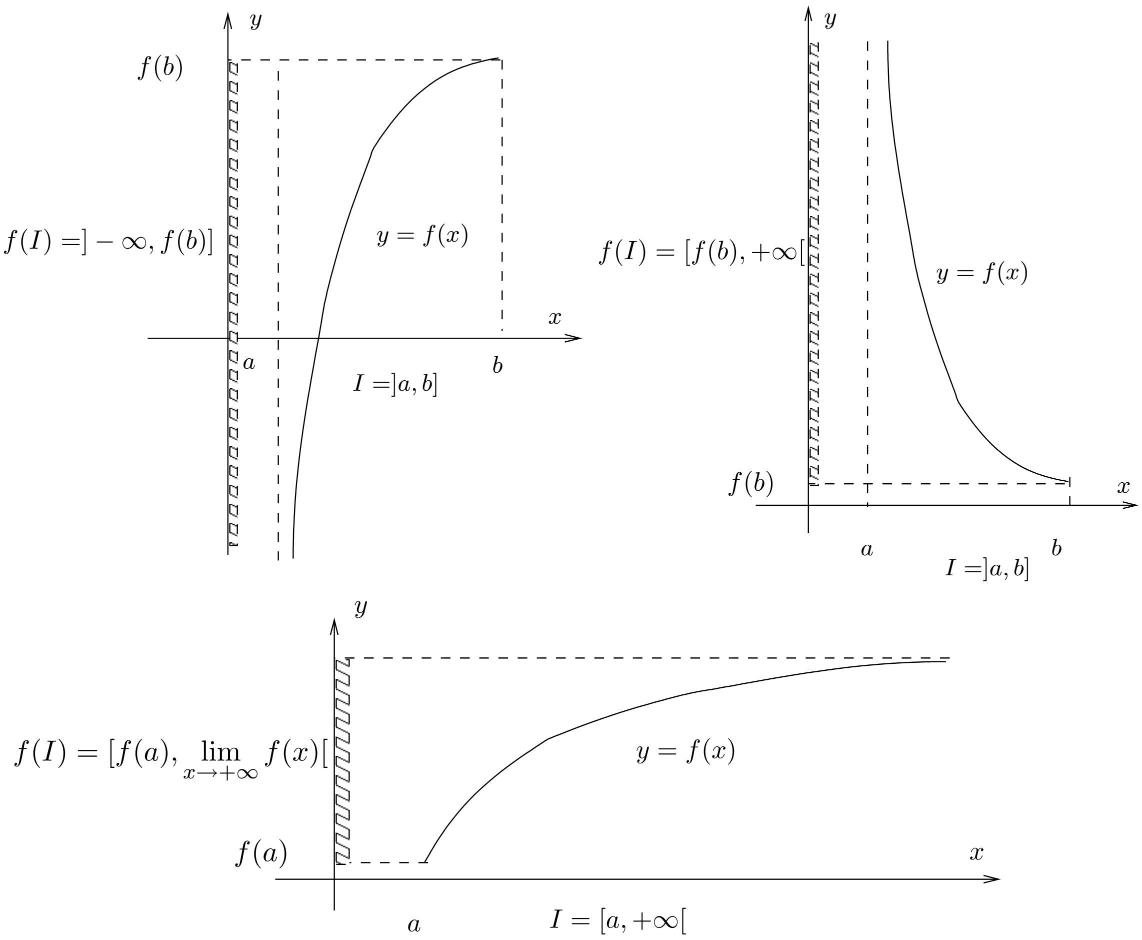

FIG. 8.5 – Images d'intervalles par quelques fonctions continues croissantes.

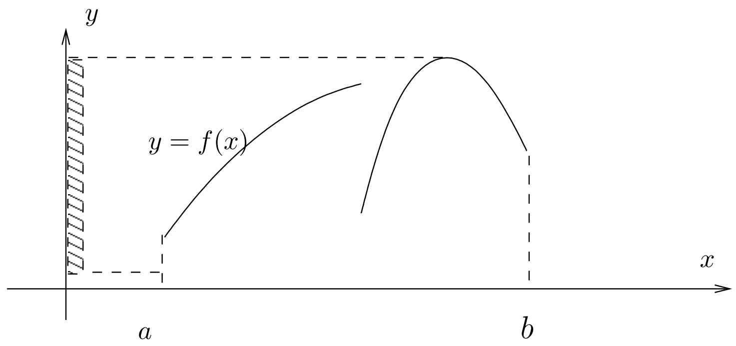

FIG. 8.6 – Voici le graphe d'une fonction discontinue définie sur un intervalle I et tel que $f(I)$ est un intervalle tout de même.

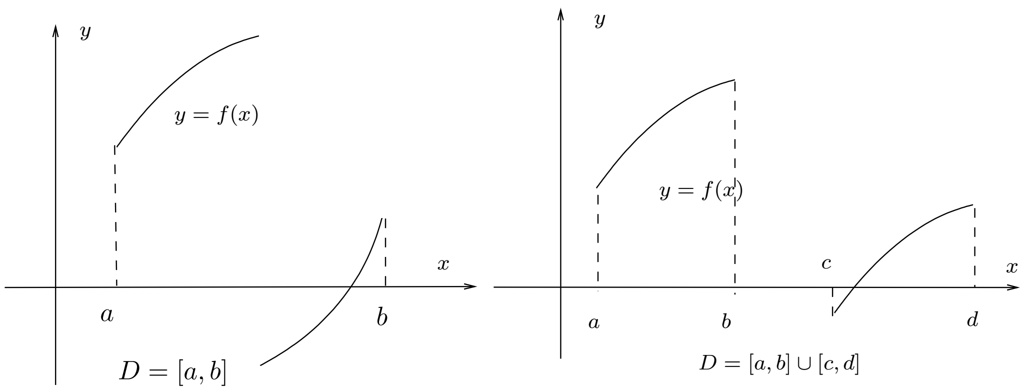

FIG. 8.7 – Ces fonctions, sont-elles continues ? Injectives ? Monotones ? Définies sur un intervalle ?

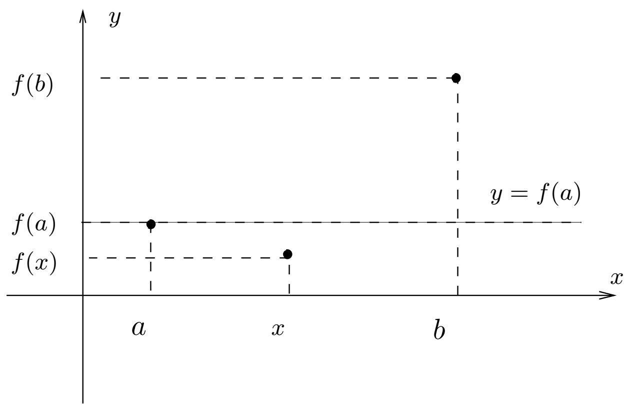

FIG. 8.8 – Entre x et b le graphe de f, que je n'ai pas dessiné, doit traverser la droite horizontale $y = f(a)$.

