ENTRER DANS L'UNIVERS MATHÉMATIQUE

Ensembles naturels, logique mathématique et démonstrations

M A T H E S I S
l'Univers Mathématique
1ère année, Semestre I, Cours n°1

Jean Barbet

Entrer dans l'Univers Mathématique

Ensembles Naturels, Logique Mathématique et Démonstrations

Jean Barbet

MATHESIS

l'Univers Mathématique

$1^{\text{ère}}$ année – Semestre I – Cours n° 1

La Règle et le Compas : www.reglecompas.fr

Avant-propos

Présentation de l'auteur

Je m'appelle Jean Barbet, je suis mathématicien indépendant et enseignant en ligne. Docteur en mathématiques, je me suis réorienté après des études en sciences de la vie. A cause de lacunes universitaires j'ai rencontré mes premières difficultés et mes premiers échecs en mathématiques. Pour réussir ma reconversion, j'ai du retravailler par moi-même dans les manuels de référence, choisir ce qui était essentiel, intégrer les connaissances et la pratique, et trouver un sens aux différentes disciplines mathématiques et un lien entre elles, parce que je n'avais pas le temps de refaire tout ce qui m'avait manqué.
J'ai suivi la même méthode pour achever mes études et c'est celle que j'utilise aujourd'hui pour apprendre et créer des mathématiques. La science mathématique possède un sens en elle-même et forme une unité, et ses différents domaines sont profondément liés. Prendre ceci en compte permet d'apprendre, d'assimiler et de comprendre de manière naturelle le noyau de la connaissance mathématique supérieure et tout ce travail m'a permis de compléter mon cursus universitaire jusqu'au Doctorat en mathématiques (obtenu en 2010).
Après plus de dix années d'expérience dans l'enseignement des mathématiques, du collège à l'université et à l'école d'ingénieurs, j'ai rassemblé les résultats de ma synthèse dans un corpus du niveau de la Licence universitaire : Mathesis, l'Univers Mathématique. Avec Mathesis, je veux donner la possibilité, à quiconque veut apprendre sérieusement des mathématiques, d'acquérir le noyau de ce qu'on appelle la mathématique supérieure, c'est-à-dire celle qu'on fait après le lycée et qui correspond à la science mathématique moderne, avec ses concepts et ses méthodes.

Mathesis - l'Univers Mathématique

Le corpus intègre l'essentiel de ce qu'on trouve dans une Licence de mathématiques à l'université, et se divise en trois années, de deux semestres chacune. Il sera publié sous la forme de fascicules correspondant chacun à un cours. Chaque semestre aborde en cinq ou six cours l'ensemble des disciplines. J'ai voulu éviter les écueils habituels liés aux contraintes de l'organisation de l'enseignement supérieur : des cours séparés dans des domaines étanches (Algèbre, Analyse...) et exposant des notions abstraites déconnectées de l'intuition, des exercices techniques trop difficiles et dépourvus de sens.
Dans Mathesis, l'abstraction mathématique, inévitable, est construite pas-à-pas

à partir de l'intuition concrète, comme on apprend aux jeunes enfants au cours élémentaire. Il n'y a pas de domaine étanche, ni plusieurs séries de manuels pour chaque domaine, mais un cursus unique, qui revient cycliquement sur chaque sujet en insistant sur les liens qu'ils entretiennent. Rien n'empêche cependant de choisir un sujet et de ne lire que les fascicules qui s'y rapportent. La pratique, essentielle, est intégrée à la théorie, en ce que des exercices d'un niveau abordable mettent en œuvre directement, à chaque section, ce qui a été exposé dans le cours, et complètent l'apprentissage par l'application des connaissances générales à des situations particulières naturelles.
La **méthode de travail** que je vous conseille est la même pour tous les cours : chaque section correspond à une leçon, et l'étudiant(e) devrait la lire une fois tranquillement, en essayant de la comprendre ; la prise de notes personnelles est recommandée, mais pas indispensable : vous pouvez aussi annoter votre cours. Lorsqu'il y a des démonstrations, il/elle est invité(e) à les analyser et à les refaire, et lorsqu'il y a des exercices, à les chercher systématiquement. Avant de commencer chaque nouvelle section, il vous faudra relire la précédente pour vous remémorer le travail accompli et vous mettre en condition.
Mathesis vous propose un apprentissage sans échec : pour construire votre connaissance mathématique il n'est pas nécessaire d'apprendre par cœur le cours ni les démonstrations (il suffit de les analyser), et il n'est pas nécessaire de trouver la solution des exercices et des problèmes (il suffit de les chercher honnêtement). L'effort sérieux et régulier est cumulatif et suffit à l'assimilation : apprendre des mathématiques est à la portée de tous, même il s'agit d'une tâche exigeante, qui demande de la persévérance. Chaque section ou leçon demande entre trente minutes et une heure de travail par jour ; à cinq jours par semaine, chaque cours demande environ un mois. Si les leçons sont trop longues, n'hésitez pas à les fractionner : il vaut mieux travailler un peu tous les jours selon sa capacité, plutôt que s'épuiser et espacer les séances d'étude.

Présentation du cours

Cet ouvrage est le premier volume de toute la série, il s'agit donc du 1$^{\text{er}}$ cours du semestre I de la 1$^{\text{ère}}$ année. Il traite des bases essentielles qu'il vous faut acquérir impérativement pour vous engager solidement dans l'apprentissage de la science mathématique, et il constitue la première étape de cet apprentissage. Ce cours en cinq chapitres comporte 23 sections ou leçons, et 45 figures :
- vous découvrirez comment tous les objets de l'univers mathématique se décrivent à l'aide d'un seul concept, celui "d'ensemble"
- vous apprendrez à vous exprimer correctement en mathématiques, et à manipuler le symbolisme et les opérations logiques usuelles
- vous intégrerez les propriétés axiomatiques élémentaires des ensembles naturels de nombres (entiers naturels, entiers relatifs, rationnels et réels)
- vous construirez les fondements de théorie des ensembles dont vous avez besoin, en les articulant à l'expression et à la logique mathématiques
- vous assimilerez les règles de démonstration usuelles en démontrant vos premiers théorèmes dans une théorie élémentaire des ensembles naturels

- tout au long du cours, vous apprendrez passivement les représentations graphiques usuelles des objets mathématiques élémentaires en consultant les figures.

Travaillez à votre rythme, chaque jour, et à l'issue de ce parcours, vous serez devenu(e) un(e) apprenti(e)-mathématicien(ne).
Et n'oubliez pas le seul conseil utile qu'on m'ait donné, et qui m'ait permis d'aller au bout de mon propre apprentissage : *n'abandonnez jamais !*

Jean Barbet, 27 août 2020

Compléments sur la méthode de travail

Comprendre le cours L'intégration du cours ne nécessite pas d'apprendre par cœur. Par contre, une simple lecture est insuffisante. Lorsqu'un enseignant donne un cours en direct, il insiste sur certains points, donne des explications supplémentaires. Ces éléments ne sont pas disponibles dans le cours écrit, il est donc nécessaire que l'étudiant(e) y supplée, ce qui est à sa portée ; il (elle) doit faire ce qu'on appelle une lecture analytique. Dans un cours de mathématiques, on distingue plusieurs parties : outre les exercices et problèmes, nous avons des explications, des définitions, des propositions et des exemples.

Les explications sont le corps du texte mathématique : on introduit un nouveau sujet, on expose les propriétés d'un nouvel objet. Il faut lire ce texte en se posant la question : est-ce que je comprends ce que je lis ? Si ce n'est pas le cas, il faut s'arrêter et chercher les réponses : soit nous n'avons pas compris le texte lui-même, soit nous sommes mal assurés relativement à un point exposé dans une section précédente ; il nous faut alors y revenir pour clarifier notre pensée.

Les définitions introduisent de nouveaux objets ou de nouvelles notions, toujours à partir d'objets ou de notions introduits précédemment. Comme pour le corps du texte, il faut s'assurer de bien comprendre les définitions, les analyser en détail et revenir à des sections précédentes si nécessaire. Parfois, certains notions du lycée ou du collège sont utilisées de manière intuitive, sans être redéfinies immédiatement : l'étudiant(e) les retrouvera facilement par ses propres moyens.

Les propositions (appelées propositions, théorèmes, lemmes et corollaires) énoncent des propriétés essentielles des objets dont traite le cours, ceux qui précisément constituent la connaissance mathématique propre, celle qu'on met en évidence. Comme pour les définitions, il faut s'assurer de bien en comprendre les énoncés, mais à la différence des définitions il faut aussi en comprendre les démonstrations. Une démonstration est une argumentation mathématique, qui cherche à établir la véracité de la proposition énoncée. Il faut l'analyser, c'est-à-dire en identifier les différentes parties et leurs articulations logiques, et chercher à en comprendre chaque partie, et comment toutes les parties s'agencent pour établir le résultat annoncé. Une fois une démonstration comprise, il est bon de chercher à la reproduire soi-même.

Les exemples servent à illustrer les nouveaux concepts introduits par les définitions, ou bien les propriétés démontrées dans les propositions. Ces concepts et propriétés sont en effet la plupart du temps des généralités : il est donc important de comprendre comment ils se réalisent ou se manifestent dans des cas particuliers. Les exemples sont à bien comprendre également.

L'étudiant(e) qui veut faire des fiches devrait prendre en note surtout les définitions et les énoncés des propositions. Quelques exemples choisis parmi les plus suggestifs peuvent illustrer utilement ses notes. Enfin, il est bon, avant de commencer une nouvelle séance d'étude, de relire le cours étudié à la session précédente ou de relire ses notes, pour se remémorer les concepts et propriétés étudiés juste avant. Comme tout apprentissage, l'apprentissage mathématique est cumulatif.

Travailler les exercices Les exercices mathématiques consistent à mettre en œuvre ou appliquer le cours dans des situations particulières. Les problèmes sont des exercices d'un niveau supérieur qui consistent à résoudre une question ou une série de questions en faisant preuve de plus de créativité. Il n'est pas toujours possible de trouver la solution d'un exercice ou d'un problème à la première tentative ; on peut même échouer régulièrement. Aussi surprenant soit-il, l'important dans la recherche de la solution d'un exercice ou d'un problème n'est pas de trouver la solution, mais de la chercher honnêtement.
La résolution d'un exercice ou d'un problème consiste à développer une stratégie et à la mettre en œuvre. La première étape consiste à analyser l'exercice ou le problème : il faut s'assurer qu'on en comprend tous les termes, et qu'on comprend la question posée ; cette étape est essentielle et est une première mise en œuvre du cours. La seconde étape consiste à élaborer une stratégie : en fonction de la question posée, il faut identifier les idées qui nous viennent à l'esprit, souvent de manière désordonnée, et inventer une série d'étapes pour aboutir à la réponse ; souvent, il faut identifier comment les éléments du cours présents dans l'énoncé peuvent être utilisés pour atteindre l'objectif. La troisième étape consiste à mettre en œuvre la stratégie : il faut faire un ou des calcul(s), un ou des raisonnement(s), de manière rigoureuse. La seconde et la troisième étapes se font souvent simultanément ; il n'est en général possible d'analyser la démarche adoptée qu'après avoir effectué une tentative.
On a cherché l'exercice ou le problème honnêtement quand on est allé aussi loin qu'on le peut. Parfois, l'analyse de la question s'avère déjà difficile, et on n'a pas d'idée pour la résoudre. Parfois une stratégie nous vient à l'esprit, mais il nous manque l'adresse nécessaire pour aboutir, soit raisonner ou calculer efficacement ; ou alors, la stratégie est incomplète ou erronée. Parfois enfin, on arrive jusqu'au bout ; si c'est la situation la plus satisfaisante, ce n'est toutefois pas toujours le cas : la difficulté est inhérente à la mathématique, et à l'impossible nul n'est tenu. Lorsqu'on n'aboutit pas à la solution du problème, on peut (et on devrait) y revenir ultérieurement. Mais il est possible de chercher honnêtement la solution de chaque exercice, le minimum étant l'analyse de la question posée ; celle-ci est en principe toujours accessible, si bien qu'on n'échoue à l'exercice que lorsqu'on renonce à se poser la question.

Table des matières

Chapitre 1

L'Univers Mathématique

1.1 Les objets de la science mathématique

1.1.1 Objets et intuition

Traditionnellement, les mathématiciens ont cherché à conceptualiser et théoriser des notions intuitives telles que les nombres, les figures, les grandeurs, les formes... et dans les temps modernes et contemporains les objets de la mathématique se sont étendus, avec le développement de la mathématique elle-même, mais aussi l'avènement de la science expérimentale et de la technique moderne, aux espaces, aux fonctions, aux ensembles, aux langages formels, etc...
Par ailleurs, les mathématiciens ont toujours été intéressés par des sujets majeurs comme l'infini, le continu et l'espace.
Comme toute autre science, la mathématique est enracinée dans l'intuition de son ou de ses objet(s). Les exemples précédents soulignent la diversité historique des objets de la science mathématique, et posent la question de l'unité de la discipline. Il semble que ce que tous ces exemples - et les nouveaux qui apparaissent - ont en commun, est que la mathématique traite essentiellement, d'une manière ou d'une autre, de *multiplicités* : les nombres sont la forme des multiplicités finies, les figures et les formes sont des multiplicités géométriques, les grandeurs sont des multiplicités idéales, etc...

1.1.2 Le problème de la rigueur en mathématiques

Un problème récurrent de l'histoire de notre science est celui de la *rigueur* : la mathématique procède avec des preuves plutôt qu'avec des expériences, et prétend ainsi à l'exactitude.
L'activité mathématique n'est cependant jamais exempte d'erreurs, lesquelles proviennent d'un manque de clarté soit dans l'appréhension des objets mathématiques, soit dans le maniement du discours mathématique, notamment démonstratif.
Si la mathématique s'enracine dans l'intuition, celle-ci est aussi le ferment de la créativité mathématique. Il est toutefois nécessaire de la compléter par une méthode rigoureuse de description et de définition des objets mathématiques d'une part, d'articulation du raisonnement mathématique d'autre part.

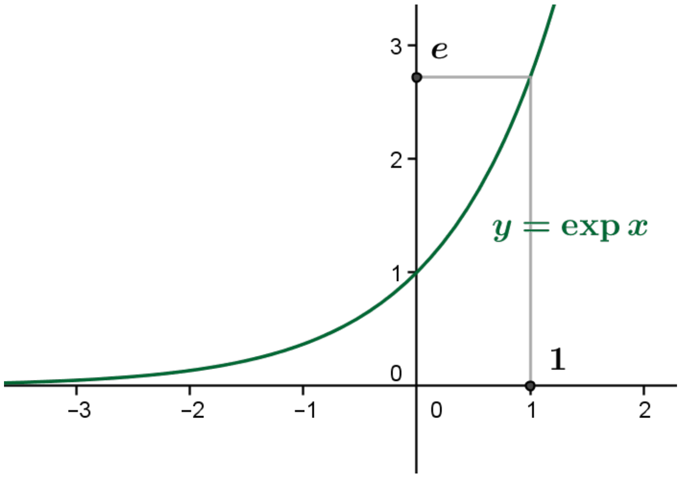
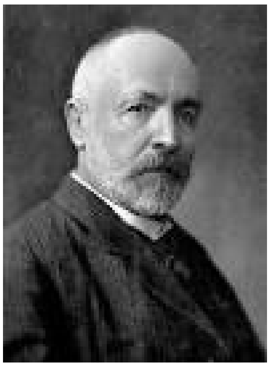


Figure 1.1: Une représentation graphique de la fonction exponentielle.

En fait, déterminer la nature des objets mathématiques et élaborer une méthode mathématique rigoureuse semblent être deux problèmes impliqués l'un dans l'autre, et la *théorie des ensembles* et sa logique mathématique sous-jacente ont fourni les moyens adéquats pour résoudre les deux.



Georg Cantor, le père de la théorie des ensembles.

1.1.3 La contribution décisive de la théorie des ensembles

La naissance de la théorie des ensembles à la fin du dix-neuvième siècle avec Cantor, et de la logique mathématique moderne avec Frege à la même époque, ont permis d'adresser les deux questions suivantes, qui reflètent la double problématique précédente :
i) Existe-t-il une unité dans la diversité des objets de la science mathématique ?
ii) Quelle est la méthode rigoureuse en mathématique ?
La notion d'ensemble capture sur le plan théorique ce que nous entendons par l'idée de "multiplicité", et tout objet mathématique peut virtuellement se concevoir ou se représenter comme un ensemble.
La théorie des ensembles est donc une théorie des "multiplicités" abstraites, notamment de leurs propriétés et des "constructions" dont elles sont l'objet, et elle fournit un *cadre théorique universel* qui est le *langage conceptuel* de ce que la mathématique

est devenue.
Cette théorie, extrêmement naturelle et puissante, fournit également la base d'une méthode mathématique claire, essentiellement articulée à la définition des objets et du discours, descriptif et démonstratif, qui les concerne.
En somme, **l'univers mathématique possède une structure "ensembliste"**, et **le discours mathématique est modelé sur cette structure**, avec sa syntaxe et sa logique.