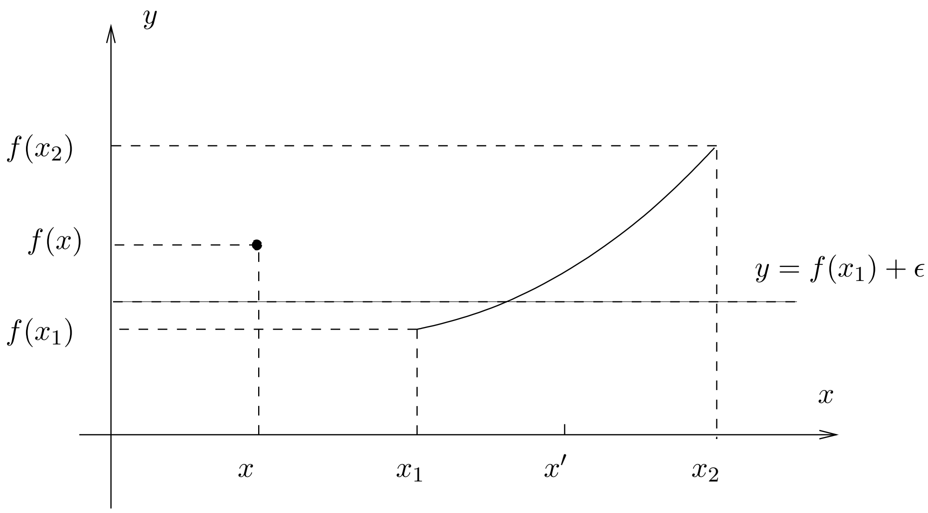

FIG. 8.9 – Ici $\alpha = x$ et $\beta = x_2$. Le graphe de f ne peut pas passer par le point $(x, f(x))$ indiqué. En effet, si non, il traverserait la droite $y = f(x_1) + \epsilon$ deux fois au moins : une fois entre x et x_1, et une deuxième entre x_1 et x_2.

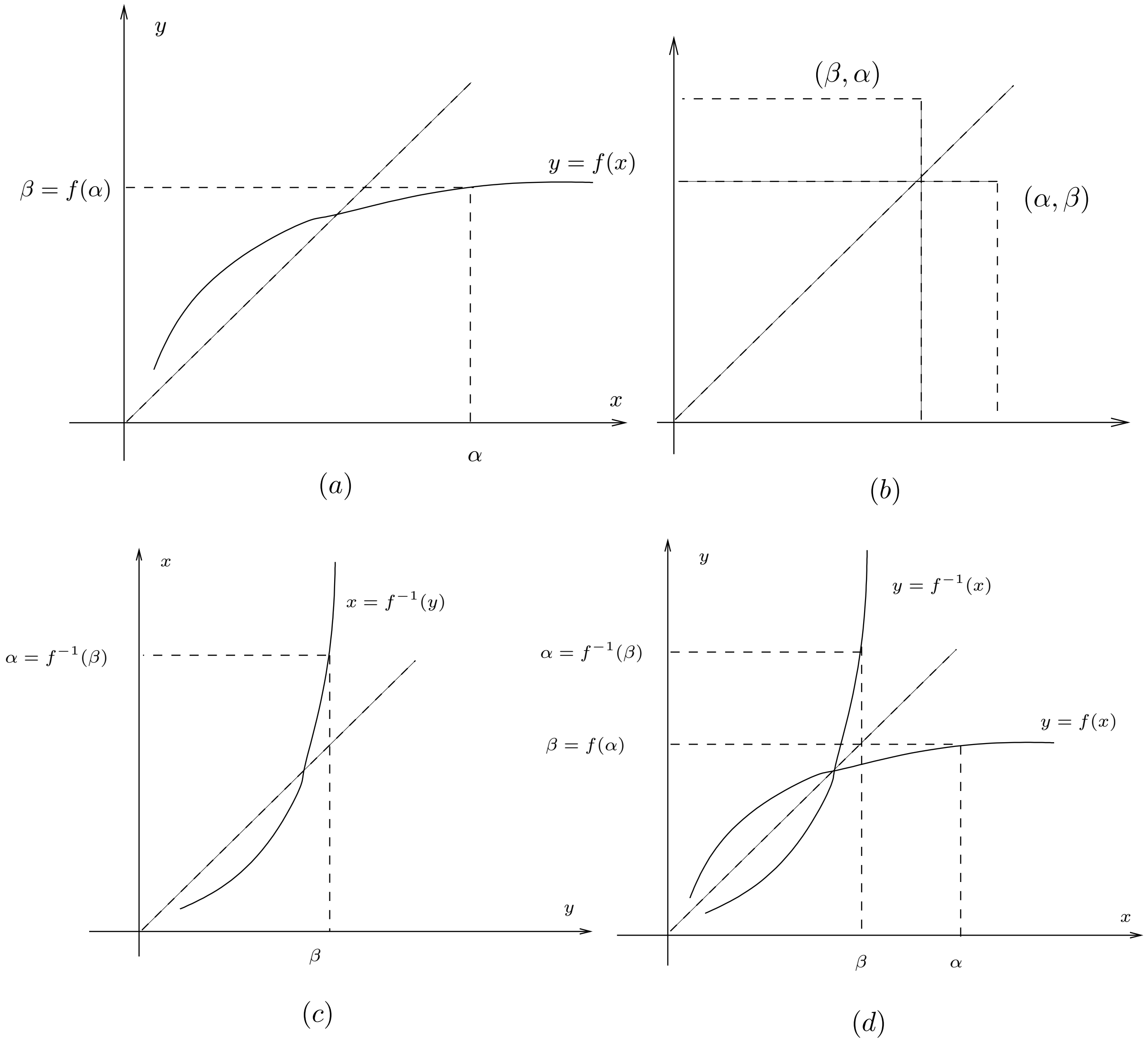

FIG. 8.10 – (a) Le graphe d'une fonction croissante. (b) Le point (α, β), et son image symétrique par rapport à la bissectrice.(c) Le graphe de f^{-1}. Attention, l'axe des y est horizontal. (d) Les deux graphes ensemble. Attention, j'ai changé le nom de la variable de la fonction réciproque : elle s'appelle x aussi !!!

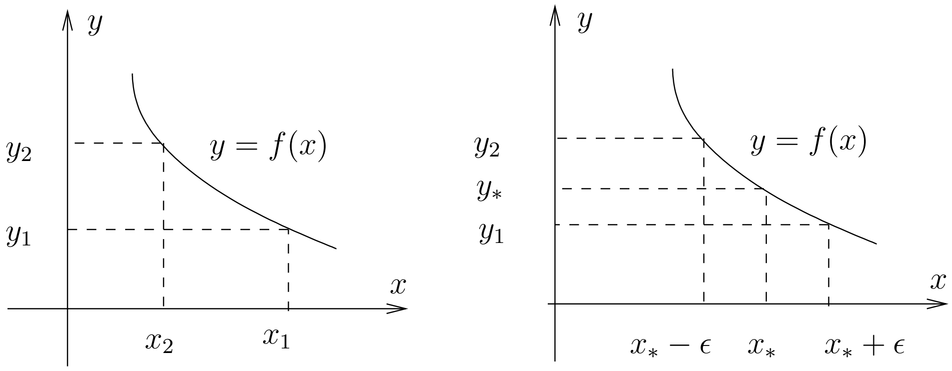

FIG. 8.11 – Monotonie et continuité de la fonction réciproque

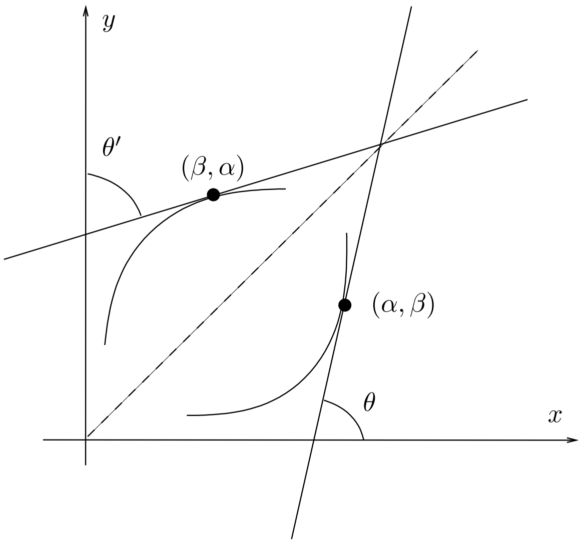

FIG. 8.12 – Comprendre géométriquement la formule pour la dérivée de f^{-1}.

Chapitre 9

Les nombres : au delà du rationnel

Publié dans :
« L'oral du Capes de mathématiques : Face au jury »(Ellipses 2007).

S. De Bièvre

Chapitre 10

Le nombre complexe : au delà du réel

Pense, ne te fie pas à ton instinct.
d'après Qui-Gon Jinn

10.1 Introduction

Comme le carré de tout nombre réel est positif, l'équation

$$x^2 + 1 = 0 \tag{10.1}$$

n'admet évidemment pas de solution x appartenant à $\mathbb{R}$. Plus généralement, lorsque $a, b, c \in \mathbb{R}, a \neq 0$, l'équation

$$ax^2 + bx + c = 0,$$

admet des solutions réelles si et seulement si $b^2 - 4ac \geq 0$; en effet elle peut être réécrite

$$a(x + \frac{b}{2a})^2 + (c - \frac{b^2}{4a}) = 0 \text{ ou } (x + \frac{b}{2a})^2 = \frac{1}{4a^2}(b^2 - 4ac).$$

Ceci suggère d'élargir le concept de *nombre* de façon à remédier à ce problème. Cette démarche, que j'expliquerai en détail dans la section suivante, ne doit plus vous paraître bizarre, puisqu'elle vous est déjà familière de la Section 1.7. En effet, nous avons remarqué d'abord que l'équation

$$x + 1 = 0$$

elle aussi n'a pas de solutions, si on restreint le concept de nombre à celui de nombre entier naturel : il n'y a pas de x appartenant à $\mathbb{N}$ telle que $x + 1$ vaut zéro. Or, au collège vous avez appris qu'il suffit d'introduire les nombres entiers négatifs pour résoudre ce problème. De même, un peu plus tard, on vous a présenté l'ensemble $\mathbb{Q}$ des nombres rationnels, dans lequel on peut résoudre toute équation du type $ax + b = 0$, avec les coefficients a et b eux-mêmes rationnels. Finalement, nous avons vu qu'il n'existe pas de nombre rationnel x dont le carré vaut 2, ce qui veut dire que l'équation

$$x^2 - 2 = 0$$

n'a pas de solution rationnelle. Cette observation nous a servi de motivation pour l'introduction de l'ensemble des nombres réels et nous avons vu qu il existe un unique nombre réel positif dont le carré vaut 2, et qui n'est pas rationnel.

Si vous vous y arrêtez un moment, vous serez obligé d'être d'accord avec moi que le concept de nombre négatif n'a déjà rien d'évident. Celui de nombre irrationnel l'est encore moins, le Chapitre 9 est là pour en témoigner. Néanmoins, vous avez aujourd'hui une certaine familiarité avec ces concepts, au point peut-être d'avoir la (fausse) impression qu'il s'agit là de choses simples. Mon but dans ce chapitre est d'élargir une dernière fois le concept de nombre afin de vous présenter le concept de nombre complexe, qui englobe celui de nombre réel. Nous verrons en particulier que dans l'ensemble $\mathbb{C}$ des nombres complexes (qui contient donc celui des réels $\mathbb{R}$) toute équation quadratique admet deux solutions et que, plus généralement, toute équation polynomiale de degré n admet n solutions. J'espère vous convaincre que le concept de nombre complexe n'est – en dépit de son nom évocateur – rien de bien compliqué.

J'ai motivé l'introduction des nombres complexes ici en disant qu'ils fournissent un cadre pour la résolution des équations quadratiques. Je ne suis pas tout à fait sûr qu'ils figureraient au programme de DEUG s'ils ne servaient qu'à cela. Il s'avère que les nombres complexes forment un outil redoutable en analyse, et pour les sciences de l'ingénieur, et je tenterai de donner une petite idée de leur efficacité dans ce contexte dans le Chapitre **??**.

10.2 Le plan complexe

10.2.1 Définition

Il y a trois opérations que vous avez appris à exécuter avec les nombres, qu'ils soient entiers, rationnels ou réels : les ajouter, les multiplier et les comparer. Je vais maintenant vous présenter les nombres complexes, et montrer comment on les ajoute et multiplie : on verra aussi qu'on ne peut pas les comparer.

Considérons l'ensemble $\mathbb{R}^2$ des couples (x, y) de nombres réels, que l'on peut représenter de la façon habituelle en choisissant deux axes perpendiculaires et une origine. Sur $\mathbb{R}^2$ on définit alors le produit suivant, que j'appellerai le produit complexe :

$$(x, y) \cdot (x', y') = (xx' - yy', xy' + x'y). \tag{10.2}$$

En d'autres termes, étant donnés deux points (x, y) et (x', y') dans $\mathbb{R}^2$, on en construit un troisième, noté $(x, y) \cdot (x', y')$, et défini par (10.2). La formule (10.2)

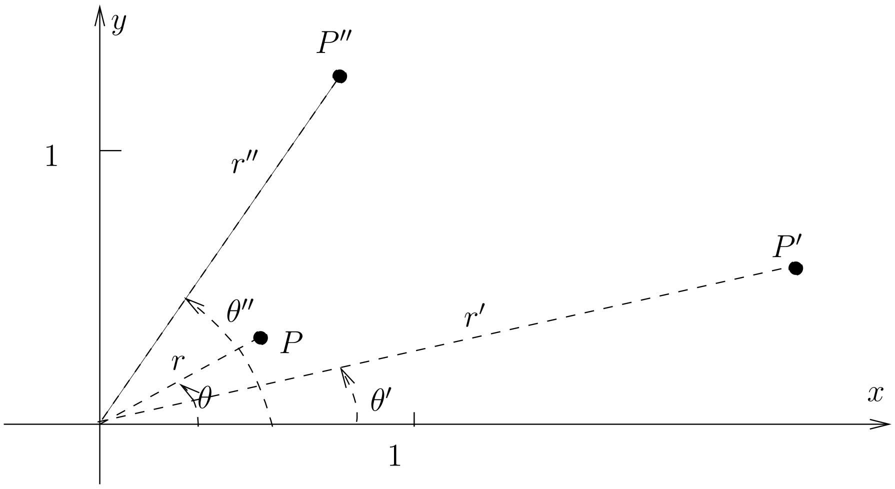

FIG. 10.1 – La représentation géométrique du produit complexe

est à première vue étrange, même si elle est très simple. Pour la démystifier un peu, remarquons d'abord que le troisième point $(x'', y'') = (x, y) \cdot (x', y')$ peut facilement être construit graphiquement de la façon suivante (Fig. 10.1). En introduisant les coordonnées polaires (r, θ) de (x, y) via $x = r\cos\theta, y = r\sin\theta$, et pareillement pour $(x', y'), (x'', y'')$, on démontre à partir de (10.2) que

$$r'' = rr', \theta'' = \theta + \theta'. \tag{10.3}$$

En effet, en utilisant les identités trigonométriques

$$\cos(\theta + \theta') = \cos\theta\cos\theta' - \sin\theta\sin\theta', \tag{10.4}$$
$$\sin(\theta + \theta') = \cos\theta\sin\theta' + \sin\theta\cos\theta' \tag{10.5}$$

on voit aisément que

$$xx' - yy' = rr'(cos\theta\cos\theta' - \sin\theta\sin\theta') = rr'\cos(\theta + \theta'), etc.,$$

d'où le résultat suit. Etant donnés deux points de coordonnées (x, y) et (x', y'), on construit donc le troisième en remarquant qu'il est situé sur l'axe faisant un angle $\theta + \theta'$ avec l'axe des x à une distance rr' de l'origine. On en conclut en particulier que, si $r' = 1$, alors multiplier par (x', y') revient à tourner dans le plan sur un angle θ'. Le plan $\mathbb{R}^2$, équipé avec cette multiplication complexe, et avec l'addition habituelle $((x, y) + (x', y') = (x + x', y + y'))$, est appelé le *plan complexe*, que l'on désigne par $\mathbb{C}$, et ses points des *nombres complexes*.