Gottlob Frege, mathématicien et philosophe.

1.2 La notion d'ensemble et les exemples naturels

1.2.1 Les ensembles et leurs éléments

Nous avons évoqué dans la section précédente comment la théorie "naïve", c'est-à-dire *intuitive*, des ensembles, cherche à capturer sur le plan mathématique la notion intuitive de "multiplicité", laquelle donne une unité à la diversité des objets de la mathématique. Cette théorie a montré sa fécondité en ce qu'elle est devenue le fondement naturel de la science mathématique.
La notion d'ensemble, comme les notions d'objet et de (nombre) entier naturel, est une notion *primitive* en mathématique; cela signifie qu'elle ne peut être définie à partir d'une autre notion, sans assumer implicitement et d'une certaine manière sa définition. Par exemple, la définition de Cantor qu'un ensemble est une certaine "collection d'objets de notre entendement" ne nous mène guère plus loin que la signification intuitive du terme "ensemble", puisqu'on ne peut pas établir clairement la distinction entre une collection et un ensemble.
La théorie "naïve" des ensembles ne cherche donc pas à *définir* ce qu'est un ensemble, mais à *préciser* comment les ensembles peuvent être décrits ou caractérisés, quelles opérations et constructions sont permises à leur propos, en somme quels ensembles sont "permis" dans le discours mathématique.
Si un ensemble est, selon la signification intuitive usuelle du terme, une multiplicité d'objets, ces objets sont appelés ses *éléments* ou ses *membres*. Il est habituel d'utiliser des lettres pour dénoter les ensembles et certains de leurs éléments, particuliers ou génériques : $E, F, X, Y, \ldots, x, y, a, b, \ldots$. Si E est un ensemble et x un objet, la notation symbolique pour "x est un élément de E" est "$x \in E$".

La relation $\in$, dite *d'appartenance*, entre objets et ensembles est notre premier exemple de relation mathématique, en fait une relation "méta-mathématique" ou "méta-relation".
Un ensemble est une multiplicité *quelconque* d'objets, mathématiques ou non. Par exemple, si j'ai un frère dénommé Paul, alors Paul est un élément de ma famille, considérée comme un ensemble de personnes.
Une exception notable est la "collection" de tous les objets et ensembles, qui pour des raisons logiques *ne peut pas être* un ensemble de la théorie; elle est ce que nous appelons le *(méta-)univers* ou *l'univers* du discours mathématique (ce sur quoi il porte). C'est pourquoi la relation d'appartenance $\in$ a été qualifiée de "méta-relation".
Cette collection sera donc considérée comme une "multiplicité externe" à la théorie, et ce que nous entendons par "l'univers mathématique". Pour les mêmes raisons, il n'existe pas "d'ensemble de tous les ensembles" en théorie naïve des ensembles.

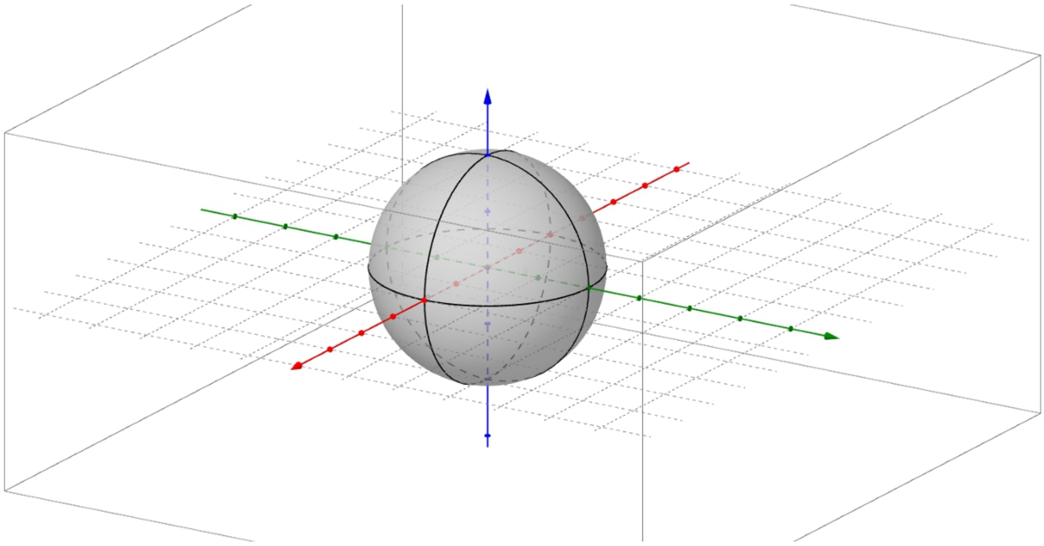


Figure 1.2: Une sphère est un ensemble infini de points de l'espace euclidien à 3 dimensions.

1.2.2 Les ensembles naturels fondamentaux

Nous avons dit que virtuellement, tout objet mathématique peut se concevoir comme un ensemble ou se représenter par un ensemble. Ce fait, que nous pourrions appeler la "méthode analytique ensembliste", a conduit à "reconstruire" en quelque sorte tous les objets mathématiques usuels, et notamment les objets géométriques, à partir de quelques *ensembles naturels de nombres*. Une série de six ensembles forme un "sentier" dans l'univers mathématique, de l'arithmétique à la géométrie. Ce sont l'ensemble $\mathbb{N}$ des *nombres entiers naturels*, l'ensemble $\mathbb{Z}$ des *nombres entiers relatifs*, l'ensemble $\mathbb{Q}$ des *nombres rationnels*, l'ensemble $\mathbb{R}$ des *nombres réels*, l'ensemble $\mathbb{C}$ des *nombres complexes* et l'ensemble $\mathbb{H}$ des *quaternions*, que nous décrivons ici de manière intuitive.

Définition 1.2.1. L'ensemble dénoté par un $\mathbb{N}$ calligraphique est par définition *l'ensemble des (nombres) entiers naturels*, par lequels nous représentons les quantités des multiplicités finies, c'est-à-dire celles que nous pouvons compter : $0, 1, 2, 3, \ldots$.

Il s'agit, intuitivement, d'un *ensemble infini*, un concept mathématique essentiel et fascinant que nous définirons précisément dans le deuxième cours.

Définition 1.2.2. L'ensemble dénoté par un $\mathbb{Z}$ calligraphique est par définition *l'ensemble des (nombres) entiers relatifs* ou *ensemble des entiers rationnels*; ce sont tous les nombres de la forme $\ldots, -3, -2, -1, 0, 1, 2, 3, 4, \ldots$, qui représentent les "opérations" sur les entiers naturels : nous ajoutons à l'ensemble $\mathbb{N}$ tous les opposés des entiers naturels pour l'addition.

Définition 1.2.3. L'ensemble dénoté par un $\mathbb{Q}$ calligraphique est par définition *l'ensemble des (nombres) rationnels*, qui sont tous les nombres "fractionnaires" de la forme a/b, pour a, b des entiers relatifs tels que $b \neq 0$, et qui représentent intuitivement toutes les "fractions" de nombres entiers, possiblement négatifs.

Exemple 1.2.4. Tout entier relatif est un nombre rationnel. Les nombres décimaux, comme 0.89, -1756.694 sont des nombres rationnels. Les fractions, comme $1/2$, $-3578906/-7654$, $3/-17$, $-255/32$, désignent sont des nombres rationnels. Les nombres $\sqrt{2}$ et π ne sont pas des nombres rationnels.

Définition 1.2.5. L'ensemble dénoté par un $\mathbb{R}$ calligraphique est par définition *l'ensemble des nombres réels*, les "points" (c'est-à-dire les "lieux") de la "droite géométrique", qui représentent intuitivement toutes les *grandeurs* ou *valeurs*, lesquelles correspondent à toutes les mesures géométriques ou physiques possibles.

Exemple 1.2.6. Tout nombre rationnel est un nombre réel. Les célèbres nombres $\sqrt{2}$ et π, ainsi que e, la base de la fonction exponentielle, sont des nombres réels.

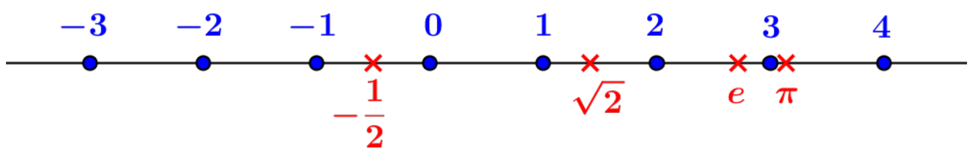


Figure 1.3: Une représentation géométrique de quelques nombres réels : les entiers relatifs $-3, -2, -1, 0, 1, 2$ et 3, le nombre rationnel $-\frac{1}{2}$ et les nombres réels $\sqrt{2}$, e et π, les deux derniers étant dits "transcendants".

Définition 1.2.7. L'ensemble dénoté par un $\mathbb{C}$ calligraphique est par définition *l'ensemble des nombres complexes*, qui sont des nombres "à deux dimensions" et représentent intuitivement les "points" du "plan géométrique".

Remarque 1.2.8. Les nombres complexes se conçoivent aussi comme des objets géométriques appelés "vecteurs", et qui représentent des "déplacements rectilignes" sur le plan.

Tout nombre complexe s'écrit de manière unique sous la forme $a+ib$ (c'est-à-dire $a+i.b$, $i.b$ étant un produit), où a et b sont des nombres réels (les coordonnées du point que $a+ib$ représente dans le plan) et i un nombre complexe très particulier. L'addition des nombres complexes se fait ainsi : si $a+ib$ et $c+id$ sont des nombres complexes, $(a+ib)+(c+id)=(a+c)+i(b+d)$ (on dit qu'on additionne "composante par composante"), mais la multiplication des nombres complexes se fait ainsi : $(a+ib).(c+id)=(ac-bd)+i(ad+bc)$, de sorte que $i^2=(0+i1)(0+i1)=-1$! De même, $(-i)^2=-1$; i et $-i$ sont des "racines carrées" de -1.
Tout nombre réel a s'identifie à un nombre complexe, à savoir $a+i0$! On peut additionner ou multiplier des nombres complexes (et donc des nombres entiers, rationnels, ou réels) dans n'importe quel ordre en obtenant le même résultat.
La multiplication des nombres complexes a une interprétation géométrique que nous découvrirons dans un autre cours de ce semestre.

Définition 1.2.9. Enfin, l'ensemble dénoté par un $\mathbb{H}$ calligraphique est par définition *l'ensemble des quaternions*, qui sont des "vecteurs à quatre dimensions", ou les "points" d'un "espace-temps algébrique".

Tout quaternion s'écrit de manière unique sous la forme $a+ib+jc+kd$, où a,b,c,d sont des nombres réels (les coordonnées du point que $a+ib+jc+kd$ représente dans l'espace-temps, a étant la coordonnée temporelle), et i,j,k sont des quaternions très particuliers. L'addition des quaternions se fait ainsi : si $a'+ib'+jc'+kd'$ est un autre quaternion, $(a+ib+jc+dk)+(a'+ib'+jc'+kd')=(a+a')+i(b+b')+j(c+c')+k(d+d')$ (encore une fois "composante par composante"), mais la multiplication des quaternions de fait ainsi : $(a+ib+jc+kd).(a'+ib'+jc'+kd')=(aa'-bb'-cc'-dd')+i(ba'+ab'+cd'-c'd+)+j(ca'+ac'+db'-d'b)+k(da'+a'd+bc'-b'c)$, de sorte que $i^2=-1$, $j^2=-1$, $k^2=-1$ et $ij=k=-ji$, $jk=i=-ij$, $ki=j=-ik$!
Tout nombre complexe "est" un quaternion : si $a+ib$ est un nombre complexe, on l'identifie au quaternion $a+ib+j0+k0$!
Notons que la multiplication des quaternions a également une interprétation géométrique, qui prolonge celle de la multiplication des nombres complexes. Nous ne donnons ici qu'une description générale, sans entrer dans les détails de la théorie, que nous abordons dans un autre cours.

Remarque 1.2.10. Par contraste avec les nombres complexes qui sont des "nombres à deux dimensions", il est difficile de concevoir les quaternions comme des "nombres à quatre dimensions", car l'ordre dans lequel on effectue le produit de deux quaternions peut donner des résultats différents ! Par exemple, nous avons vu que $ij\neq ji$.
De notre point de vue ce sont plutôt des objets géométriques. Néanmoins ils sont le cadre naturel d'un théorème d'arithmétique profond appelé le "théorème des quatre carrés", qui énoncé que *tout nombre entier naturel est la somme de quatre carrés*, et que nous aborderons au second semestre. En ce sens, l'ensemble $\mathbb{H}$ est une réalité arithmético-géométrique ultime.

Dans ce cours, nous focaliserons sur les ensembles $\mathbb{N},\mathbb{Z},\mathbb{Q}$ et $\mathbb{R}$. Nous réservons l'étude de $\mathbb{C}$ et $\mathbb{H}$ à d'autres cours de ce semestre et des suivants.

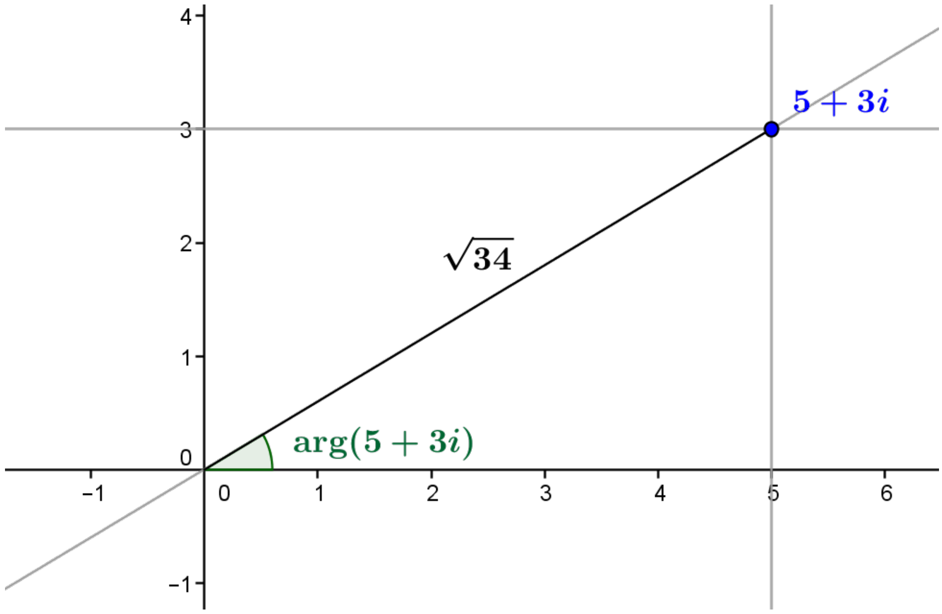


Figure 1.4: Représentation d'un point du plan, de coordonnées $(5, 3)$, comme le nombre complexe $5 + 3i$. Un nombre complexe non nul est identifié par son module (la distance du point qu'il représente à l'origine) et son argument (l'angle du vecteur qu'il représente avec l'axe des abscisses).

Exercices de la leçon

Il est important de *chercher* les exercices, plus que de les *résoudre* à la première tentative. Si ou quand vous échouez, revenez-y plus tard.

Exercice 1.2.11. Trouver un exemple :
i) d'un entier relatif qui n'est pas un entier naturel
ii) d'un rationnel qui n'est pas un entier relatif
iii) d'un nombre réel qui n'est pas un nombre rationnel.

1.3 La notion de sous-ensemble et les inclusions des ensembles naturels

1.3.1 Définition des ensembles

Il existe en mathématique deux manières essentielles de définir, c'est-à-dire de décrire, un ensemble : la définition par *extension*, et la définition par *intension*. La notation symbolique pour la définition d'un ensemble utilise les crochets ou accolades { et }.
Un ensemble est défini par *extension* lorsqu'on donne explicitement la liste de tous ses éléments. Par exemple, l'ensemble $\{0, 3, 5, 1, 4\}$ est un ensemble qui possède 5 éléments, lesquels sont les nombres entiers naturels $0, 3, 5, 1, 4$. Si mes parents ont deux enfants, ma soeur Sylvie et moi-même, ma famille est l'ensemble {Papa, Maman, Sylvie, moi}.

Un ensemble est défini par *intension* lorsqu'on décrit ses éléments à l'aide d'une propriété qu'ils ont en commun. Par exemple, les ensembles notés $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ et $\mathbb{R}$ ont été définis dans le cours précédent par intension, à partir de notions intuitives. Les "habitants de Paris" forment un ensemble qu'on n'énumère pas à cause de sa taille, mais qui est bien identifié.
Les définitions par intension sont essentielles pour décrire les ensembles infinis, dont on ne peut pas, par définition, décrire tous les éléments. De plus, une définition par extension se ramène toujours à une définition par intension : il suffit de considérer la propriété d'être l'un des éléments de la liste ! La définition par intension est donc la définition mathématique par excellence.

1.3.2 Les sous-ensembles d'un ensemble

Etant donné un ensemble E quelconque, fini ou infini, mathématique ou non, nous pouvons considérer les ensembles formés de certains éléments de E, qui sont appelés *parties*, ou *sous-ensembles*, de E. Un sous-ensemble de E peut-être E lui-même, omettre certains éléments de E ou ne pas avoir d'éléments du tout. Ayant déjà introduit la relation d'appartenance entre un objet et un ensemble, symbolisée par $\in$, nous pouvons définir rigoureusement ce qu'est un sous-ensemble, en utilisant la seule relation $\in$, comme suit :

Définition 1.3.1. Si E est un ensemble, un *sous-ensemble (ou une partie) de* E est un ensemble P tel que tout élément de P est un élément de E. Symboliquement, on écrit "$\forall x \in P,\ x \in E$", ce qui signifie "pour tout x dans P, x est dans E" (nous expliquerons ce symbolisme dans le deuxième chapitre). Nous écrivons $P \subseteq E$ pour la relation "P est un sous-ensemble de E" et nous disons aussi que P est *inclus* dans E.

Remarque 1.3.2. i) La relation $\subseteq$ est appelée relation *d'inclusion*. C'est, comme la relation d'appartenance, une méta-relation.
ii) Si $P \subseteq E$, on dit parfois que E *contient* P. Or, si $x \in E$, nous disons aussi parfois que E *contient* x, donc il y a ici une certaine ambiguïté dans l'usage du verbe "contient", qui est clarifiée par le contexte.

Voici quelques exemples de sous-ensembles. On rappelle qu'un ensemble est défini par *intension* si il est défini à partir d'une propriété.

Exemple 1.3.3. i) Chaque ensemble E est une partie de lui-même, par définition.
ii) L'ensemble $\{1, 0, 4\}$ est un sous-ensemble de l'ensemble $\{0, 3, 5, 1, 4\}$.
iii) L'ensemble P des entiers naturels pairs est un sous-ensemble de l'ensemble $\mathbb{N}$ de tous les entiers naturels, tout comme l'ensemble I des entiers naturels impairs, ou encore l'ensemble des multiples d'un nombre entier naturel donné.
iv) L'ensemble des multiples, positifs ou non, d'un entier relatif n, est un sous-ensemble de $\mathbb{Z}$.
v) L'ensemble des fractions qui s'écrivent avec 3 au dénominateur est un sous-ensemble de $\mathbb{Q}$.
vi) L'ensemble des nombres réels positifs (ou nuls) est un sous-ensemble de $\mathbb{R}$, noté $\mathbb{R}_+$. L'ensemble des nombres réels négatifs (ou nuls) est un autre sous-ensemble de

$\mathbb{R}$, noté $\mathbb{R}_-$.
vii) Un cercle dans le plan, considéré comme ensemble de points, est une partie du plan, donc de l'ensemble $\mathbb{C}$ des nombres complexes.

L'ensemble qui ne contient aucun élément est appelé *l'ensemble vide*, et noté $\emptyset$: c'est en fait un sous-ensemble de tout ensemble.
Démontrons-le : si E est un ensemble quelconque, comme $\emptyset$ n'a pas d'élément, en bonne logique il est vrai que tout élément de $\emptyset$ est un élément de E, ce qui signifie que $\emptyset \subseteq E$ par définition !
L'étudiant(e) ou la lectrice sceptique pourra temporairement admettre ceci comme une convention.

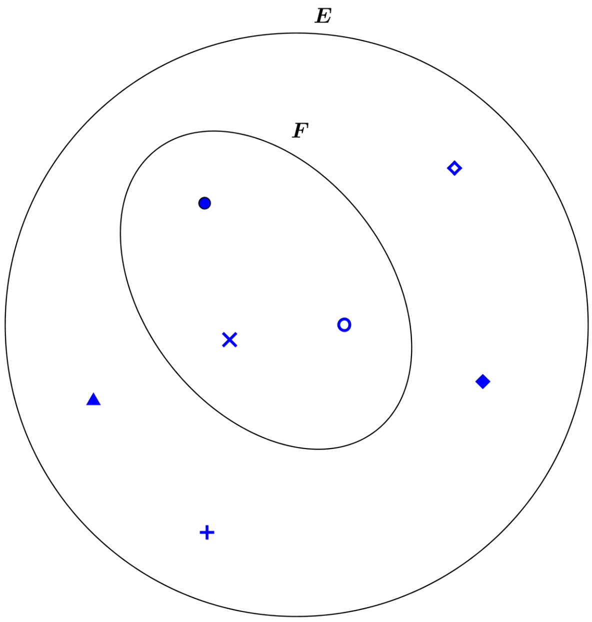


Figure 1.5: L'ensemble F est un sous-ensemble de l'ensemble E car tout élément de F est un élément de E.

1.3.3 Inclusions entre les ensembles naturels

En ce qui concerne les quatre premiers ensembles naturels introduits précédemment dans leurs version intuitive, nous avons les inclusions suivantes : $\mathbb{N} \subseteq \mathbb{Z}$, $\mathbb{Z} \subseteq \mathbb{Q}$ et $\mathbb{Q} \subseteq \mathbb{R}$, qui signifient que tout entier naturel est un entier relatif, tout entier relatif est un rationnel et tout rationnel est un nombre réel.
Au niveau où nous nous plaçons dans cette introduction, toutes ces inclusions sont vraies *par définition* : nous concevons $\mathbb{Z}$ comme une "extension" de $\mathbb{N}$, $\mathbb{Q}$ comme une "extension de $\mathbb{Z}$ et $\mathbb{R}$ comme une "extension" de $\mathbb{Q}$, et ainsi de suite. Dans des cours subséquents nous donnerons des *constructions* explicites de $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, (ainsi que $\mathbb{C}$ et $\mathbb{H}$) à partir de $\mathbb{N}$, et les inclusions présentes devront être remplacées par ce qu'on appelle des *plongements*.
Pour l'heure, en rappelant l'exercice 1.2.11 on peut remarquer qu'aucune des inclusions précédentes n'est réciproque :

- si $n \in \mathbb{N}$ et $n > 0$, alors $-n$ est dans $\mathbb{Z}$ mais pas dans $\mathbb{N}$ (ce qu'on écrit $-n \notin \mathbb{N}$), donc on n'a pas $\mathbb{Z} \subseteq \mathbb{N}$, ce qu'on écrit $\mathbb{Z} \not\subseteq \mathbb{N}$
- $1/2 \notin \mathbb{Z}$, donc $\mathbb{Q} \not\subseteq \mathbb{Z}$
- $\sqrt{2} \notin \mathbb{Q}$ (nous prouverons ceci plus tard), donc $\mathbb{R} \not\subseteq \mathbb{Q}$.

Ces inclusions peuvent être "combinées", dans le sens général "qu'un sous-ensemble d'un sous-ensemble d'un ensemble quelconque est un sous-ensemble", ce que nous énonçons précisément comme la

Proposition 1.3.4. *Si E est un ensemble, P est une partie de E et X un sous-ensemble de P, alors X est un sous-ensemble de E. Symboliquement : si $P \subseteq E$ et $X \subseteq P$, alors $X \subseteq E$.*

Démonstration. Nous voulons montrer que $X \subseteq E$: il nous faut revenir à la définition, c'est-à-dire que nous voulons prouver que tout élément de X est un élément de E. Choisissons donc un élément générique de X, que nous appelons x : par hypothèse, nous avons $X \subseteq P$, donc par définition x est un élément de P; par hypothèse à nouveau, comme $P \subseteq E$ tout élément de P est un élément de E, donc $x \in E$. Nous avons démontré que tout élément de X est un élément de E, c'est-à-dire que X est un sous-ensemble de E. □

Remarque 1.3.5. Nous expliquerons plus tard dans ce cours les noms des types d'énoncés mathématiques, comme "proposition", et nous exposerons les différentes méthodes de démonstration d'un énoncé. Pour l'instant, il suffit de se familiariser avec cette caractéristique essentielle de la mathématique : on énonce des faits mathématiques précis, et on établit leur validité ou véracité par un argument rigoureux qu'on appelle une "preuve" ou une "démonstration".

Cette proposition nous permet de déduire des inclusions élémentaires précédentes que $\mathbb{N} \subseteq \mathbb{Q}$ (car $\mathbb{N} \subseteq \mathbb{Z}$ et $\mathbb{Z} \subseteq \mathbb{Q}$), et ainsi $\mathbb{N} \subseteq \mathbb{R}$ (car $\mathbb{N} \subseteq \mathbb{Q}$ et $\mathbb{Q} \subseteq \mathbb{R}$), et aussi que $\mathbb{Z}$ est un sous-ensemble de $\mathbb{R}$ (car $\mathbb{Z} \subseteq \mathbb{Q}$ et $\mathbb{Q} \subseteq \mathbb{R}$).
Intuitivement, ceci peut être fait un nombre "fini" de fois, de sorte que dans une "chaîne" finie d'inclusions, tout membre est inclus dans le dernier membre.

Exemple 1.3.6. Pour cette raison, nous utilisons la formule abusive mais pratique $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$.

Attention : ceci n'est pas possible en général pour la relation $\in$ (on dit que la relation $\subseteq$ est *transitive*, tandis que la relation $\in$ ne l'est pas en général) !

Exercices de la leçon

Exercice 1.3.7. i) Trouver un exemple d'un ensemble non mathématique E et un exemple d'un sous-ensemble P de E qui ne soit ni E ni $\emptyset$.
ii) Trouver un nouvel exemple d'un sous-ensemble non vide pour chacun des ensembles suivants : $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ and $\mathbb{R}$.

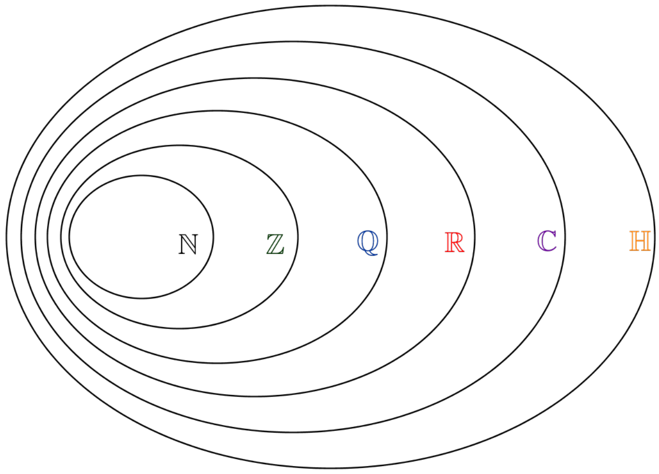


Figure 1.6: Une représentation de l'inclusion des ensembles naturels $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ et $\mathbb{H}$.

Chapitre 2

Le Langage et l'Expression mathématiques

Dans ce chapitre, nous voulons souligner les particularités du discours mathématique, et pour cela nous voulons en identifier les parties et les règles de formation.
Le discours mathématique s'inscrit dans le discours naturel, avec l'usage de symboles qui ne sont que des abréviations. Son sens s'inscrit donc naturellement dans le sens habituel du langage, mais avec des dénotations et des connotations mathématiques. Nous ne chercherons donc pas à définir le discours mathématique dans un sens mathématique (ce qui relève de la logique mathématique formelle, et ne permet pas d'ailleurs d'éviter de traiter du discours mathématiques naturel), mais seulement à préciser et clarifier les usages, qui s'acquièrent par l'expérience.
Le sens et la syntaxe du langage mathématique doivent être intégrés et compris progressivement par l'étudiant(e) ou le lecteur, comme c'est le cas dans l'apprentissage d'une langue étrangère (à ceci près qu'en mathématique il faut aussi apprendre des dénotations nouvelles du langage...).

$$\forall \boldsymbol{\epsilon} \in \mathbb{R},\ \boldsymbol{\epsilon > 0 \rightarrow (}\exists \boldsymbol{\eta} \in \mathbb{R},\ \boldsymbol{\eta > 0}\ \wedge\ \forall \boldsymbol{y} \in \mathbb{R},\ \boldsymbol{|y - x| < \eta \rightarrow |f(y) - f(x)| < \epsilon)}$$

Figure 2.1: Cette formule mathématique exprime la continuité d'une fonction f en un nombre réel x. Il s'agit d'une définition rigoureuse, par contraste avec la définition intuitive qu'on adopte au lycée.

2.1 Les types d'expressions mathématiques

Nous dirons en général qu'une locution du langage naturel est une *expression mathématique* si elle dénote un objet mathématique ou un état de choses (un fait) mathématique.
Parmi ces expressions nous distinguerons un petit nombre de types, qui sont les *termes*, les *clauses*, les *énoncés*, les *définitions* et les *notations*, que nous allons brièvement décrire.

2.1.1 Les termes

Les *termes* sont les expressions, littérales ou symboliques, qui dénotent les *objets* mathématiques, particuliers ou génériques.
Les termes sont en quelque sorte les "groupes nominaux" du discours mathématique, comparables aux noms propres lorsqu'ils dénotent des objets particuliers, aux noms communs lorsqu'ils dénotent des objets génériques.
Un terme dénote un objet générique quand il contient au moins une *variable*, c'est-à-dire une lettre ou un signe sans signification ou *valeur* fixée.
Un terme sans variable dénote un objet précis; un tel terme est dit *clos* ou *fermé*.
Il est possible de substituer des termes aux variables dans d'autres termes, quand cela est approprié.

Exemple 2.1.1. i) Les expressions $0, 1, \pi, e$ sont des termes qui dénotent des nombres particuliers (e est la base de la fonction exponentielle).
ii) Les expressions $\cos(x), \sin(x), Log(x), \exp(x)$ sont des termes qui dénotent des fonctions particulières (cosinus, sinus, logarithme et exponentielle). On note aussi ln le logarithme (dit népérien).
iii) Les expressions $\cos\ \ x, y + z, 5x + 12, Log\ u$ sont des termes qui dénotent des nombres génériques (le cosinus de x, la somme de y et de z, la some de 5 fois x et de 12, le logarithme de u). Nous pouvons substituer le terme π pour x dans $cos\ x$ pour obtenir le nombre réel $cos\ \pi$, dont la valeur est -1.
iv) La fonction logarithme n'est définie que pour des nombres réels strictement positifs. Si $x \geq 0$, on a $5x + 12 > 0$, donc il est possible de substituer le terme $5x + 12$ pour u dans $Log\ u$ pour obtenir le terme générique $Log(5x + 12)$.
v) L'expression x^2+2x+3 est un terme qu'on appelle *polynôme*. Ces termes sont très importants en algèbre, où on les représente par les suites finies de leurs *coefficients*, ici $3, 2, 1$.

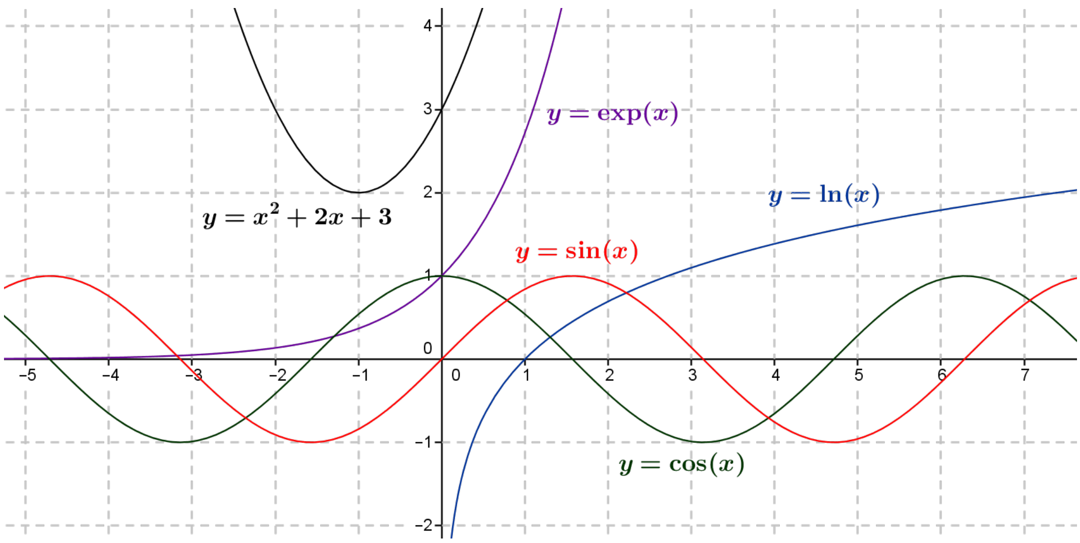


Figure 2.2: Représentation graphique des fonctions dénotées par les termes $\cos x, \sin x, \ln x, \exp x$ et $x^2 + 2x + 3$.