Il est à peu près clair à partir de ce qui précède qu'on ne peut pas dire qu'un nombre complexe (x, y) est plus grand ou plus petit qu'un autre (x', y'). Cette notion n'a pas de sens (ou, plus précisément, ne peut pas être définie de façon utile) pour des points dans le plan.

10.2.2 Propriétés élémentaires – notations utiles

Avant d'expliquer comment le produit complexe résout le problème posé au début du chapitre, il vaut mieux introduire des notations qui facilitent le calcul avec les nombres complexes. Dans ce but, il faut remarquer les propriétés suivantes du produit complexe, qui se vérifient par de simples calculs à partir de la définition (10.2). D'abord, l'ordre dans lequel les facteurs sont placés dans la multiplication est sans incidence sur le résultat :

$$(x, y) \cdot (x', y') = (x', y') \cdot (x, y).$$

On dit que le produit complexe est *commutatif.* De même, le produit complexe est *associatif,* ce qui veut dire que , pour tout $(x, y), (x', y'), (x'', y'')$ dans $\mathbb{R}^2$, on a

$$\big((x, y) \cdot (x', y')\big) \cdot (x'', y'') = (x, y) \cdot \big((x', y') \cdot (x'', y'')\big),$$

ce que vous vérifierez facilement à partir de la définition. Il est aussi *distributif* par rapport à l'addition :

$$(x, y) \cdot \big((x', y') + (x'', y'')\big) = (x, y) \cdot (x', y') + (x, y) \cdot (x'', y'').$$

On remarque finalement encore que

$$(x, y) \cdot (1, 0) = \quad (x, y), \tag{10.6}$$
$$(x, 0) \cdot (x', 0) = \quad (xx', 0), \tag{10.7}$$
$$(0, 1) \cdot (y, 0) = \quad (0, y). \tag{10.8}$$

De (10.7) on remarque que la multiplication (respectivement l'addition) des points $(x, 0)$ et $(x', 0)$ sur l'axe des x donne le point $(xx', 0)$ (respectivement $(x+x', 0)$) sur le même axe, ce qui suggère d'identifier cet axe avec les nombres réels, et d'écrire simplement x, plutôt que $(x, 0)$. C'est dans ce sens que l'ensemble des réels est un sous-ensemble de l'ensemble des nombres complexes. Par ailleurs, on a grâce à (10.8)

$$(x, y) = (x, 0) + (0, y) = (x, 0) + (0, 1) \cdot (y, 0),$$

ce qui se réécrit donc, utilisant la notation simplifiée que je viens d'introduire,

$$(x, y) = x + (0, 1) \cdot y. \tag{10.9}$$

Puisque, comme on le verra par la suite, le point $(0, 1)$ joue un rôle important, on lui donne un nom. On écrit

$$i = (0, 1) \tag{10.10}$$

de façon à ce que (10.9) devienne

$$(x, y) = x + iy, \tag{10.11}$$

où j'ai de surcroît adopté la convention habituelle qui consiste à ne pas écrire le $\cdot$ si ce n'est pas strictement nécessaire. Plutôt que d'écrire (x, y) pour les élements du plan complexe, on les désigne le plus souvent par la seule lettre z, ce qui donne $z = (x, y)$. Pour les raisons évoquées plus haut, on dit que x est la *partie réelle* de z (notée Re z). Par ailleurs, on appelle y la *partie imaginaire* du nombre complexe z (notée Im z).

Remarquons finalement que

$$(0,1) \cdot (0,1) = (-1,0), \tag{10.12}$$

ce qui se réécrit avec les notations introduites comme

$$i \cdot i = i^2 = -1.$$

Du coup, il est clair que l'équation quadratique

$$z^2 + 1 = 0$$

a deux solutions dans le plan complexe, à savoir i et $-i$. C'est dans ce sens que la *racine carré de moins un*, dont on vous a dit pendant des années qu'elle n'existe pas *en tant que nombre réel*, existe bel et bien *en tant que nombre complexe*.

Le nombre $(1, 0) = 1$ joue, au vu de (10.6) aussi un rôle particulier : multiplier un nombre complexe par $(1, 0)$ ne le change pas. Ceci pose la question de l'existence d'une inverse pour chaque z en $\mathbb{C}$: étant donné $z = x + iy$, existe-t-il un $z' = x' + iy'$ tel que

$$z \cdot z' = 1?$$

Un calcul simple montre que

$$z \cdot z' = 1 \iff xx' - yy' = 1 \text{ et } xy' + yx' = 0.$$

Ces deux équations linéaires en deux inconnues x' et y' ont une solution unique donnée par

$$x' = x/(x^2 + y^2)^{1/2}, \qquad y' = -y/(x^2 + y^2)^{1/2}, \tag{10.13}$$

pourvu que $(x, y) \neq (0, 0)$. On écrira z^{-1} ou encore $\frac{1}{z}$ pour l'inverse de z.

Associés à chaque nombre complexe z sont son *complexe conjugué* $\bar{z}$, défini par

$$\bar{z} = x - iy,$$

et son *module*, défini par

$$|z| = \sqrt{\bar{z} \cdot z}.$$

On constate que

$$|z| = |\bar{z}|, \qquad |z_1 z_2| = |z_1||z_2|, \qquad |z^{-1}| = \frac{1}{|z|}.$$

On calcule facilement le module de z en termes de sa partie réelle et imaginaire :

$$|z| = \big((x + iy)(x - iy)\big)^{1/2} = \sqrt{x^2 + y^2}.$$

En coordonnées polaires, on a donc

$$|z| = r.$$

Comme vous voyez (j'espère), la notion de nombre *complexe* n'a donc en effet rien de mystérieux, et en fait, la construction des nombres complexes à partir des nombres réels est bien plus simple que celle des réels à partir des rationnels. Il me semble plus facile de comprendre la construction de i, la racine carré de -1, esquissée ci-dessus, que d'appréhender celle d'un nombre dont le carré vaut 2, et qui ne peut être de la forme $\frac{p}{q}$, avec $p, q \in \mathbb{N}$. Chaque fois que vous hésitez sur la signification de i, il faut revenir à (10.2), (10.10) et (10.12), et se dire que i n'est rien d'autre que le point $(0, 1)$ du plan $\mathbb{R}^2$, équipé avec un produit bizarre, donné par (10.2).