2.1.2 Les clauses

Les *clauses* sont les expressions, littérales ou symboliques, qui dénotent des états de choses (des faits) mathématiques, qu'ils soient particuliers ou génériques.
Une variable dans une clause est dite *libre* quand sa signification n'est pas déterminée à l'intérieur de la clause; autrement, elle est dite *liée* (ce deuxième cas apparaît avec la quantification, que nous introduirons bientôt).
Quand une clause contient au moins une variable libre, elle dénote une propriété générique des types d'objets dénotés par ses variables libres.
Quand elle ne contient aucune variable libre, nous l'appelons un *énoncé* et elle dénote une *valeur de vérité*, c'est-à-dire le "vrai" ou le "faux", selon la véracité de l'état de choses qu'elle exprime à propos des objets dont elle contient les signes.
Si P ou $P(x)$ désigne une clause contenant une variable libre x, générique pour un ensemble E, et si a est un élément de E, la *substitution de a pour x dans P* est une clause (un énoncé si x est la seule variable libre) que nous écrirons $P(a)$ ou $P(a/x)$.

Exemple 2.1.2. i) Si a n'est pas un objet précis dans le contexte, la clause "$a < 5$" possède une variable libre a et exprime que a est (strictement) inférieur à 5. Si on *substitue* un nombre approprié à a, cette clause se transforme est un énoncé qui est vrai ou faux selon la valeur attribuée à a. Par exemple, si on remplace a par 2 (on dit parfois qu'on "pose" $a = 2$), alors la clause devient $2 < 5$, laquelle est vraie; tandis que si l'on pose $a = 2\pi$, elle devient $2\pi < 5$, ce qui est faux.
ii) La clause "$\forall x \in \mathbb{N},\ 0 < x$" se traduit par "pour tout nombre entier naturel x, on a $0 < x$". Bien qu'elle contienne la variable x, cette variable n'est pas libre, car on ne peut lui assigner une valeur : son "sens" est lié à la quantification "pour tout". Cette clause est donc un énoncé, et dénote le faux, parce que 0 n'est pas strictement inférieur à lui-même.
iii) L'expression "m est un multiple de n", où m et n sont deux variables qui dénotent des entiers naturels, est une clause mathématique avec deux variables libres, m and n. Elle peut se reformuler comme : "il existe un entier naturel d tel que $m = n \times d$", symboliquement $\exists d \in \mathbb{N}, m = n \times d$, où d est une variable "auxiliaire", quantifiée existentiellement et donc liée (nous parlerons bientôt en détail de la quantification).

Parmi les clauses, nous distinguerons les *clauses élémentaires*, qui expriment des relations mathématiques simples entre les objets qu'elles contiennent.

Exemple 2.1.3. i) La clause "$a < 5$" est élémentaire, ainsi que les clauses "$0 = 7$" et "$(5 \times 12) + (-\pi) > Log(e + 19)$".
ii) La clause "$\forall x \in \mathbb{N},\ 0 < x$" n'est pas élémentaire, car elle est construite à partir de la clause élémentaire "$0 < x$" par l'utilisation d'une *quantification (universelle).*
iii) La clause "$m = n \times d$" est élémentaire, mais la clause "$\exists d, m = n \times d$" qui exprime que m est un multiple de n, ne l'est pas. Cependant, si nous introduisons la notation (standard) "$n|m$" (qui se lit "n divise m") pour la relation "m est un multiple de n", la clause $n|m$ est élémentaire. Le caractère élémentaire d'une clause dépend donc du vocabulaire symbolique que nous utilisons, et donc du contexte.

Lorsqu'on substitue des termes à toutes les variables libres d'une clause, on obtient une nouvelle clause. Si tous les termes substitués sont clos, cette opération transforme la clause d'origine, qui possède une signification "ouverte" en un énoncé, qui est soit vrai soit faux, selon la substitution opérée.

Exemple 2.1.4. i) Dans la clause "$x < y$", si nous remplaçons x par π et y par 2, nous obtenons l'énoncé $\pi < 2$, qui est faux. Si nous remplaçons cependant x par 10 et y par 10^{10}, nous obtenons un énoncé vrai.
ii) Dans la clause "$\forall x \in \mathbb{N},\ y \leq x$", où y est la seule variable libre, si nous remplaçons y par 0, nous obtenons un énoncé vrai, tandis que si nous remplaçons y par tout autre entier naturel, nous obtenons un énoncé faux.
iii) Dans la clause "$n|m$", si nous remplaçons n par 2 et m par 6, nous obtenons un énoncé vrai, si nous remplaçons n par 17 et m par 23, nous obtenons un énoncé faux. Si nous remplaçons n et m par des entiers naturels tels que $n > m$, nous obtenons toujours un énoncé faux (nous prouverons ceci plus tard).

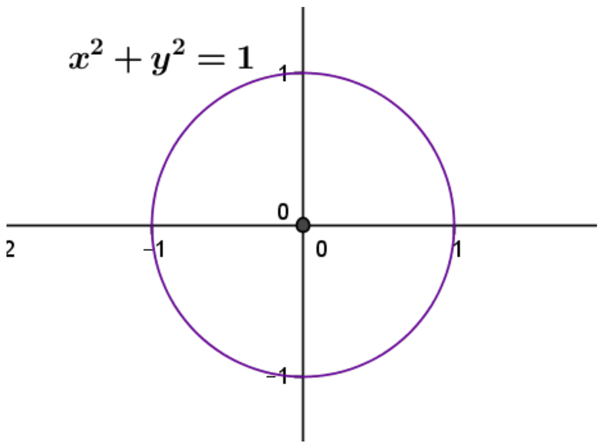


Figure 2.3: La clause "$x^2 + y^2 = 1$" possède deux variables libres et exprime dans le plan que la distance du point (x, y) à l'origine vaut 1. Elle permet ainsi de définir le cercle de centre $(0, 0)$ et de rayon 1.

2.1.3 Les définitions et les notations

Les *définitions* sont les expressions mathématiques qui introduisent de nouveaux objets ou de nouvelles notions, à partir d'objets déjà connus ou définis, et de leurs propriétés.

Exemple 2.1.5. Voici quelques exemples de définitions. L'étudiant(e) ou la lectrice n'est pas censé(e) tout connaître.
i) Un nombre réel x est dit *positif* s'il est supérieur à 0, symboliquement si $x \geq 0$.
ii) Une fonction $f : [a, b] \to \mathbb{R}$ est dite *intégrable (au sens de Riemann)* si le supremum et l'infimum de l'ensemble des intégrales de fonctions en escaliers qui respectivement minorent et majorent f, coïncident. Leur valeur commune est alors appelée *intégrale (de Riemann) de f entre a et b.*
iii) Si m et n sont des entiers naturels, on dit que m *divise* n si il existe un entier naturel d tel que $n = m.d$ (la multiplication se note souvent par un point).

Les *notations* sont les expressions mathématiques qui introduisent un nouveau symbole pour un objet bien défini, particulier ou générique, et souvent en même temps que la définition de cet objet.

Exemple 2.1.6. Voici quelques exemples contenant une notation.
i) Soit E un ensemble.
ii) Si $f : [a, b] \to \mathbb{R}$ est intégrable au sens de Riemann, on note $\int_a^b f(t)\, dt$ l'intégrale de f entre a et b.
iii) On note $m|n$ la relation "m divise n".

Remarque 2.1.7. Les notations peuvent être utilisées de deux façons : soit pour désigner de manière durable une notion clairement définie, comme dans les clauses (ii) et (iii) de l'exemple précédent, soit comme une désignation accessoire dans le flux du discours mathématique, comme dans la clause (i), pour une explication ou une démonstration par exemple.

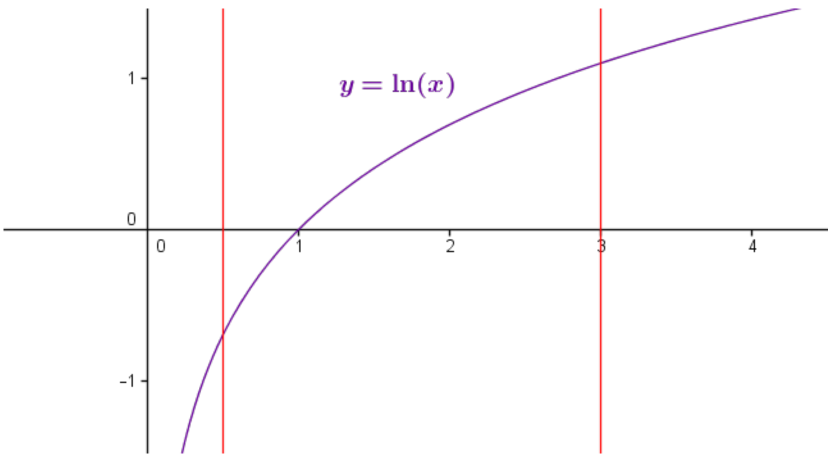


Figure 2.4: L'intégrale de la fonction logarithme entre les valeurs $\frac{1}{2}$ et 3 s'interprète comme une mesure de l'aire de la surface délimitée par la courbe de la fonction, l'axe des abscisses, et les deux droites en rouge.

2.2 Les opérations logiques sur les clauses (I)

2.2.1 Combinaisons grammaticales

Les clauses mathématiques, en tant que clauses du langage naturel, sont susceptibles de combinaisons grammaticales.
La théorie des ensembles étant la trame conceptuelle dans laquelle nous interprétons tout l'univers mathématique, la clarté et la simplicité de l'objet mathématique font que ces combinaisons sont restreintes en nombre, identifiables en principe, et parfaitement univoques, ce qui permet de libérer le discours mathématique des ambiguïtés inutiles et mathématiquement nocives du langage naturel.
En suivant une tradition qui remonte aussi loin qu'au philosophe grec Aristote et qui est fondamentale dans le développement de la logique moderne, nous utiliserons des lettres capitales $P, Q, \ldots$ pour dénoter les clauses mathématiques.
Le "P" est pour "proposition", ce qui est un peu fâcheux car si le terme est valable pour la grammaire naturelle (en grammaire française on appelle plutôt "proposition" ce que nous appelons ici "clause"), en mathématique ce mot a un sens très

précis qui sera expliqué plus tard dans le cours.
Lorsque nous nous référerons à une clause par un symbole, par exemple "P", nous en détaillerons explicitement le contenu par des guillemets, par exemple P : "$x \geq 0$".
Il est important de se souvenir que les expressions mathématiques sont des *objets linguistiques* et pas des *objets mathématiques.* Cela signifie d'une part que les symbolismes des unes et des autres ne doivent pas être confondus, et d'autre part que la théorie présentée ici n'est pas intrinsèquement mathématique, et n'a d'autre but que de fixer les idées et de préciser les usages.

Exemple 2.2.1. Soit P la clause "x est un entier naturel pair". Rappelons que selon la valeur a assignée à x, P peut être transformée en un énoncé vrai ou faux, $P(a/x)$.

Avant d'aborder les combinaisons grammaticales, c'est-à-dire logiques, des clauses mathématiques, nous avons besoin de préciser la notion d'*équivalence logique* de clauses mathématiques.
Deux énoncés P et Q sont dits *(logiquement) équivalents* si ils ont la même valeur de vérité, autrement dit si ils sont vrais tous les deux, ou faux tous les deux.
En général, deux clauses P et Q sont dites *(logiquement) équivalentes* si les énoncés obtenus en substituant les mêmes variables libres dans P et Q par les mêmes termes clos, sont (toujours) logiquement équivalents.

Exemple 2.2.2. i) Les énoncés P : "10 est un multiple de 2" et Q : "π et $\sqrt{2}$ sont des nombres réels" sont logiquement équivalents, car ils sont tous deux vrais, même si leurs significations ne sont pas explicitement liées.
ii) Les clauses P : "x est un nombre réel positif" (c'est-à-dire "$x \in \mathbb{R}$ et $x \geq 0$") et Q : "x est le carré d'un nombre réel" sont logiquement équivalentes. En effet, il est bien connu qu'un carré est toujours ≥ 0, et si $x \geq 0$, x est le carré de sa racine carrée, ce sur quoi nous aurons l'occasion de revenir ultérieurement.

Le philosophe grec Aristote (copie romaine d'un bronze perdu de Lysippe).

2.2.2 La négation d'une clause

Si P est une clause, la *négation de P* est la clause notée $\neg P$ et qui signifie "non P".
En particulier, si P est un *énoncé*, alors par définition $\neg P$ est vraie si et seulement si P est fausse.

Exemple 2.2.3. i) La négation de la clause "$x \geq 0$" (c-à-d "x est positif") est "x n'est pas positif", c-à-d "x est strictement inférieur à zéro", symboliquement $x < 0$. Notons que même si cette clause possède une variable libre x, sa signification (générique) et celle de sa négation sont claires. La première clause est appelée une *inégalité large*, sa négation une *inégalité stricte*.
ii) La négation de l'énoncé "$2|5$" ("2 divise 5"), est "2 ne divise pas 5", symboliquement "$2 \nmid 5$". Le premier énoncé est faux, donc sa négation est vraie. Revenant à la définition, cette négation se lit "il n'y a aucun entier naturel d tel que $2 \times d = 5$". Nous reviendrons sur ce type de négation à partir de la section sur la quantification.
iii) La négation de la clause "$5x + 6y = \pi$" est la clause "$5x + 6y \neq \pi$". Les deux ont deux variables libres x et y. La première clause est une *équation*, sa négation est une *inéquation*.

Remarque 2.2.4. Dans le premier exemple nous utilisons implicitement l'équivalence logique, car nous y reformulons la négation : nous interprétons "$\neg(x \geq 0)$" comme équivalente à "$x < 0$". Dans les autres exemples, nous introduisons plutôt un nouveau symbole pour la négation de la relation élémentaire impliquée ($|$ ou $=$).

2.2.3 La conjonction de deux clauses

Si P et Q sont deux clauses, la *conjonction de P et Q* est la clause notée $P \wedge Q$ qui signifie "P et Q".
Par définition, si P et Q sont des *énoncés*, alors $P \wedge Q$ est vraie si et seulement si P et Q sont tous les deux vrais.

Exemple 2.2.5. i) Si P est la clause "$x \geq 0$" et Q la clause "$x \neq 0$", où x dénote un nombre réel générique, alors la conjonction $P \wedge Q$ est logiquement équivalente à $x > 0$: en remplaçant x par n'importe quel nombre réel a, $(P \wedge Q)(a)$ est vraie si et seulement si $a > 0$.
ii) Si P est la clause "$2|y$" et Q est la clause "$3|y$", où y dénote un entier naturel générique, alors la conjonction $P \wedge Q$, qui est $(2|y) \wedge (3|y)$, est équivalente à $6|y$ (c'est une conséquence d'un théorème d'arithmétique).
iii) Si P est la clause "$x = 27$" et Q est la clause "$y = 11x$", où x et y dénotent par exemples des entiers relatifs génériques, alors $P \wedge Q$ est "$x = 27$ et $y = 11x$", un *système de deux équations*, équivalent à "$x = 27$ et $y = 297$" (on substitue la valeur de x donnée par la première équation, dans la seconde équation).

Bien sûr, on peut effectuer la conjonction de plus de deux clauses : on se ramène alors à la définition pour la conjonction de deux clauses. Par exemple, si P_1, P_2 et P_3 sont trois clauses, alors leur conjonction $P_1 \wedge P_2 \wedge P_3$ est la clause $(P_1 \wedge P_2) \wedge P_3$: si P_1, P_2 et P_3 sont des énoncés, cette clause est vraie si et seulement si P_1, P_2 et P_3 sont vrais tous les trois.

2.2.4 La disjonction de deux clauses

Si P et Q sont deux clauses, la *disjonction de P et Q* est la clause notée $P \vee Q$ et dont la signification est "P ou Q".

Par définition, si P et Q sont des *énoncés*, alors $P \vee Q$ est vraie si et seulement si P est vraie ou Q est vraie (et possiblement les deux).

Exemple 2.2.6. i) Si P est la clause "$x > 0$" et Q la clause "$x = 0$", où x dénote un nombre réel générique, alors la disjonction $P \vee Q$ est logiquement équivalente à $x \geq 0$. En effet, si a est un nombre réel quelconque, alors $(P \vee Q)(a)$ est vraie si et seulement si $a > 0$ ou $a = 0$, c'est-à-dire si et seulement si $a \geq 0$, par définition de $\geq$.
ii) Si y dénote un entier naturel générique et P est la clause "$y|2$" et Q la clause "$y|3$", alors la disjonction $P \vee Q$ est équivalente à "$y = 1$ ou $y = 2$ ou $y = 3$".
iii) Si P est la clause "$x = 27$" et Q est la clause "$x|11$", la disjonction $P \vee Q$ est équivalente à "$x = 1$ ou $x = 11$ ou $x = 27$".

Comme pour la conjonction, on peut aussi effectuer la disjonction de plus de deux clauses. Par exemple, si P_1, P_2 et P_3 sont trois clauses, alors leur disjonction $P_1 \vee P_2 \vee P_3$ est la clause $(P_1 \vee P_2) \vee P_3$: si P_1, P_2 et P_3 sont des énoncés, cette clause est vraie si et seulement si l'un d'entre eux (au moins) est vrai.

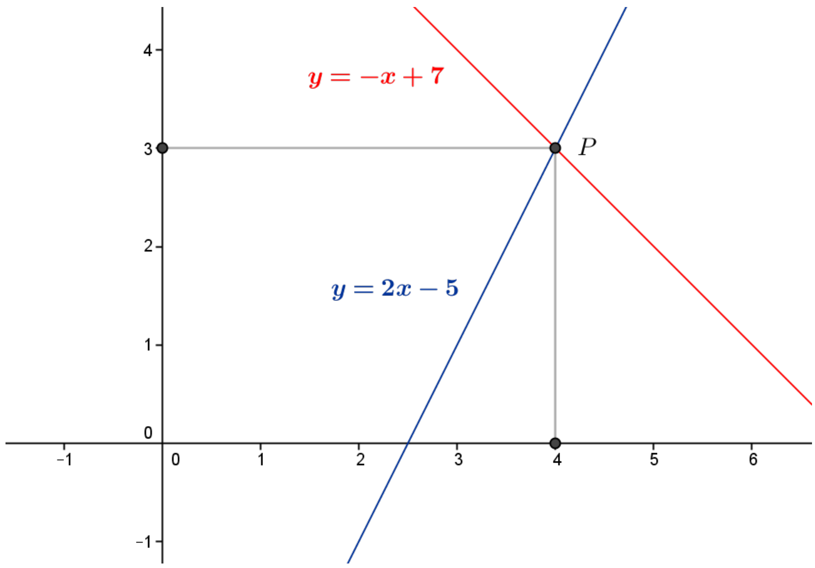


Figure 2.5: Les expressions $y = 2x-5$ et $y = -x+7$ définissent deux droites du plan. Leur conjonction est un système de deux équations, dont la solution est donnée par les coordonnées $x = 4$ et $y = 3$ du point d'intersection P des deux droites.

Exercices de la leçon

Exercice 2.2.7 (Négation). i) On rappelle que si m et n sont deux variables pour des entiers relatifs, la définition de la relation "$m|n$" est qu'il existe un entier relatif d tel que $n = m.d$. Donner une expression équivalente à la négation de $m|n$.
ii) Si E et F désignent deux ensembles, exprimer la négation de l'inclusion $E \subseteq F$ en introduisant une variable.
iii) Expliquer pourquoi, si P est un énoncé, l'énoncé "$\neg(\neg(P))$", c'est-à-dire "non(non P)", est logiquement équivalent à P.

Exercice 2.2.8 (Conjonction). i) Si n est une variable pour un entier naturel, soient P la clause "$n \geq 10$", Q la clause "$3|n$" et R la clause "$n|24$". Pour quelles valeurs de n la clause $P \wedge Q \wedge R$ devient-elle un énoncé vrai ?
ii) Donner une clause élémentaire équivalente à la conjonction "2 divise n et 3 divise n".
iii) Soient P_1, P_2 et P_3 trois énoncés. Expliquer pourquoi $(P_1 \wedge P_2) \wedge P_3$ est logiquement équivalent à $P_1 \wedge (P_2 \wedge P_3)$.

Exercice 2.2.9 (Disjonction). i) Si n désigne un entier naturel générique, donner une clause élémentaire équivalente à la disjonction de P : "$3|n$" et Q : "$6|n$".
ii) Donner une valeur de la variable x (qui dénote un nombre réel) dans la disjonction "$x \leq 1$ ou $x^2 \geq 5$", pour laquelle cette disjonction devient un énoncé faux.
iii) Soient P_1, P_2 et P_3 trois énoncés. Expliquer pourquoi $(P_1 \vee P_2) \vee P_3$ est logiquement équivalent à $P_1 \vee (P_2 \vee P_3)$.
iv) Si P_1, P_2 et Q sont trois clauses, expliquer pourquoi $Q \wedge (P_1 \vee P_2)$ est équivalente à $(Q \wedge P_1) \vee (Q \wedge P_2)$, et $Q \vee (P_1 \wedge P_2)$ est équivalente à $(Q \vee P_1) \wedge (Q \vee P_2)$.

2.3 Les opérations logiques sur les clauses (II)

2.3.1 Clauses universellement valides

Avant de poursuivre notre exposition des opérations logiques sur les clauses mathématiques, nous introduisons la notion de clause *universellement valide.*
Une clause mathématique P est dite *universellement valide*, si l'énoncé obtenu en remplaçant chaque variable libre de P par un terme clos approprié est toujours vrai.

Exemple 2.3.1. i) Si P est la clause $(x^2+2)^2 \geq 4$, où x désigne un nombre réel générique, alors P est universellement valide. En effet, si a est un nombre réel quelconque, le nombre réel a^2 est positif, donc on a $a^2+2 \geq 2$, donc $(a^2+2)^2 \geq 4$.
ii) Si P est la clause $1|m$, où m est une variable pour un entier relatif, alors P est universellement valide. En effet, si a est un entier relatif, on peut toujours écrire $a = a.1$, donc $1|a$ par définition.
iii) Si P est la clause "$(x-y)^2 = x^2 - 2xy + y^2$", où x et y sont des variables pour des nombres complexes, alors P est universellement valide. En effet, si z et w sont des nombres complexes, l'égalité $(z-w)^2 = z^2 - 2zw + w^2$ est toujours vraie.

2.3.2 L'implication de deux clauses

Si P et Q sont deux clauses, l'*implication de Q par P*, appelée "P implique Q", est la clause notée $P \Rightarrow Q$ et dont la signification est "si P, alors Q".
Intuitivement, cette clause signifie que si P est vraie, alors Q est nécessairement vraie aussi. Pour rendre cette idée précise, on définit cette clause par des opérations existantes, à savoir comme $(\neg P) \vee Q$. L'expression "$P \Rightarrow Q$" est donc une abréviation. Ceci signifie que si P et Q sont des énoncés, alors $P \Rightarrow Q$ est vraie si et seulement si P est fausse ou Q est vraie. En d'autres termes, il n'est pas possible que P soit vraie mais que Q soit fausse : c'est bien le sens intuitif de l'implication.

De ce point de vue, il faut faire attention à ce qu'il n'est pas nécessaire que les clauses P et Q aient des significations explicitement liées pour que la clause $P \Rightarrow Q$ puisse être formée, ce qui contrevient à l'intuition de la condition "si...alors" telle qu'utilisée habituellement dans le langage naturel.

Exemple 2.3.2. i) Si P est la clause "$x \geq 2$" et Q la clause "$x^2 \geq 4$", où x est une variable générique pour un nombre réel, alors l'implication $P \Rightarrow Q$ correspond à la clause "si $x \geq 2$, alors $x^2 \geq 4$". Quelle que soit la valeur choisie pour x, si $x \geq 2$ on a bien $x^2 \geq 4$, donc $P \Rightarrow Q$ est universellement valide. Si l'on remplace P par la clause élémentaire "$x \geq -2$", on peut trouver ce qu'on appelle un *contre-exemple* à $P \Rightarrow Q$: pour $x = 0$, l'énoncé $P(0)$ est "$0 \geq -2$", qui est vrai, tandis que l'énoncé $Q(0)$ est "$0^2 \geq 4$", qui est faux, donc $P(0) \Rightarrow Q(0)$ est faux, si bien que $P \Rightarrow Q$ n'est pas universellement valide.
ii) Si P est la clause "$m|n$" et Q la clause "$m \leq n$", avec m et n des variables pour des entiers naturels, alors l'implication $P \Rightarrow Q$, qui signifie "si m divise n, alors $m \leq n$", est universellement valide (nous le démontrons dans la dernière partie du cours). En revanche, si m et n sont des variables pour des entiers *relatifs*, alors l'implication $P \Rightarrow Q$ n'est plus universellement valide. Par exemple, pour $m = 2$ et $n = -6$, on a bien $2| - 6$ puisque $-6 = (-3).2$ (donc $P(2/m, -6/n)$, c'est-à-dire l'énoncé obtenu par substitution de 2 à m et de -6 à n, est vrai), tandis que l'on n'a pas $2 \leq -6$ (donc $Q(2/m, -6/n)$ est faux), donc $(P \Rightarrow Q)(2/m, -6/n)$ est faux.
iii) Si P est l'énoncé "$\sqrt{2} \in \mathbb{Q}$" et Q l'énoncé "$\pi \in \mathbb{Q}$", alors P et Q sont tous les deux faux (nous démontrerons que P est faux dans la dernière partie du cours, nous admettons le second, qui est un théorème de von Lindemann). Ainsi, l'énoncé $(\neg P) \vee Q$ est vrai, puisque $\neg P$ est vrai. Cet énoncé est $P \Rightarrow Q$, ce qui montre qu'une implication peut être vraie, tandis que sa conclusion est fausse ! En outre, cet exemple illustre qu'il n'est pas nécessaire d'avoir un lien explicite entre P et Q pour pouvoir former $P \Rightarrow Q$ et étudier les conditions de sa véracité.

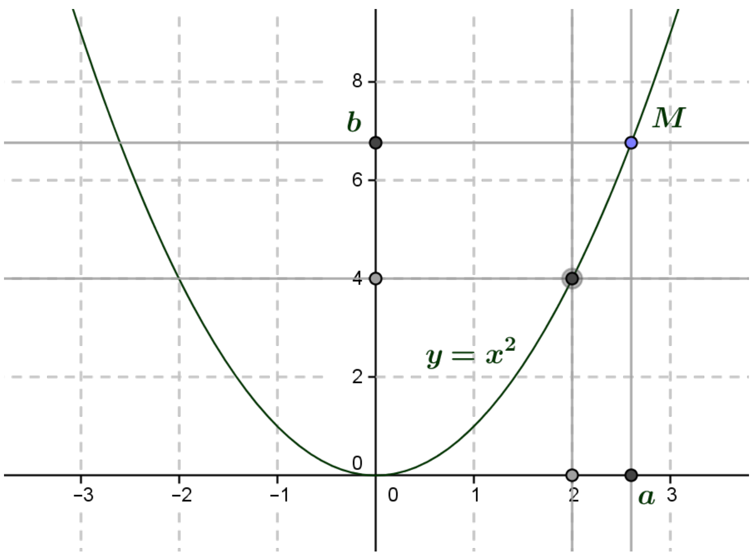


Figure 2.6: La clause "$(x \geq 2) \Rightarrow (x^2 \geq 4)$" est universellement valide : si l'abscisse a d'un point M de la parabole d'équation $y = x^2$ est ≥ 2, alors son ordonnée b est ≥ 4.

2.3.3 L'équivalence de deux clauses

Si P et Q sont deux clauses, l'*équivalence de P et Q* (à ne pas confondre avec l'équivalence logique) est la clause notée $P \Leftrightarrow Q$ et dont la signification est "P est équivalente à Q".
Intuitivement, cette clause signifie que P et Q sont conjointement valides ou conjointement invalides. Pour rendre cette idée précise, on définit ici aussi cette clause comme l'abréviation de $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$, ou encore en revenant à la définition de $P \Rightarrow Q$, $(\neg P \vee Q) \wedge (\neg Q \vee P)$.
Ceci signifie que si P et Q sont des *énoncés*, alors $P \Leftrightarrow Q$ est vraie si et seulement si P et Q sont tous deux vrais, ou bien P et Q sont tous deux faux.
Comme pour l'implication, les significations explicites de P et Q n'ont pas besoin d'être liées de manière évidente pour qu'on puisse former $P \Leftrightarrow Q$.

Remarque 2.3.3. Le rapport entre l'équivalence de deux clauses et l'équivalence logique est le suivant. Si P et Q sont deux clauses, alors P est logiquement équivalente à Q si et seulement si la clause $P \Leftrightarrow Q$ est *universellement valide*, autrement dit si l'énoncé obtenu en remplaçant toutes les variables libres de P et Q par les mêmes termes clos (c'est-à-dire les mêmes "noms" d'objets), est toujours vrai.

Exemple 2.3.4. i) Si P est la clause "$x \geq 0$" et Q la clause "x est un carré", où x est une variable pour un nombre réel, alors la clause $P \Leftrightarrow Q$ est universellement valide, car P et Q sont logiquement équivalentes. Si on remplace P par "$x > 0$", la clause $P \Rightarrow Q$ est universellement valide, mais pas la clause $Q \Rightarrow P$, puisque pour $x = 0$, $Q(0)$ est vrai et $P(0)$ est faux. La nouvelle clause $P \Leftrightarrow Q$ n'est donc pas universellement valide.
ii) Si P est la clause "$15|n$" et Q la clause "$3|n$ et $5|n$", où n désigne un entier relatif générique, alors la clause $P \Leftrightarrow Q$ est universellement valide (ceci provient d'un théorème général d'arithmétique). Si on remplace P par $-30|n$, alors la clause $P \Rightarrow Q$ est universellement valide (car $3|30$ et $5|30$), mais le nombre $n = 15$ est un contre-exemple pour $Q \Rightarrow P$, puisque $Q(15)$ est vrai, tandis que $P(15)$ est faux, donc la nouvelle clause $P \Leftrightarrow Q$ n'est pas universellement valide.
iii) Si P est la clause "$(z = i) \vee (z = -i)$" et Q la clause "$z^2 = -1$", où z est une variable pour un nombre complexe, la clause $P \Leftrightarrow Q$ est universellement valide, car il existe exactement deux nombres complexes dont le carré vaut -1, à savoir i et $-i$.

La "signification" de $P \Rightarrow Q$ et de $P \Leftrightarrow Q$ est, comme pour toutes les clauses, induite de la signification de chaque énoncé obtenu à partir de l'une d'entre elles par la substitution de termes fermés pour toutes leurs variables libres. On doit bien faire attention à remplacer les mêmes variables libres dans P et Q par les mêmes termes.

2.3.4 Vocabulaire lié à l'implication et l'équivalence

Pour terminer, il nous faut ici évoquer un aspect essentiel du vocabulaire mathématique, lié à l'implication et l'équivalence : de nombreux énoncés mathématiques se présentent comme, ou comportent, une clause de la forme "P si et seulement si Q". Il faut bien noter que l'expression mathématique "si et seulement si" n'est rien d'autre qu'une reformulation de l'équivalence de deux clauses.

Exemple 2.3.5. Si x dénote un nombre réel générique, la clause "x est positif si et seulement x est un carré" est une reformulation de la première clause de l'exemple précédent.

Précisons les choses, pour lever toute ambiguïté : dans l'expression "P si et seulement si Q", le premier "si" a trait à l'implication *inverse*, c'est-à-dire que "P si Q" signifie "$Q \Rightarrow P$", tandis que que le "seulement si" a trait à l'implication *directe*, c'est-à-dire que "P seulement si Q" signifie "$P \Rightarrow Q$" (autrement dit, on ne peut pas avoir P sans Q).
On dit aussi souvent pour $P \Rightarrow Q$ que Q est une *condition nécessaire de* P, et pour $Q \Rightarrow P$ que Q est une *condition suffisante* de P. Ainsi, $P \Leftrightarrow Q$ est synonyme de "P si et seulement si Q", ou encore de "P est une condition nécessaire et suffisante de Q".

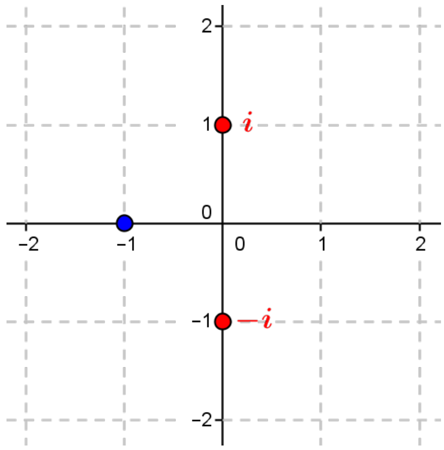


Figure 2.7: Les nombres complexes i et $-i$, représentés ici en rouge comme points du plan, sont les "racines carrées" de -1.

Exercices de la leçon

Exercice 2.3.6. i) Démontrer que la clause $n|0$, où n est un entier naturel générique, est universellement valide.
ii) Trouver un contre-exemple à l'implication $(x < 0) \Rightarrow (x^2 \geq 1/2)$, où x est une variable pour un nombre réel.
iii) Si P est la clause "$(2|m) \wedge (2|n)$" et Q la clause "$4|mn$" (où m et n sont des variables pour des entiers relatifs et mn est le produit de m et de n), trouver un contre-exemple à l'équivalence $P \Leftrightarrow Q$.
iv) Donner deux clauses mathématiques avec une variable libre dont l'implication n'est pas universellement valide. Même question avec l'équivalence.

2.4 La quantification des clauses mathématiques

2.4.1 Principe de la quantification mathématique

La théorie des ensembles étant la trame conceptuelle de la mathématique, toutes les clauses mathématiques se ramènent essentiellement à des clauses “construites” à partir de clauses élémentaires, grâce aux opérations précédentes et ce qu'on appelle les *quantifications.*
En effet, les propriétés mathématiques d'un objet particulier ou générique sont décrites *en relation à d'autres objets*, et *à l'intérieur de certains ensembles.*
A cause de l'universalité de la méta-relation $\in$ entre les objets et les ensembles, pour obtenir toute la puissance expressive du langage mathématique il n'est nécessaire de compléter la combinaison des clauses élémentaires par les opérations logiques que par l'information concernant l'*existence* d'un objet ayant une “sous-propriété” ou l'*universalité* des objets ayant une telle sous-propriété. Par une “sous-propriété”, nous entendons de manière informelle une propriété décrite par une partie d'une clause.