Une bonne notation en est une qui permet de calculer sans trop réfléchir. Voyons si celle introduite ci-dessus satisfait à ce critère. Soient $(5, 2)$ et $(6, 4)$ deux nombres complexes, et calculons, suivant (10.2)

$$(5, 2) \cdot (6, 4) = (30 - 8, 20 + 12) = (22, 32).$$

Dans les nouvelles notations, ceci devient

$$(5 + 2i)(6 + 4i) = 30 + 12i + 20i + 8i^2 = 22 + 32i,$$

où j'ai, sans trop y réfléchir, utilisé les propriétés de commutativité, d'associativité et de distributivité énoncées plus haut ainsi que l'identité cruciale $i^2 = -1$.

On peut aussi facilement retrouver la formule pour l'inverse de z, introduite dans la section précédente, en remarquant que la définition du module de z implique que

$$\frac{\bar{z}}{|z|^2} \cdot z = 1,$$

de façon à ce que

$$z^{-1} = \frac{\bar{z}}{|z|^2},$$

ce qui est à comparer avec (10.13).

Il est également utile de refaire dans les nouvelles notations le calcul menant à (10.3). On a

$$\begin{aligned} z \cdot z' &= rr'(\cos\theta + i\sin\theta)(\cos\theta' + i\sin\theta') \\ &= rr'(\cos(\theta + \theta') + i\sin(\theta + \theta')). \end{aligned}$$

On en tire facilement, en itérant,

$$(\cos\theta + i\sin\theta)^n = \cos n\theta + i\sin n\theta,$$

pour tout $n \in \mathbb{N}$: c'est la formule de Moivre.

Le lecteur s'entraîne :

1. Soient z et z' deux nombres complexes distincts, et tels que $|z| = |z'| = r \neq 0$. Montrer que

$$\frac{r^2 - zz'}{z - z'} \in \mathbb{R}.$$

2. Montrer que, pour tout $z_1, z_2, z_3 \in \mathbb{C}$, on a

$$|z_1 + z_2| \leq |z_1| + |z_2|, \qquad |z_1 - z_3| \leq |z_1 - z_2| + |z_2 - z_3|.$$

Interpréter cette dernière inégalité géométriquement.

3. Montrer que, quelque soient $z, z' \in \mathbb{C}$,

$$zz' = 0 \Rightarrow z = 0 \text{ ou } z' = 0.$$

4. Démontrer la formule de Moivre.

10.3 La fonction exponentielle complexe

Soit Ω un sous-ensemble de $\mathbb{C}$. Une fonction complexe f d'une variable complexe appartenant à Ω est une règle qui associe à chaque élément z de Ω un nombre complexe $f(z)$. Une fonction complexe est donc une fonction, telle que j'ai défini cette notion dans le Chapitre 3.

Les polynômes et les fractions rationnelles sont – comme dans le cas des fonctions numériques d'une variable réelle – les exemples les plus simples et les plus immédiats de fonctions complexes d'une variable complexe :

$$f(z) = (3 + 2i)z^2 + \pi z + (exp\pi + i\sqrt{2})$$

est un polynôme d'ordre 2, à coefficients complexes, défini pour tout $z \in \mathbb{C}$. De même

$$f(z) = \frac{(3 + 2i)z^2 + \pi z + sine}{z^2 + 1}$$

est une fraction rationnelle, définie en tout point $z \in \mathbb{C}, z \neq \pm i$.

La plus importante des fonctions complexes est néanmoins sans doute l'omniprésente fonction *exponentielle*, définie de la façon suivante :

Définition 10.1. $\exp : \mathbb{C} \to \mathbb{C}$ *est la fonction définie pour tout* $z = x + iy \in \mathbb{C}$ *par*

$$\exp z = (\exp x)(\cos y + i \sin y). \qquad (10.14)$$

Remarquons que, si $z = x + i0$, alors on a bien $\exp z = \exp x$, donc la définition choisie étend la fonction exponentielle de son domaine de définition original, à savoir l'ensemble des nombres réels à celui des nombres complexes.

Je ne suis pas, pour le moment, en mesure de vous montrer pourquoi cette fonction est tellement importante (Nous y verrons plus clair dans le Chapitre **??**), mais je peux toutefois vous donner une première petite idée de l'origine de la définition ci-dessus. J'ai déjà longuement insisté sur l'importance de la fonction exponentielle $\exp x$, lorsque x est un nombre réel. On se souviendra qu'une des propriétés cruciales de l'exponentielle est que $\exp(x_1 + x_2) = \exp x_1 \exp x_2$. Essentiellement, la formule (10.14) a été retenu comme définition de l'extension de la fonction exponentielle aux nombres complexes parce qu'elle implique la propriété suivante :

Proposition 10.2. *Quelque soit* $z_1, z_2 \in \mathbb{C}$,

$$\exp(z_1 + z_2) = \exp z_1 \exp z_2. \tag{10.15}$$

Démonstration : Il suffit de calculer :

$$\begin{aligned}
\exp z_1 \exp z_2 &= \exp x_1 \exp x_2 \,(\cos y_1 + i \sin y_1)\,(\cos y_2 + i \sin y_2) \\
&= \exp x_1 \exp x_2 ((\cos y_1 \cos y_2 - \sin y_1 \sin y_2 \\
&\qquad + i(\cos y_1 \sin y_2 + \sin y_1 \cos y_2)) \\
&= \exp(x_1 + x_2)\,(\cos(y_1 + y_2) + i \sin(y_1 + y_2)) \\
&= \exp(z_1 + z_2).
\end{aligned}$$

Remarquez que ce résultat est une conséquence immédiate des formules trigonométriques pour le cosinus et le sinus de la somme de deux angles.

Etant donné (10.15), personne ne s'étonnera plus, j'espère, qu'on utilise également la notation

$$e^z = \exp z.$$

Je pense que vous serez aussi d'accord pour dire qu'une définition de $\exp z$ qui ne satisferait pas à (10.15) ne serait pas acceptable. En effet, la notation exp évoque automatiquement cette propriété et il serait malsain d'utiliser cette notation pour une fonction ne l'ayant pas.

Dans le cas où $z = iy$ est un nombre imaginaire, la définition (10.14) devient

$$e^{iy} = \exp iy = \cos y + i \sin y. \tag{10.16}$$

Ceci permet de réécrire un nombre complexe z quelconque en termes de ces coordonnées polaires de la façon suivante. Soit $z = x + iy \neq 0$ un point du plan complexe de coordonnées polaires $r > 0$ et $\theta \in [0, 2\pi[$, alors on a

$$z = x + iy = r(\cos\theta + i \sin\theta) = re^{i\theta}.$$

On appelle θ *l'argument* de z. Le calcul du produit donne ainsi

$$z \cdot z' = (re^{i\theta}) \cdot (r'e^{i\theta'}) = rr'e^{i(\theta+\theta')},$$

où, utilisant (10.15), j'ai retrouvé sans peine (10.3).

Comme cas particuliers, on a ainsi

$$e^{i\pi} = -1, \quad e^{i\frac{\pi}{2}} = i, \quad e^{2i\pi} = 1.$$

Ces formules semblent assez mystérieuses et ont beaucoup étonné les mathématiciens du 18-ième et 19-ième siècles. Elles semblaient établir des liens plutôt magiques et incompréhensibles entre des nombres aussi importants que π, e et i. En particulier, si on pense à e^3 comme "le produit de e trois fois avec lui-même", et qu'on essaie alors de voir $e^{i\pi}$ comme "le produit de e $i\pi$ fois avec lui-même", on ne peut pas espérer comprendre comment cela peut valoir -1. Pour les étudiants aussi, la manipulation d'expressions contenant $\exp i\theta, \exp it$ ou $\exp i\phi$ relève au départ de la sorcellerie. Si vous vous souvenez de la définition (10.16), le mystère se dissipera rapidement, et vous comprendrez alors, à travers les multiples applications, l'efficacité extraordinaire du calcul avec les nombres complexes et avec la fonction exponentielle.