Exemple 2.4.1. Si P est la clause “$x \geq 0$ et $x^2 \neq 5$”, alors les clauses “$x \geq 0$” et “$x^2 \neq 5$” expriment des sous-propriétés de la propriété générique exprimée par P.

Si l'on considère la propriété P de l'exemple, il est naturel de se poser deux questions :
- existe-t-il un nombre réel a ayant la propriété P (c'est-à-dire tel que $P(a/x)$ est vrai) ?
- tous les nombres réels a ont-ils la propriété P ?
Ces deux possibilités correspondent aux deux types de quantifications, *existentielle* et *universelle*, et l'expression de ces deux types de faits suffit à compléter notre description du langage mathématique.
La quantification n'est pas un artifice de la science mathématique : elle correspond à l'addition de l'adverbe “tous” ou “tout” dans les expressions naturelles (pour la quantification universelle), ou de l'adverbe “certains” ou “certain” pour la quantification existentielle.
Ces deux quantifications étaient déjà bien connues dans l'Antiquité grecque; on les retrouve notamment chez Aristote, et à travers son héritage dans la logique de la scolastique médiévale.

Exemple 2.4.2. Un exemple de ces quantifications naturelles tiré de l'ancienne logique grecque (Aristote) est le suivant : “tous les hommes sont mortels”. Ici, l'expression “les hommes sont mortels” est complétée par le “quantificateur 'tous' ”. L'analogue pour le quantificateur existentiel est l'expression “certains hommes sont mortels”. La négation naturelle de “tous les hommes sont mortels” est “certains hommes ne sont pas mortels”; il existe une relation essentielle entre ces deux quantifications, liée à la négation, que nous aborderons ici dans le cadre mathématique propre.

Nous avons déjà vu des exemples de quantifications, et ils montrent que les énoncés mathématiques “intéressants” doivent souvent être construits à partir de clauses

élémentaires contenant des variables libres, de manière à pouvoir affirmer quelque chose de plus élaboré que de simples relations particulières (même si certaines équations, entre nombres et fonctions par exemple, ont un intérêt mathématique essentiel; par exemple, l'étudiant(e) ou le lecteur pourra comprendre à son niveau, à la fin du semestre, la *formule d'Euler*, soit $e^{i\pi} + 1 = 0$).
Nous avons aussi utilisé la quantification pour introduire des définitions, comme dans l'exemple de la divisibilité. Il s'agit donc d'un mode ubiquitaire de "transformation" des expressions mathématiques, qui "ferme" les clauses par rapport aux variables qu'elles contiennent.

Thomas d'Aquin, l'un des maître de la philosophie scolastique (retable de Carlo Crivelli, 1494).

2.4.2 La quantification existentielle

Si P est une clause et x une variable pour les éléments d'un ensemble E, la *quantification existentielle de P par x*, notée "$\exists x \in E,\ P$" (lire "il existe $x \in E$ tel que P"), est la clause dont la signification est "il existe au moins un élément a de E tel que la clause obtenue en remplaçant x par a dans P, est valide".

Remarque 2.4.3. i) La notation de la quantification peut varier selon les textes mathématiques : par exemple, on pourra écrire $(\exists x \in E)\ P$ pour $\exists x \in E,\ P$. En général, il n'y a aucune difficulté pour s'adapter à ces variations mineures : l'important est l'usage du symbole $\exists$.
ii) Il se peut que la variable x n'apparaisse pas dans P, ou que P possède d'autres variables libres que x : nous ne préjugeons rien à ce sujet.

Si x est la seule variable libre de P, alors la clause "$\exists x \in E,\ P$" est un énoncé qui par définition est vrai exactement lorsqu'il existe un élément a de E tel que l'énoncé $P(a/x)$ est vrai. Cet énoncé est faux exactement lorsque pour aucun élément a de E, l'énoncé $P(a/x)$ n'est vrai.

Exemple 2.4.4. i) Si m et n dénotent des entiers relatifs génériques, la relation "m divise n" ("$m|n$") a été définie par une quantification existentielle. En effet, si P est la clause "$m.d = n$", où d est une nouvelle variable générique pour un entier relatif, la relation $m|n$ est définie par la clause $\exists d \in \mathbb{Z},\ P$, soit "$\exists d \in \mathbb{Z},\ m.d = n$",

dont la signification intuitive est qu'il existe un entier relatif d pour lequel $m.d = n$, ce qui traduit effectivement l'idée que n est un multiple de m.
ii) Si x est une variable pour un nombre réel, nous avons affirmé dans la leçon précédente que la clause P : "$x \geq 0$" est équivalente à Q : "x est un carré" (c'est une propriété de l'ensemble $\mathbb{R}$, que nous démontrerons ultérieurement). L'expression rigoureuse de Q se fait à l'aide d'un quantificateur existentiel, sous la forme "$\exists y \in \mathbb{R},\ y^2 = x$", clause comprenant la variable libre x et la variable y pour un nombre réel, *quantifiée* existentiellement.
iii) Si m et n dénotent des entiers naturels génériques, la relation habituelle $m \leq n$ peut se définir à partir de l'addition et d'une quantification existentielle, par la clause $\exists p \in \mathbb{N},\ m + p = n$, pour p une nouvelle variable pour un entier naturel. Noter l'analogie avec la définition de la divisibilité.

Remarque 2.4.5. Lorsqu'on écrit une clause sous forme symbolique, on ne précise pas les ensembles correspondants aux éléments génériques dénotés par les variables libres : cela est précisé dans le contexte. Par contraste, sous la forme dans laquelle nous présentons ici la quantification, on a tendance à écrire l'ensemble correspondant à chaque variable quantifiée ("$\exists x \in E,\ P$" plutôt que "$\exists x\ P$"). Il n'est cependant pas interdit d'omettre l'ensemble de référence dans la quantification, surtout lorsque toutes les variables se rapportent au même ensemble. Le symbolisme n'est pas forcément synonyme de formalisme.

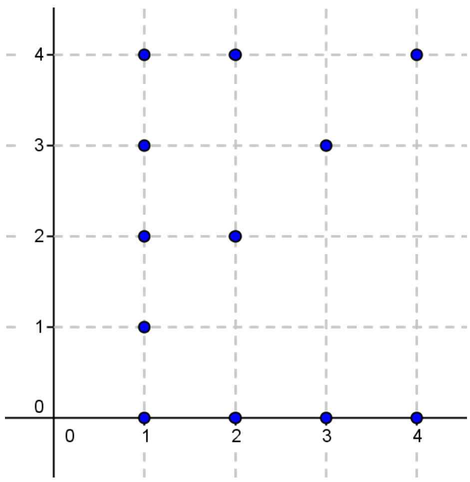


Figure 2.8: Les points représentés en bleu sont ceux dont la première coordonnée divise la seconde.

2.4.3 La quantification universelle

Si P est une clause et x une variable pour les éléments d'un ensemble E, la *quantification universelle de P par x*, notée "$\forall x \in E,\ P$" (lire "pour tout $x \in E$, P") est la clause dont la signification est "pour tous les éléments a de E, la clause obtenue en substituant x par a dans P, est valide".

Remarque 2.4.6. Comme pour la quantification existentielle, on peut trouver des variations de cette notation, que nous emploierons occasionnellement, comme par exemple $(\forall x \in E)\ P$.

Si x est la seule variable libre de P, alors la clause "$\forall x \in E,\ P$" est un énoncé qui est vrai exactement lorsque pour tout élément a de E, l'énoncé $P(a/x)$ est vrai. Il est donc faux exactement lorsqu'il existe un élément a de E pour lequel $P(a/x)$ est faux (c'est la version mathématique de "tous les hommes sont mortels").
On voit ainsi qu'il existe une "dualité" entre la quantification existentielle et la quantification universelle, qui passe par la négation et est analogue d'une dualité entre la disjonction et la conjonction. Nous aurons l'occasion d'y revenir dans deux sections.

Remarque 2.4.7. De manière analogue au rapport existant entre l'équivalence logique et la validité universelle de l'équivalence de deux clauses, il existe un rapport entre la quantification universelle et la validité universelle. Si P est une clause possédant une unique variable libre x pour les éléments d'un ensemble E, alors P est universellement valide si et seulement si l'énoncé "$\forall x \in E,\ P$" est vrai, ce qui découle immédiatement des définitions.

Exemple 2.4.8. i) Si P est la clause "$(x \geq 0) \Rightarrow (\exists y \in \mathbb{R},\ y^2 = x)$", avec x un nombre réel générique ("si x est positif, alors x est un carré), alors l'énoncé $\forall x,\ P$ est vrai car P est universellement valide (voir l'exemple précédent).
ii) Un entier naturel p est appelé un nombre *premier* s'il est différent de 1 et n'est divisible que par 1 et lui-même. On peut exprimer cette propriété par la clause suivante, un peu complexe, où p est un entier naturel générique : "$(p \neq 1) \wedge (\forall n \in \mathbb{N}, n|p \Rightarrow ((n = 1) \vee (n = p)))$". C'est un bon exercice que de décomposer cette écriture symbolique pour comprendre pourquoi elle exprime que p est un nombre premier.
iii) Contrairement aux nombres réels, tout nombre complexe possède une racine carrée ! Ceci peut s'exprimer symboliquement par l'énoncé "$\forall z \in \mathbb{C}, \exists w \in \mathbb{C},\ w^2 = z$". On observe ici une combinaison des deux types de quantification.

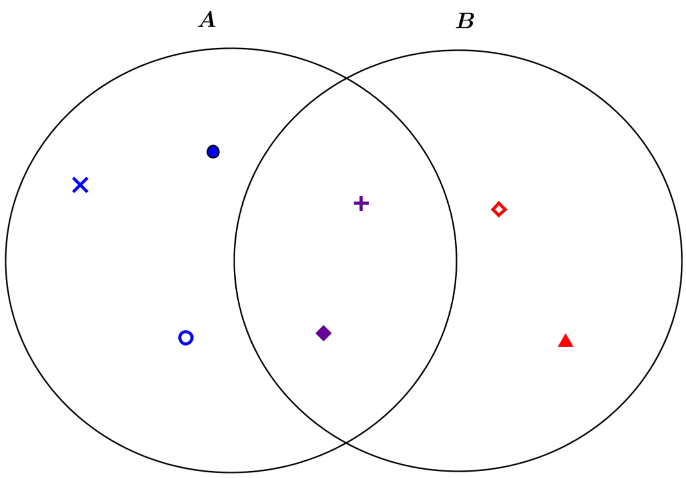


Figure 2.9: L'ensemble A n'est pas inclus dans l'ensemble B : en effet, il n'est pas vrai que tout élément de A est élément de B, autrement dit il existe $a \in A$ tel que $a \notin B$.

Exercices de la leçon

Exercice 2.4.9. i) Utiliser une quantification existentielle pour exprimer la relation $m < n$ entre deux entiers naturels à partir de la seule addition et du nombre 1.
ii) L'énoncé $\exists x,\ x^2 = 2$, où x dénote un nombre réel générique, est-il vrai ?
iii) Exprimer symboliquement la propriété "0 est le plus petit entier naturel" (c'est-à-dire : "0 est inférieur à tout entier naturel") à l'aide de la relation $\leq$ et d'une quantification universelle.
iv) Ecrire un énoncé faux comportant une quantification universelle.

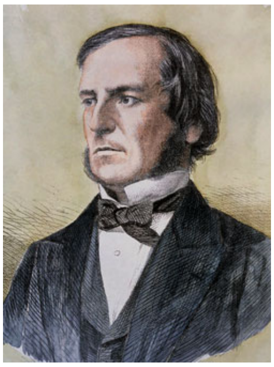
2.5 Relations entre les opérations logiques (I)

2.5.1 Le jeu des opérations logiques et la négation

Les opérations et quantifications précédentes sont tout ce qu'il est nécessaire d'introduire en termes de logique mathématique naturelle pour formuler tous les énoncés mathématiques à partir de clauses élémentaires.
Ceci illustre la puissance de la théorie des ensembles et de sa logique associée, les deux étant profondément enracinées dans l'intuition naturelle et la réalité mathématique.
De manière informelle, on peut considérer que *toute clause mathématique est obtenue à partir de clauses élémentaires par le seul usage des opérations* $\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow$ *et des quantifications* $\exists$ *et* $\forall$.
La "symbolisation" des clauses mathématiques ne change pas leur statut linguistique, et doit être utilisée de manière consistante avec une formulation correcte dans le langage naturel.
La possibilité de la négation des clauses mathématiques induit une relation entre les opérations logiques "duales" que sont $\wedge$ et $\vee$, et entre les quantifications "duales" $\exists$ et $\forall$, et ces dualités doivent être maîtrisées pour pouvoir couramment travailler avec l'expression mathématique. Comprendre la signification de la négation d'une clause est en effet essentiel dans le processus de détermination de la véracité ou de la fausseté d'un énoncé complexe particulier.
Plus généralement, il existe de nombreuses relations entre les opérations logiques et les quantifications, dont certaines ont déjà été esquissées (rappelons que nous avons défini l'implication et l'équivalence à partir de $\neg$, $\wedge$ et $\vee$). Dans cette fin de chapitre, nous considérons la relation de la négation avec les autres opérations logiques et les quantifications. L'étudiant(e) ou la lectrice acquerra les autres relations naturellement par l'usage.

2.5.2 Calcul Booléen

Le "calcul Booléen", nommé d'après le logicien, mathématicien et philosophe George Boole, traite de l'entrelacement des opérations de négation, conjonction et disjonction.
Nous considérerons seulement ici les lois fondamentales suivantes. En écrivant des clauses symboliquement, nous considérons implicitement que la négation est pri-



George Boole, logicien, mathématicien et philosophe.

oritaire sur $\wedge$ et $\vee$, ce qui permettra d'alléger parfois la notation en supprimant certaines parenthèses. Si P et Q sont des clauses, alors les trois lois fondamentales du calcul Booléen sont les suivantes. Les exemples sont donnés pour illustrer la "gymnastique" de conversion des formes d'expressions.

Loi 2.5.1. *Les clauses $\neg(\neg P)$ et P sont logiquement équivalentes.*

En effet, si P est un énoncé, alors par définition $\neg(\neg P)$ est vrai si et seulement si $\neg P$ est faux, si et seulement si P est vrai.
Rappelons que ce type de "loi" n'est pas ici un théorème mathématique, car il porte sur le langage naturel. La règle est tirée de l'application aux énoncés - pour lesquels on a une définition claire de la négation en termes de valeurs de vérité - et étendue à toutes les clauses, puisque le sens de celles-ci a été défini grâce aux énoncés obtenus à partir d'elles par substitution.
Cette première règle peut se reformuler simplement en disant que P est la négation de $\neg P$, ce qui paraît évident au vu de la définition de $\neg$, mais doit être établi clairement.

Exemple 2.5.2. i) Si P est la clause "$x > 0$" ("x est strictement positif") pour x un nombre réel générique, alors la négation de P est (logiquement équivalente à) "$x \leq 0$" ("x est négatif"), donc on vérifie bien que $\neg(\neg P)$, et partant P, est logiquement équivalente à "x n'est pas négatif" (ce que nous savions déjà par définition des notions de positivité et de négativité...).
ii) Si n désigne un entier relatif générique et P est la clause "$0 \nmid n$" ("0 ne divise pas n"), alors $\neg P$ est équivalente à $0|n$. Or, par définition de la relation $|$, 0 ne peut diviser que 0, donc $\neg P$ est équivalente à $n = 0$, si bien que P elle-même est équivalente à $n \neq 0$.

Les deux lois suivantes ont été formulées par le mathématicien et logicien Augustus De Morgan.

Loi 2.5.3 (Première loi de De Morgan)**.** *Les clauses $\neg(P \wedge Q)$ et $\neg P \vee \neg Q$ sont logiquement équivalentes.*

En effet, si P et Q sont des énoncés, alors par définition $\neg(P \wedge Q)$ est vrai si et seulement si $P \wedge Q$ est faux, si et seulement si P est faux ou Q est faux, si et

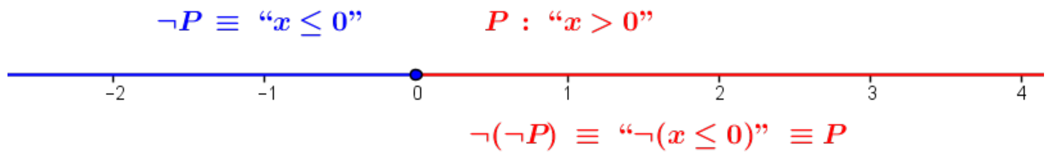


Figure 2.10: La propriété P : "$x > 0$ décrit l'ensemble des réels > 0 (en rouge); sa négation $\neg P$, équivalente à "$x \leq 0$", décrit donc l'ensemble des réels ≤ 0 (en bleu). La double négation $\neg(\neg P)$ décrit le même ensemble que P (le signe $\equiv$ signifie "équivalent".

seulement si $\neg P \vee \neg Q$ est vrai.
Comme pour la règle sur la double négation, on s'appuie ici sur l'intuition naturelle sous-jacente à l'idée de vérité d'un énoncé, et on généralise à toutes les clauses mathématiques grâce au principe d'équivalence logique.
Dans ce cas toutefois, on s'appuie sur une relation *intuitive* entre la négation, la conjonction et la disjonction : dire que l'énoncé $P \wedge Q$ est faux si et seulement si P est faux ou Q est faux relève de cette intuition, inhérente au sens même des termes "et" et "ou".

Exemple 2.5.4. Si x est une variable pour un nombre réel, P la clause "$x \geq 0$" et Q la clause "$x \leq 0$", alors la clause $P \wedge Q$ est équivalente à $x = 0$. Sa négation est par définition équivalente à $x \neq 0$, et par la première loi de De Morgan, elle est donc équivalente à $\neg P \vee \neg Q$, soit par équivalence logique à $(x < 0) \vee (x > 0)$ (voir l'exemple précédent).

Loi 2.5.5 (Deuxième loi de De Morgan)**.** *Les clauses $\neg(P \vee Q)$ et $\neg P \wedge \neg Q$ sont logiquement équivalentes.*

En effet, si P et Q sont des énoncés, alors $\neg(P \vee Q)$ est vrai si et seulement si $P \vee Q$ est faux, si et seulement si P est faux et Q est faux, si et seulement si $\neg P \wedge \neg Q$ est vrai.
Les remarques faites à propos de la première loi de De Morgan sont valables ici également (cette loi est en quelque sorte "duale" à la première).

Exemple 2.5.6. Si n est une variable pour un entier naturel, P la clause "$7 \nmid n$" (c'est-à-dire 7 ne divise pas n) et Q la clause "$11 \nmid n$", alors la clause $\neg(P \vee Q)$ est par la seconde loi équivalente à la clause $\neg P \wedge \neg Q$, soit encore à "$(7|n) \wedge (11|n)$", qui pour des raisons élémentaires d'arithmétique (voir le troisième cours) est équivalente à "$77|n$".

Exercices de la leçon

Exercice 2.5.7. i) Si P et Q sont des clauses, expliquer pourquoi $\neg(\neg P \wedge \neg Q))$ est équivalente à $P \vee Q$. A quelle clause plus simple $\neg(\neg P \vee \neg Q)$ est-elle équivalente ?
ii) Créez des clauses P et Q à une variable libre de votre choix, et vérifiez la validité

Augustus De Morgan, mathématicien et logicien.

des lois de De Morgan pour P et Q.
iii) Soient P : "$x > -1$" et Q : "$x < 1$". Donner une clause équivalente à $\neg(P \wedge Q)$ ne contenant aucune négation.
iv) A quelle clause ne mentionnant pas de conjonction la clause $P \wedge \neg Q$ est-elle équivalente ?

2.6 Relations entre les opérations logiques (II)

2.6.1 Négation de l'implication

En ce qui concerne l'implication il est important de comprendre sa négation, pour pouvoir *réfuter* une clause de la forme $P \Rightarrow Q$, c'est-à-dire pour démontrer sa fausseté. Nous avons déjà rencontré implicitement cette négation lorsque nous avons traité des *contre-exemples* pour les implications.
Nous revenons à la définition rigoureuse de $P \Rightarrow Q$, c'est-à-dire $\neg P \vee Q$. La négation de $P \Rightarrow Q$ est donc par définition $\neg(\neg P \vee Q)$, ce qui d'après le calcul Booléen est logiquement équivalent à $(\neg\neg P) \wedge (\neg Q)$ (seconde loi de De Morgan), ou encore $P \wedge \neg Q$ (par réduction de la double négation).
Si P et Q sont des énoncés, ceci signifie que par définition, $P \Rightarrow Q$ est faux exactement quand P est vrai et Q est faux, ce qui s'accorde avec l'intuition que P n'implique pas Q précisément dans ce cas.
Notons que si P est faux, quelle que soit la valeur de vérité de Q, l'implication $P \Rightarrow Q$ est vraie ! Ainsi, l'implication mathématique a été définie pour prendre exclusivement en compte le rapport de la véracité de Q à la véracité de P lorsque P est vraie.

Exemple 2.6.1. Si x désigne un nombre réel générique, P la clause "$\exists y,\ y^2 = x$" et Q la clause "$x \geq 0$", alors nous avons déjà vu que la clause $P \Rightarrow Q$ est universellement valide (un carré est toujours positif), donc sa négation, équivalente à $P \wedge \neg Q$ est universellement fausse : cela signifie qu'aucun carré réel ne peut être strictement négatif.

2.6.2 Négation de l'équivalence

En ce qui concerne l'équivalence, par définition la négation de $P \Leftrightarrow Q$ est $\neg((P \Rightarrow Q) \wedge (Q \Rightarrow P))$, ce qui selon le calcul Booléen est logiquement équivalent à $(\neg(P \Rightarrow Q)) \vee (\neg(Q \Rightarrow P))$ (première loi de De Morgan), qui est équivalent par ce qui précède à $(P \wedge \neg Q) \vee (Q \wedge \neg P)$.
Si P et Q sont des énoncés, montrer que $P \Leftrightarrow Q$ est faux, c'est-à-dire que P n'est pas équivalent à Q, est donc équivalent à mettre en défaut l'une des deux implications $P \Rightarrow Q$ ou $Q \Rightarrow P$, soit à montrer que soit P est vrai et Q est faux, soit Q est vrai et P est faux, ce qui une fois encore est en accord avec l'intuition de l'équivalence.

Exemple 2.6.2. Si n est un entier relatif générique, P est la clause "$7|n$" et Q la clause "$11|n$", alors $P \Leftrightarrow Q$ n'est pas universellement valide. Pour le voir, on peut chercher à montrer que $P \Rightarrow Q$ n'est pas toujours vraie, autrement dit trouver une valeur a de n pour laquelle $P(a/n) \wedge \neg Q(a/n)$ est vraie; pour $n = 7$, on a bien $7|7$ et $11 \nmid 7$, donc $P(7/n)$ est vraie, et $Q(7/n)$ est fausse.

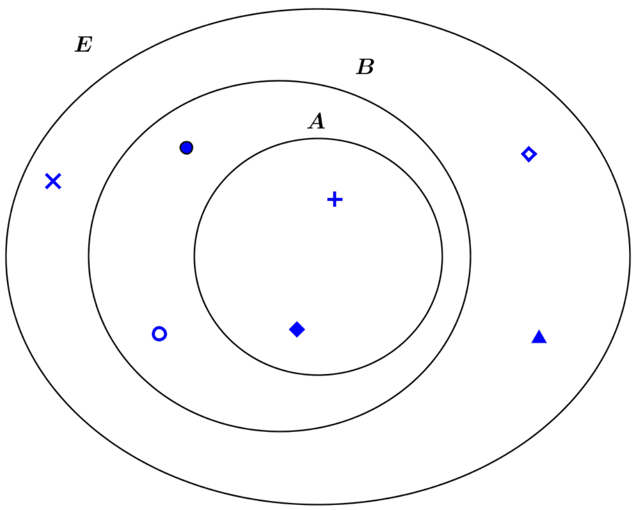


Figure 2.11: Si A et B sont respectivement les sous-ensembles de E formés des objets ayant les propriétés P et Q, alors $P \Rightarrow Q$ est universellement valide car $A \subseteq B$, mais $Q \Rightarrow P$ n'est pas valide, car on n'a pas $B \subseteq A$.

2.6.3 Négation et quantifications

Nous avons vu que la quantification des clauses est une caractéristique typique de l'expression mathématique, qui lui donne sa puissance singulière, en ce qu'elle permet d'énoncer au-delà des combinaisons logiques de relations élémentaires entre objets particuliers.
Il est essentiel de comprendre la relation entre la négation et la quantification, qui est analogue à la relation entre la négation et les deux opérations $\vee$ et $\wedge$ (leçon précédente). Cette relation a d'ailleurs été anticipée dans la description précédente des quantifications existentielle et universelle.

2.6.4 Négation et quantification existentielle

Si P est une clause et x une variable pour un élément générique d'un ensemble E, et si il n'y a pas d'autre variable libre que x dans P (même si x n'apparaît pas dans P), l'énoncé "$\neg(\exists x \in E,\ P)$" signifie par définition qu'il est faux qu'il existe un élément a de E pour lequel $P(a/x)$ est vrai.
En d'autres termes, il signifie que *pour tout élément a de E, $P(a/x)$ est faux*, c'est-à-dire $\neg P(a/x)$ est vrai.
En utilisant le quantificateur universel, ceci signifie que l'énoncé "$\neg(\exists x \in E, P)$" est logiquement équivalent à "$\forall x \in E,\ \neg P$". Ceci est donc la *définition* que nous adoptons pour la négation de "$\exists x \in E,\ P$" en général, c'est-à-dire quand il peut y avoir dans P d'autres variables libres que x.

Remarque 2.6.3. Ici encore, on ne fait que préciser des usages et le sens - ensembliste - qu'on donne intuitivement aux quantifications, par rapport à la négation : "l'équivalence" précédente dans le cas de deux énoncés ne fait qu'exprimer l'intuition qu'on a de la relation entre les deux quantifications.

Exemple 2.6.4. i) La négation de l'énoncé P : "$\exists x \in \mathbb{R},\ x < 0$", est équivalente à l'énoncé "$\forall x \in \mathbb{R},\ x \geq 0$", qui bien sûr est faux.
ii) La négation de la clause $m|n$, où m et n désignent des entiers naturels génériques, est celle de "$\exists d \in \mathbb{N},\ m.d = n$"; elle est équivalente à "$\forall d \in \mathbb{N},\ m.d \neq n$", soit "$n$ n'est pas un multiple de m".

2.6.5 Négation et quantification universelle

De même, si P ne contient pas d'autre variable libre éventuelle que x, l'énoncé "$\neg(\forall x \in E,\ P)$" signifie qu'il n'est pas vrai que pour tout $a \in E$, $P(a/x)$ soit vrai. Intuitivement, il signifie qu'il existe au moins un élément a de E pour lequel $P(a/x)$ est faux, ou encore qu'il existe $a \in E$ pour lequel $\neg P(a/x)$ est vrai.
En utilisant le quantificateur existentiel, ceci signifie que "$\neg(\forall x \in E,\ P)$" est logiquement équivalent à "$\exists x \in E,\ \neg P$". C'est la définition que nous adoptons, à nouveau, pour la négation de "$\forall x \in E,\ P$" en général, lorsque P peut contenir d'autres variables libres éventuelles que x.

Exemple 2.6.5. i) L'énoncé "$\forall n \in \mathbb{N},\ 0 \leq n$" est vrai, donc sa négation, équivalente à "$\exists n \in \mathbb{N},\ n < 0$", est fausse. Par contre, l'énoncé "$\exists n \in \mathbb{Z},\ n < 0$", est vrai.
ii) La négation de la clause P : "$\forall y \in \mathbb{R},\ y^2 \neq x$", où x est un nombre réel générique, est équivalente à la clause "$\exists y \in \mathbb{R},\ y^2 = x$". Etant donné que la seconde clause est équivalente à "$x \geq 0$" comme nous l'avons déjà évoqué, la clause P est équivalente à $x < 0$.

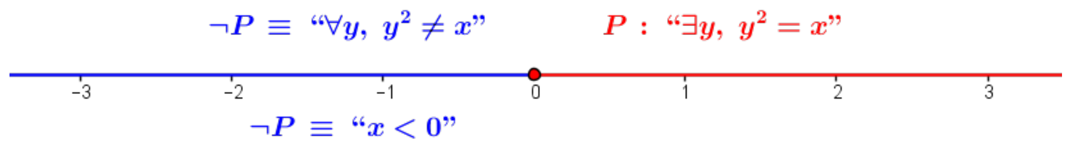


Figure 2.12: La propriété P : "$\exists y,\ y^2 = x$ est équivalente à "$x \geq 0$", donc sa négation, équivalente à "$\forall y,\ y^2 \neq x$", est équivalente à "$x < 0$".

Exercices de la leçon

Exercice 2.6.6. i) L'implication "$(3|n) \Rightarrow (6|n)$" (n entier naturel générique) est-elle universellement valide ? Sinon, écrire sa négation sous forme d'une conjonction et trouver un contre-exemple.
ii) L'équivalence "$(x > 0) \Leftrightarrow (\exists y,\ y^2 = x)$", où x est une variable pour un nombre réel, n'est pas universellement valide. Écrire sa négation sous forme d'une disjonction et donner un contre-exemple.
iii) (Subtil) Si P est une clause, x une variable qui n'apparaît pas dans P et a un objet approprié, quelle est la clause $P(a/x)$ obtenue en substituant a pour x dans P ?
iv) Écrire une clause équivalente à la négation de la clause P : "$\exists p \in \mathbb{N},\ m+p = n$" (où m et n sont des entiers naturels génériques) commençant par une quantification universelle. A quelle clause élémentaire $\neg P$ est-elle équivalente ?
v) Écrire une clause équivalente à la négation de la clause P : "$\forall x \in \mathbb{R},\ x < 0$", commençant par une quantification existentielle et ne comportant aucune négation.
vi) (Plus difficile) Soit P l'énoncé $\forall x \in \mathbb{R}, \exists y \in \mathbb{R},\ y^2 = x$. Écrire un énoncé équivalent à $\neg P$ commençant par deux quantifications, et en déduire que P est faux.

Chapitre 3

Propriétés Élémentaires des Ensembles Naturels

Félicitations ! A ce stade nous avons fait l'effort "technique" principal du cours. Nous n'avons pas voulu en évoquer les aspects un peu pénibles à l'avance pour ne pas vous décourager. Il y a souvent des passages de ce genre dans les textes mathématiques, c'est ainsi. La bonne nouvelle, c'est qu'à chaque situation de ce genre on fait une avancée significative en mathématiques. Le chapitre précédent était important et vous aurez sans doute à y revenir.
Avec l'acquisition du langage et de l'expression mathématiques, nous avons franchi une étape importante. Nous allons désormais pouvoir approfondir rigoureusement la connaissances des ensembles fondamentaux $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ et $\mathbb{R}$, que nous avons seulement décrits de manière intuitive dans la première partie.
En rappelant les inclusions fondamentales $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$ abordées dans le premier chapitre, nous introduisons dans cette partie du cours les propriétés spécifiques élémentaires de chacun de ces quatre ensembles. Ces propriétés sont fondées sur la définition de ces ensembles et l'intuition de leurs objets, et ont trait aux opérations $+$ et $\times$ et aux relations $|, \leq$ et $<$. Elles ont toutes été évoquées de manière plus ou moins formelle dans les exemples et les exercices du chapitre 2.
Grâce à tout le travail effectué en logique mathématique naturelle dans les leçons précédentes, nous pouvons maintenant exprimer ces propriétés de manière claire et si nécessaire, symbolique, et distinguer des propriétés analogues mais distinctes entre ces ensembles.
Certains types de propriétés mathématiques sont préservées lorsqu'on les applique à des sous-ensembles (en adaptant les quantifications à des variables concernant les sous-ensembles en question s'il y a lieu). C'est pourquoi nous commençons l'exposé par les propriétés de $\mathbb{R}$, dont *certaines* se transmettent naturellement à $\mathbb{N}$, $\mathbb{Z}$ et $\mathbb{Q}$.
Toutes ces propriétés sont introduites ici sur le plan *intuitif* : nous en admettons beaucoup comme des *postulats*, c'est-à-dire des énoncés considérés comme vrais mais indémontrables. En fait, on pourrait considérer que les jeux de propriétés énoncés pour chacun des ensembles $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ et $\mathbb{R}$ sont en quelque sorte une manière "axiomatique" de définir ou de décrire ces ensembles. Nous cherchons seulement ici à exposer les propriétés essentielles qui permettent de travailler avec l'intuition mathématique.

Que l'étudiant(e) ou le lecteur minimaliste se rassure : au fur et à mesure, nous aborderons dans ce semestre la *construction* des ensembles fondamentaux et la définitions des opérations et relations fondamentales à partir de $\mathbb{N}$: pour ce dernier nous verrons qu'on peut le "caractériser" par des axiomes, pour les autres nous pourrons *redémontrer* les propriétés présentées ici comme conséquences de leur définition.

3.1 L'ensemble $\mathbb{R}$ des nombres réels (I)

La "structure de base" de l'ensemble $\mathbb{R}$, appelé aussi *droite réelle* (expression qui met l'accent sur le caractère à la fois arithmétique et géométrique de $\mathbb{R}$), consiste en les opérations habituelles d'addition (notée $+$) et de multiplication (notée $\times$), ainsi qu'en *l'ordre linéaire (ou strict)*, noté $<$. Rappelons que *l'ordre large*, noté $\leq$, est défini ou caractérisé pour des nombres réels x, y par $x \leq y$ si et seulement si $x < y$ ou $x = y$.
Nous listons ici les propriétés élémentaires de ces opérations et relations, que nous avons déjà demandé à l'étudiant(e) ou la lectrice de mobiliser dans les nombreux exemples et exercices du précédent chapitre.
Même si à ce niveau de compréhension, ces propriétés sont *intuitives*, nous pouvons les formuler de manière rigoureuse grâce à l'expression mathématique spécifique.