Lemme 10.3. *Soient $z, z' \in \mathbb{C}$. Alors $\exp z = \exp z'$ si et seulement si il existe $k \in \mathbb{Z}$ tel que*

$$z' = z + 2\pi k i.$$

En particulier, quelque soit $\phi, \phi' \in \mathbb{R}$,

$$e^{i\phi'} = e^{i\phi} \Leftrightarrow \exists k \in \mathbb{Z}, \phi' = \phi + 2\pi k. \tag{10.17}$$

En d'autres termes, le lemme affirme que la fonction exponentielle a une période purement imaginaire donnée par $2\pi i$. Elle n'est donc pas du tout injective, comme la fonction exponentielle réelle ! C'est surtout (10.17) qui s'avère souvent utile dans les applications.

Démonstration : Comme

$$\exp(x+iy) = \exp x(\cos y + i \sin y), \text{ et } \exp(x'+iy') = \exp x'(\cos y' + i \sin y')$$

on constate que $|z| = |z'|$ et donc que $\exp x = \exp x'$ ce qui implique $x = x'$. Puis, en égalisant les parties imaginaires et réelles de $\exp z$ et de $\exp z'$, on trouve

$$\cos y = \cos y', \qquad \sin y = \sin y',$$

d'où un peu de trigonométrie élémentaire permet de conclure qu'il existe $k \in \mathbb{Z}$ tel que

$$y' = y + 2\pi k,$$

ce qui montre que $z' = z + 2\pi k i$; (10.17) est alors immédiat.

Comme dernière remarque, je vous offre en cadeau l'observation suivante. Si vous vous souvenez de

$$\exp i(\theta + \theta') = \exp i\theta \exp i\theta',$$

– et ce serait tout de même très difficile de l'oublier, même en essayant – et de (10.16), vous pouvez vous permettre d'oublier les formules trigonométriques (10.4)-(10.5) ! En effet, elles en sont une conséquence facile, comme vous vérifierez sans problème.

On définit maintenant facilement les fonctions $\sin z, \cos z, \sinh z$ et $\cosh z$:

$$\begin{aligned}
\sin z &= \tfrac{1}{2i}(\exp iz - \exp -iz),\\
\cos z &= \tfrac{1}{2}(\exp iz + \exp -iz)\\
\sinh z &= \tfrac{1}{2}(\exp z - \exp -z),\\
\cosh z &= \tfrac{1}{2}(\exp z + \exp -z).
\end{aligned}$$

Celaa donne en particulier aussi :

$$\sin iz = i \sinh z \text{ et } \cos iz = \cosh z.$$

On s'étonnera maintenant moins des analogies surprenantes entre le sinus, le cosinus, et leurs cousins hyperboliques, qu'on avait rencontrées dans la Section 8.8

Le lecteur s'entraîne :

1. On considère l'application (ou, si vous préférez, la fonction complexe) $f : \mathbb{C}\backslash\{2\} \longrightarrow \mathbb{C}$, définie, pour tout $z \neq 2$, par

$$f(z) = \frac{z-(1+i)}{z-2}.$$

a) Calculer la partie réelle et la partie imaginaire de $f(-i)$.

b) Interpréter géometriquement le module et l'argument de $f(z)$.

c) Déterminer l'ensemble des complexes $z \in \mathbb{C}$ tels que $|f(z)| = 1$, puis tel que $f(z)$ est un imaginaire pur.

2. (a) Calculer, en fonction de θ, les sommes suivantes :

$$C(\theta) = \sum_{k=0}^{N} \cos(k\theta) \quad \text{ et } \quad S(\theta) = \sum_{k=0}^{N} \sin(k\theta).$$

Indication : Penser à calculer

$$\sum_{k=1}^{N} e^{ik\theta}$$

en remarquant que c'est une somme géométrique. Puis, étudier sa partie réelle et imaginaire.

(b) Etudier le graphe de $C(\theta), S(\theta)$.

3. Soit $\alpha \in]-\pi/2, \pi/2[$. On considère l'équation (E) suivante, d'inconnue complexe z :

$$(E) \quad (1+iz)^3(1-i\tan\alpha) = (1-iz)^3(1+i\tan\alpha).$$

a) Soit z une solution de (E). Montrer que $|1+iz| = |1-iz|$. En déduire que z est réel.

b) Exprimer $\frac{1+i\tan\alpha}{1-i\tan\alpha}$ en fonction de $e^{i\alpha}$.

c) Résoudre (E) en posant $z = \tan\varphi$, $\varphi \in]-\pi/2, \pi/2[$, et en justifiant ce changement de variable.

10.4 Résoudre les équations quadratiques

J'ai commencé ce chapitre en me plaignant parce que certaines équations quadratiques $ax^2 + bx + c = 0$, avec $a, b, c \in \mathbb{R}$ n'ont pas de solution réelle. J'ai alors introduit les nombres complexes, et j'ai constaté que maintenant certaines équations ont des solutions complexes, comme par exemple l'équation $z^2+1=0$ qui a en effet deux solutions complexes $\pm i$, tandis que $x^2+1=0$ n'en avait pas de réelles. Mais qu'en est-il maintenant du cas général

$$az^2 + bz + c = 0, a, b, c \in \mathbb{C}, a \neq 0? \tag{10.18}$$

On a le résultat suivant.

Lemme 10.4. *L'équation (10.18) a exactement deux solutions complexes distinctes (appelées racines de l'équation) lorsque $\Delta = b^2 - 4ac \neq 0$. Si $\Delta = 0$, elle en a une seule.*

Je rappelle que Δ s'appelle le discriminant de l'équation. Il est possible et même assez facile de donner des expressions explicites pour les racines, mais c'est sans utilité. Je préfère vous montrer comment on trouve les solutions. Pour cela remarquons d'abord que l'équation (10.18) est équivalente à (c'est à dire a exactement les mêmes solutions que) l'équation :

$$a(z + \frac{b}{2a})^2 + c - \frac{b^2}{4a} = 0 \tag{10.19}$$

que je préfère réécrire encore de la façon suivante :

$$w^2 = \Delta, w = 2a(z + \frac{b}{2a}). \tag{10.20}$$

Le problème est donc réduit à celui de trouver les solutions de $w^2 = \Delta$, c'est à dire de trouver ce qu'on appelle les racines carrés de Δ. Regardons un exemple et résolvons

$$z^2 + 2iz + (1 + 3i) = 0, \tag{10.21}$$

que je réécris comme ci-dessus :

$$w^2 = -8 - 12i.$$

Posant $w = x + iy$, on tire de cette dernière équation (en identifiant les parties réelles et imaginaires) deux équations pour les deux inconnues x, y :

$$x^2 - y^2 = -8, \quad 2xy = -12.$$

Ces équations suffisent à trouver x, y, mais il est nettement plus commode de remarquer que, par ailleurs, $|w|^2 = |8 + 12i|$, et donc qu'on a une troisième équation :

$$x^2 + y^2 = \sqrt{4^2(4+9)} = 4\sqrt{13}.$$

De la première et la troisième équation, on trouve facilement x^2 et y^2 :

$$x^2 = 2\sqrt{13} - 4, \quad y^2 = 2\sqrt{13} + 4.$$

En remarquant que $xy < 0$ (parce que $2xy = -12$), on voit que x et y sont de signe opposé, c'est à dire que les deux solutions recherchées se trouvent dans le deuxième ou le quatrième quadrant du plan. On a

$$w_1 = \sqrt{2\sqrt{13} - 4} - \sqrt{2\sqrt{13} + 4}\ i, \quad w_2 = -w_1.$$

Finalement, les deux solutions de (10.21) sont

$$z_1 = -i + w_1/2, z_2 = -i + w_2/2.$$

On peut mener à bien le calcul ci-dessus exactement de la même façon pour n'importe quelle équation quadratique (et il faut savoir le faire !) Il est néanmoins instructif de le réécrire d'une façon différente, qui permet de comprendre mieux ce qui se passe géométriquement.

Considérons donc à nouveau léquation

$$w^2 = \Delta, \tag{10.22}$$

avec $\Delta \neq 0$. On a alors $\Delta = r_* \exp(i\theta_*), \theta_* \in [0, 2\pi)$. On pose $w = r\exp(i\theta)$ et on recherche donc r et θ. En d'autres termes, plutôt que de chercher les parties imaginaire et réélle de w, je vais chercher son module r et son argument θ. On a

$$r^2 \exp(2i\theta) = r_* \exp(i\theta_*).$$

On en conclut immédiatement que $r = \sqrt{r_*}$ et donc

$$\exp(2i\theta) = \exp(i\theta_*),$$

d'où l'on conclut, via (10.17), qu'il existe $k \in \mathbb{Z}$ tel que $2\theta = \theta_* + 2\pi k$, ou encore que $\theta = \theta_k = \frac{\phi_*}{2} + \pi k$. Selon ce raisonnement, les solutions de l'équation sont donc *à priori* ($k \in \mathbb{Z}$)

$$w_k = \sqrt{r_*} \exp(i\frac{\theta_*}{2}) \exp(i\pi k).$$

Comme $\exp(i\pi k) = (-1)^k$ on en conclut qu'il n'y a que deux solutions différentes, $w_0 = \sqrt{r_*} \exp(i\frac{\theta_*}{2}), w_1 = -w_0$. On voit maintenant comment construire géométriquement les racines carrés d'un nombre complexe Δ quelconque donné. L'argument de la première racine w_0 est la moitié de celui de Δ et elle est à une distance $\sqrt{|\Delta|}$ de l'origine. La deuxième est placée symétriquement par rapport à l'origine (Fig. 10.2). Cela paraît presque plus simple que la solution en termes de la partie réelle et de la partie imaginaire. Mais attention ! Il est rare qu'on puisse trouver très explicitement l'argument ϕ_* de Δ. Si $\Delta = 1 + i$, c'est simple, mais si $\Delta = 11 + 12i$, c'est moins clair . . . . En effet, dire que $\phi_* = \arctan \frac{12}{11}$ est correct, mais pas très explicite. Donc, si vous avez besoin des parties réelle et imaginaire des racines de Δ, il vaut mieux passer par le premier calcul ci-dessus. Attention ! Lorsque a est un nombre réel positif, on utilise la notation $\sqrt{a}$ ou $a^{1/2}$ pour désigner l'unique racine carré *positif* de a. Lorsque Δ est un nombre

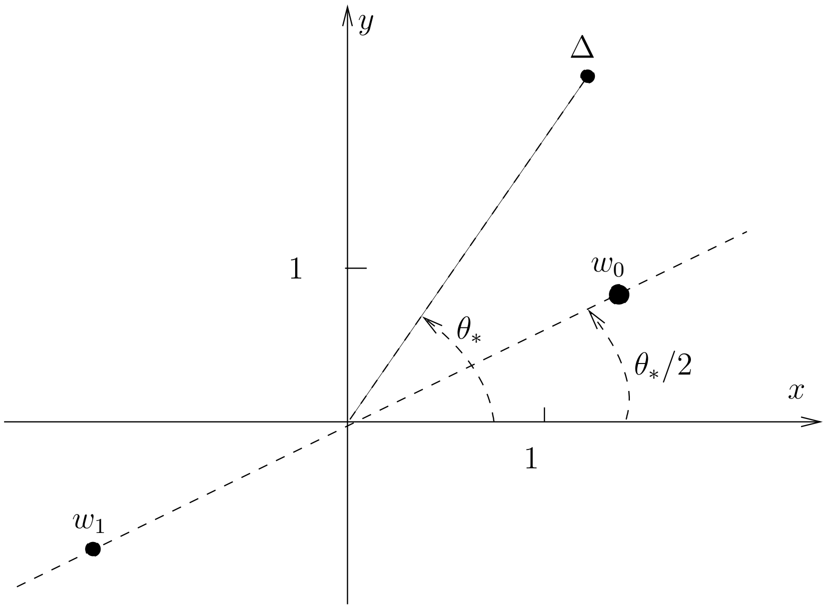

FIG. 10.2 – Les deux racines $w_0, w_1 = -w_0$ de l'équation $z^2 = \Delta$.

complexe quelconque, la notation $\sqrt{\Delta}$ est ambiguë, et donc à proscrire. En effet, Δ a deux racines complexes dont, en général aucune n'est un réel positif – comme on vient de le voir – et la notation n'indique pas de laquelle des deux elle parle. Dans un cours un peu plus avancé, on donne tout de même un sens précis à cette notation, mais dans un premier temps, il vaut mieux que les débutants que vous êtes ne s'en servent pas.

Le lecteur s'entraîne :

1. Soit $f(z) : \mathbb{C}\backslash\{1\} \to \mathbb{C}$, l'application définie par $f(z) = \frac{z^2}{1-z}$ pour $z \neq 1$.

a) Déterminer les sous-ensembles $f^{-1}(\{0\})$, $f^{-1}(\{-4\})$ et $f^{-1}(\{3i\})$.

b) Soit $u \in \mathbb{C}$. Combien $f^{-1}(u)$ a-t-il d'éléments ?

c) L'application f est-elle injective ? Surjective ?

2. Soient $r \in]0, 1[$ et $\theta \in [0, 2\pi]$.

a) Résoudre dans $\mathbb{C}$ l'équation $z^2 - 2r\cos\theta\, z + r^2 = 0$. On notera z_1 et z_2 les solutions.

b) On pose $u_n = (z_1)^n + (z_2)^n$, pour $n \geq 1$. Montrer que $u_n = 2r^n \cos n\theta$, puis calculer $\lim_{n\to+\infty} u_n$.

10.5 Racines n-ièmes

10.5.1 Le théorème de d'Alembert

Reprenons un moment mon discours de l'introduction. J'ai expliqué que le concept de nombre a été élargi de façon répétée, d'abord pour s'assurer que toutes les équations linéaires, puis les équations quadratiques aient des solutions. Faudra-t-il de nouveau inventer un concept de "nombre" plus général pour que les équations de troisième degré comme

$$a_3z^3 + a_2z^2 + a_1z + a_0 = 0, \text{ avec } a_0, a_1, a_2, a_3 \neq 0 \in \mathbb{C},$$

aient des solutions ? Et après, que se passera-t-il avec les équations de degré $4, 5, \ldots$? La réponse est donnée par le théorème de d'Alembert :

Théorème 10.5. *(Théorème de d'Alembert) Soit*

$$P(z) = a_nz^n + a_{n-1}z^{n-1} + \cdots + a_1z + a_0$$

un polynôme de degré n ($a_0, \ldots, a_n \in \mathbb{C}, a_n \neq 0$). Alors il existe des nombres complexes $z_1, z_2, \ldots, z_n$, appelés racines de P, tels que

$$P(z) = a_n(z - z_1)(z - z_2)\ldots(z - z_{n-1})(z - z_n).$$

Donc, de ce point de vue, pas besoin d'élargir le concept de nombre au delà de celui de nombre complexe : tout polynôme de degré n a n racines. Ouf ! Nous y reviendrons en plus de détail dans le Chapitre **??**. Le théorème de d'Alembert est un théorème d'existence : il dit que les racines *existent*, mais pas comment les trouver. En général, ce n'est pas du tout facile, mais il y a un cas simple et intéressant que je traite maintenant.

10.5.2 Racines n-iémes

Il est facile de trouver toutes les solutions complexes de

$$z^n - a_0 = 0,$$

c'est à dire de trouver toutes les racines n-ièmes de $a_0 \in \mathbb{C}$. Le cas $n = 2$ a été traité dans la section précédente, et le cas général se traite de la même façon. Posons $a_0 = r_0 \exp(i\theta_0)$ et $z = r \exp(i\phi)$. On a

$$r^n \exp in\phi = r_0 \exp i\theta_0,$$

et donc $r = r_0^{1/n}$, $n\phi = \theta_0 + 2\pi k$. On conclut que les solutions de $z^n - a_0 = 0$ sont ($k \in \mathbb{Z}$) :

$$z_k = r_0^{1/n} \exp i\phi_k, \qquad \phi_k = \frac{\theta_0}{n} + 2\pi\frac{k}{n}.$$

En particulier

$$z_0 = r_0^{1/n}e^{i\theta_0}, \quad z_k = z_0e^{2\pi i\frac{k}{n}}.$$

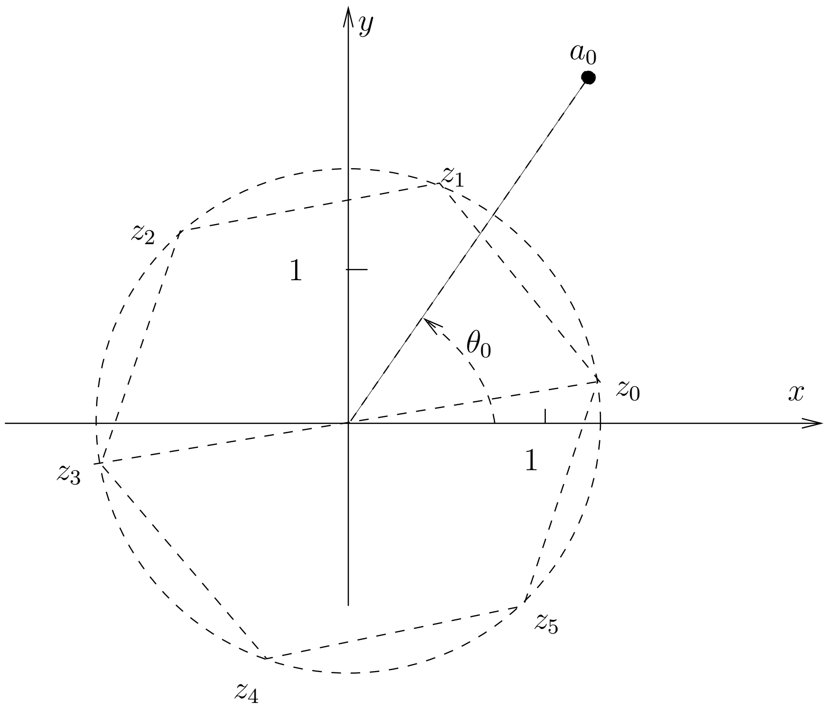

FIG. 10.3 – Les racines 6-ièmes de a_0

On remarque alors deux choses : il y a n racines distinctes, puisque $z_n = z_0$, $z_{n+1} = z_1$, *etc.* et les racines sont obtenues à partir de z_0 en effectuant une rotation d'angle $\frac{2\pi}{n}$. Elles sont donc toutes placées sur le cercle de centre 0 et de rayon $a_0^{1/n}$, aux n sommets d'un polygone régulier. Un exemple avec $n = 6$ est dessiné dans la figure 10.3

Le lecteur s'entraîne :

1. Soient $a, b \in \mathbb{C}$.

a) A quelle condition la similitude $z \in \mathbb{C} \to az+b \in \mathbb{C}$ est-elle une rotation ? Préciser son centre et son angle.

b) Vérifier, à l'aide de l'écriture complexe, que la composée de deux rotations est encore une rotation.

c) Retrouver l'expression analytique d'une rotation de centre $(x_0, y_0) \in \mathbb{R}^2$ et d'angle θ.

2. Fournir l'écriture complexe

a) d'une droite passant par un point $\Omega \in \mathbb{C}$ et faisant un angle φ avec l'axe des abscisses, ainsi que de la perpendiculaire à cette droite au point Ω.

b) d'un cercle de centre Ω et de rayon R.

S. De Bièvre

Chapitre 11

L'intégrale

Publié dans :
« L'oral du Capes de mathématiques : Face au jury »(Ellipses 2007).

Bibliographie

[AA] E. Azoulay, J. Avignant, *Mathématiques DEUG A, Tomes 1& 2*, Mc Graw Hill – Paris 1990.

[C] S.C. Coutinho, *The mathematics of ciphers – Number theory and RSA cryptography.* Ed. A.K. Peters, Natick Massachusetts, 1999.

[De] J.P. Delahaye, *Merveilleux nombres premiers,* Belin-Pour la Science, 2000.

[D] J. Dieudonné, *Pour l'honneur de l'esprit humain*, Hachette 1987.

[DH] P.J. Davis et R. Hersh, *L'univers mathématique*, Gauthier-Villars – Paris, 1985.

[DKM] J.M. De Koninck, A. Mercier, *Introduction à la théorie des nombres*, Modulo Edition, 1994.

[DV] J.C. Dupin, J.L. Valein, *Initiation au raisonnement mathématique (logique et théorie des ensembles)*, Flash U, Armand Colin 1993.

[E] I. Ekeland, *Le chaos*, Dominos – Flammarion, 1995.

[H] G.H. Hardy, *L'apologie d'un mathématicien*, Bélin – Paris, 1985.

[Hi] P.M. Higgins, *Mathematics for the curious*, Oxford University Press – Oxford-New York, 1998.

[Ho] D. Hofstadter, *Gödel, Escher, Bach, les brins d'une guirlande éternelle*, InterEditions – Paris 1985.

[HW] E. Hairer, G. Wanner, *Analysis by its history,* Undergraduate texts in mathematics, Springer 1995.

[LFA] J. Lelong-Ferrand, J.M. Arnaudies, *Cours de mathématiques, tome 2, Analyse*, Dunod 1996.

[LM] F. Liret, D. Martinais, *Cours de mathématiques, Algèbre 1ère année, Analyse 1ère année*, Dunod 1997.

[Pe] R. Penrose, *L'esprit, l'ordinateur et les lois de la physique*, InterEditions – Paris 1992.

[P1] H. Poincaré, *La science et l'hypothèse*, Champs-Flammarion, 1968.

[P2] H. Poincaré, *La valeur de la science*, Champs-Flammarion, 1970.

[RT] H. Rademacher, O. Toeplitz, *The enjoyment of math*, Princeton Science Library, Princeton University Press – Princeton 1994.

[S] S. Singh, *Histoire des codes secrets,* Ed. J.C. Lattes, 1999.

S. De Bièvre