3.1.1 Les relations $<$ et $\leq$

Nous commençons par les propriétés des deux relations d'ordre $<$ et $\leq$.

Propriété 3.1.1. Si x, y, z sont des nombres réels :
i) on a $x \leq x$
ii) si $x < y$ et $y < z$, alors $x < z$
iii) si $x \leq y$ et $y \leq z$, alors $x \leq z$
iv) si $x \leq y$ et $y \leq x$, alors $x = y$
v) on ne peut avoir à la fois $x < y$ et $y < x$
vi) on a $x < y$ si et seulement si $x \leq y$ et $x \neq y$
vii) on a $x \leq y$ si et seulement si $x < y$ ou $x = y$
viii) on a toujours soit $x < y$, soit $x = y$, soit $y < x$.

Toutes ces propriétés sont encore valides pour n'importe quel sous-ensemble de $\mathbb{R}$, donc en particulier pour les sous-ensembles $\mathbb{N}$, $\mathbb{Z}$ et $\mathbb{Q}$ de $\mathbb{R}$, autrement dit si nous choisissons x, y, z comme entiers naturels, entiers relatifs ou nombres rationnels, elles sont encore vraies.
Cependant, il faut faire attention à ce que toutes les propriétés mathématiques d'un ensemble donné ne sont pas toujours préservées dans un sous-ensemble : nous en verrons bientôt des exemples.
Pour l'étudiant(e) ou le lecteur curieux, il faut savoir que la préservation d'une propriété à un sous-ensemble dépend de la *manière* dont on peut écrire cette propriété; nous n'aborderons pas ceci en détail à cet endroit du cours.

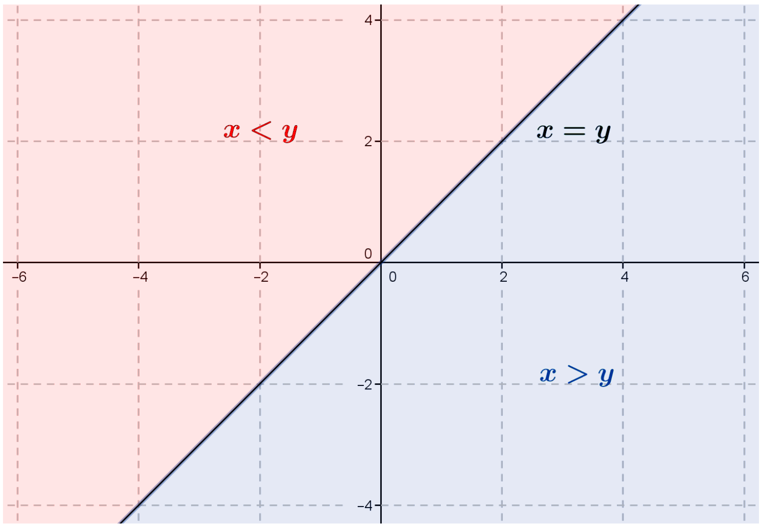


Figure 3.1: Représentation de la relation $<$ entre les nombres réels : la droite d'équation $x = y$ coupe le plan en deux parties. A droite se trouvent les points (x, y) tels que $x > y$ (en bleu), à gauche les points (x, y) tels que $x < y$ (en rose).

3.1.2 L'addition des nombres réels

En ce qui concerne l'addition et son rapport aux relations précédentes, on a les propriétés suivantes, parmi lesquelles on trouvera aussi le rapport des inégalités aux changements de signes.

Propriété 3.1.2. Si x, y, z sont des nombres réels :
i) on a $x + 0 = 0 + x = x$
ii) on a $(x + y) + z = x + (y + z)$ (on dit que l'addition est *associative*)
iii) on a $x + y = y + x$ (on dit que l'addition est *commutative*)
iv) si $x < y$, alors $x + z < y + z$
v) si $x \leq y$, alors $x + z \leq y + z$
vi) si $x < y$, alors $-x > -y$
vii) si $x \leq y$, alors $-x \geq -y$.

Comme pour les propriétés de $<$ et $\leq$, ces propriétés de l'addition sont encore valables dans les ensembles $\mathbb{N}$, $\mathbb{Z}$ et $\mathbb{Q}$.

3.1.3 La multiplication des nombres réels

En ce qui concerne la multiplication et son rapport à l'addition et aux relations d'ordre, on a les propriétés suivantes; on rappelle qu'on note $x.y$ et même souvent xy le produit $x \times y$ de deux nombres réels x et y.

Propriété 3.1.3. Si x, y, z sont des nombres réels :
i) on a $x.1 = x$ et $x.0 = 0$
ii) on a $(x.y).z = x.(y.z)$ (la multiplication est associative)
iii) on $x.y = y.x$ (la multiplication est commutative)
iv) $z.(x + y) = z.x + z.y$ (on dit que la multiplication est *distributive* sur l'addition)

v) si $z > 0$ et $x < y$, alors $z.x < z.y$
vi) si $z \geq 0$ et $x \leq y$, alors $z.x \leq z.y$
vii) si $z < 0$ et $x < y$, alors $z.x > z.y$
viii) si $z \leq 0$ et $x \leq y$, alors $z.x \geq z.y$.

Remarque 3.1.4. Les propriétés (vii) et (viii) généralisent les propriétés (vi) et (vii) de la liste 3.1.2, au sens où ces dernières en sont des cas particuliers, pour $z = -1$.

A nouveau, toutes ces propriétés de la multiplication sont encore valides dans les sous-ensembles $\mathbb{N}$, $\mathbb{Z}$ et $\mathbb{Q}$ de $\mathbb{R}$. La propriété suivante, de nature différente, est très importante.

Propriété 3.1.5. Pour tous nombres réels x, y, si $xy = 0$ alors $x = 0$ ou $y = 0$.

On peut la reformuler de manière peut-être plus suggestive par contraposée, un mode de raisonnement que nous exposerons dans le dernier chapitre : si x et y sont des nombres réels non nuls, alors le produit $x.y$ est non nul.

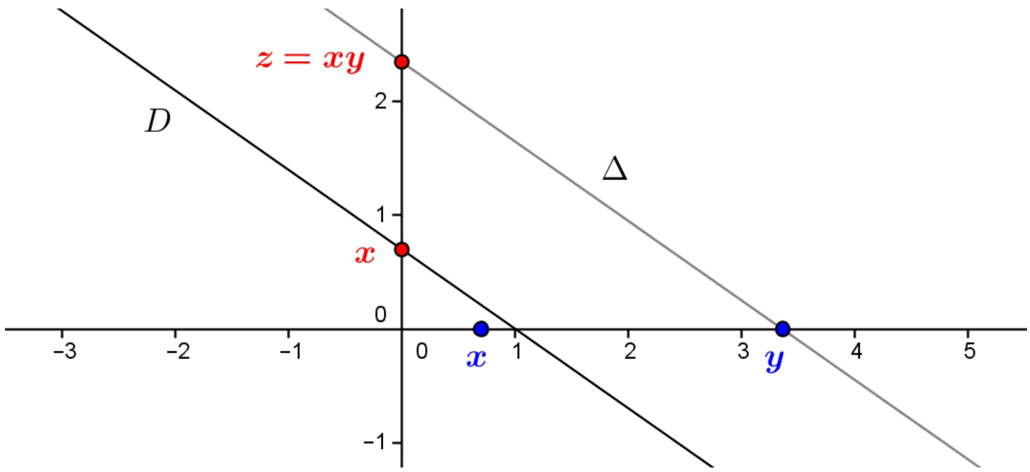


Figure 3.2: On peut représenter géométriquement la multiplication de deux nombres réels x et y. En reportant x en ordonnées et en joignant le point $(1, 0)$ au point $(0, x)$ on obtient la droite D; la droite Δ, parallèle à D et passant par le point $(y, 0)$, coupe l'axe des ordonnées en $(0, z)$. Par le théorème de Thales (voir le cours de Géométrie), on a $y/1 = z/x$, d'où $z = xy$!

Exercices de la leçon

Comme pour les exercices et les problèmes en général, il n'est pas anormal ou inquiétant de ne pas pouvoir résoudre ces exercices à la première tentative. L'essentiel est de *chercher* à les résoudre, pour mettre en oeuvre les connaissances acquises.

Exercice 3.1.6. o) Réécrire tous les propriétés de la leçon sous forme purement symbolique, en utilisant le chapitre 2.
i) Sachant que $1 < \sqrt{2}$, $\sqrt{2} < 2$, $2 < e$, $e < 3$, $3 < \pi$ et $\pi < 4$ (ce qu'on peut écrire abusivement $1 < \sqrt{2} < 2 < e < 3 < \pi < 4$), comparer à l'aide de la relation $<$ les nombres réels $-\sqrt{2}, -\pi$ et $-e$. Représenter tous ces nombres sur la droite réelle.

ii) Établir que que $e - \sqrt{2} > 0$.
iii) Établir que $-2\pi < -6$.

3.2 L'ensemble $\mathbb{R}$ des nombres réels (II)

3.2.1 Puissances entières d'un nombre réel

Il est utile d'ajouter ici les règles de formation des *puissances* d'un nombre réel par un nombre entier relatif. D'abord, si $x \in \mathbb{R}$ et $n \in \mathbb{N}$, l'expression x^n ("x puissance n") dénote intuitivement la multiplication de x par lui-même, "n fois" : nous définirons cette idée proprement dans le dernier chapitre section grâce à la notion de *définition par récurrence.*
Intuitivement, "multiplier x par lui-même 0 fois" conduit à la "puissance zéro" de x, qui par convention est 1. Ceci peut se justifier de la manière suivante : ajouter 0 fois un nombre, c'est ajouter 0, le nombre qui ajouté à un autre nombre ne le change pas; de manière analogue, multiplier 0 fois par un nombre, c'est le multiplier par 1, le nombre qui multipliant un autre nombre ne le change pas.
Ensuite, si x est non nul, alors le nombre x^n est non nul par la propriété 3.1.5 (le produit de deux nombres réels non nuls est non nul), ce qu'il faudrait démontrer par récurrence (et que l'étudiant(e) ou la lectrice saura faire à la fin du dernier chapitre). On définit alors x^{-n} comme $1/x^n$, à partir de x^{-1} étant conçu comme l'*inverse* de x, soit $1/x$, ce qui permet de définir x^n pour tout réel x non nul et tout entier relatif n : si $x \neq 0$ et $n < 0$, alors $-n > 0$ et on peut définir x^n comme $x^{-(-n)}$, c'est-à-dire $1/(x^{-n})$!

Exemple 3.2.1. Par exemple, le nombre π est strictement positif, d'où $-\pi < 0$, et on a donc $(-\pi)^{-3} = \frac{1}{(-\pi)^{-(-3)}} = 1/(-\pi)^3 = 1/-\pi^3 = -1/\pi^3$.

Les propriétés essentielles des puissances entières sont résumées comme suit :

Propriété 3.2.2. Si x, y sont des nombres réels et n, m des entiers relatifs, on a :
i) si $n \in \mathbb{N}$ ou $x, y \in \mathbb{R}^*$, alors $(xy)^n = x^n y^n$
ii) si $n, m \in \mathbb{N}$ ou $x, y \in \mathbb{R}^*$, alors $x^{n+m} = x^n.x^m$
iii) si $n, m \in \mathbb{N}$ ou $x, y \in \mathbb{R}^*$, alors $(x^n)^m = x^{nm}$.

Remarque 3.2.3. Dans l'exemple précédent, nous avons utilisé la propriété suivante, qui est une conséquence de la propriété (i) : pour tout nombre réel x et pour tout entier naturel n, on a $(-x)^n = ((-1).x)^n = (-1)^n.x^n$, ce qui vaut x^n si n est pair (car alors $(-1)^n = 1$) et $-x^n$ si n est impair (car alors $(-1)^n = -1$).

3.2.2 La propriété d'Archimède

La propriété suivante est essentielle à l'analyse réelle et est introduite à ce niveau, insistons, comme un postulat ou axiome, c'est-à-dire un principe considéré valide sur la base de l'intuition, mais qui n'est pas démontré; nous la démontrerons dans le cours d'analyse réelle de ce semestre.

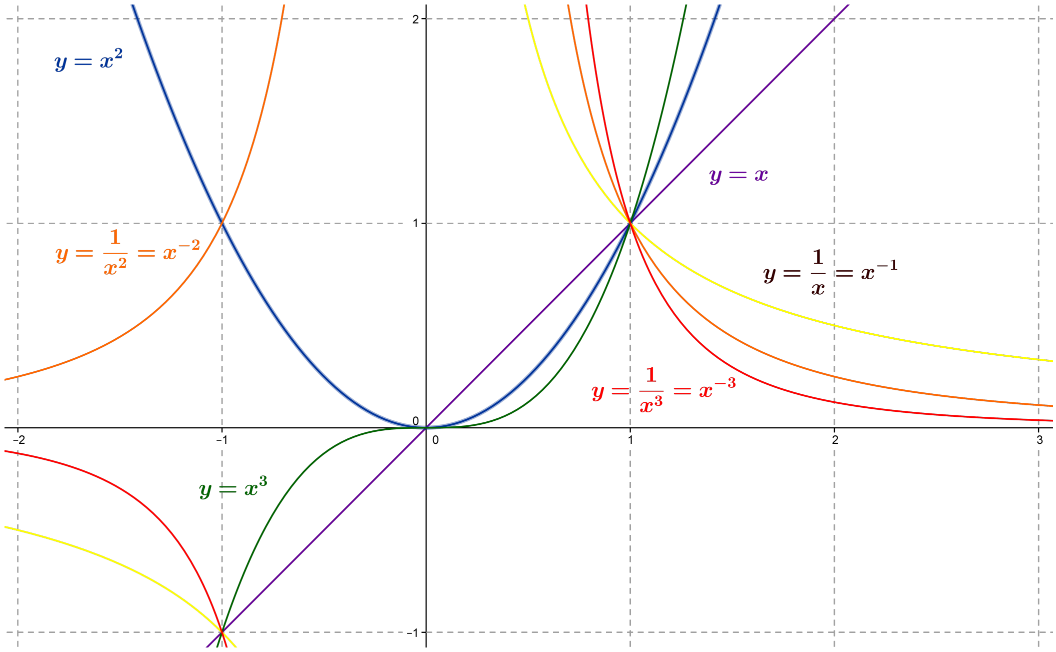


Figure 3.3: Représentation des fonctions puissance x, x^2, x^3, $x^{-1} = 1/x$, $x^{-2} = 1/x^2$ et $x^{-3} = 1/x^3$. Observer la symétrie complexe de la figure.

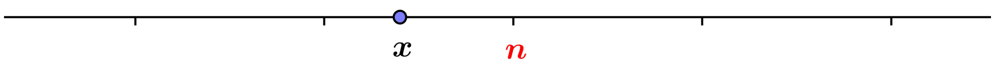


Figure 3.4: Propriété d'Archimède : quelque soit le nombre réel x, il existe un nombre entier n tel que $x < n$ (les points de la droite représentent les réels, les graduations représentent les entiers).

Elle dit intuitivement que “l'ensemble $\mathbb{N}$ des entiers naturels n'est pas borné dans l'ensemble $\mathbb{R}$ des nombres réels”, ou bien qu'“il n'existe pas de nombre réel plus grand que tout entier naturel”, ou encore de manière plus rigoureuse, que “pour tout nombre réel, il existe un entier naturel qui est plus grand que ce nombre”. En utilisant la quantification et un peu de symbolisme, elle s'énonce comme suit :

Axiome 1 (Propriété d'Archimède)**.** *Pour tout nombre réel x, il existe un entier naturel n tel que $x < n$.*

Dans la dernière partie de ce cours nous démontrerons des résultats intéressants grâce à la propriété d'Archimède, qui établissent notamment un rapport fondamental entre la division euclidienne des entiers relatifs et la possibilité de mesurer des grandeurs réelles. Ceci donnera de la substance à l'idée un peu vague que “l'ensemble $\mathbb{R}$ est de nature à la fois arithmétique et géométrique”.

3.2.3 La valeur absolue

La dernière notion que nous voulons introduire à propos de l'ensemble $\mathbb{R}$ est celle de *valeur absolue* d'un nombre réel x, qui est un nombre réel noté $|x|$ nous donnant, indépendamment du signe de x, son "amplitude" en tant que grandeur. Si x est un nombre réel, on définit $|x|$, la valeur absolue de x, comme suit :
- soit $x \geq 0$ et la valeur absolue de x est par définition x lui-même (on dit qu'on *pose* $|x| = x$)
- soit $x < 0$ et la valeur absolue de x est par définition le nombre positif de même "amplitude", soit $-x$ (on pose $|x| = -x$).
Les propriétés élémentaires de la valeur absolue sont les suivantes :

Propriété 3.2.4. Pour tous nombres réels x, y, z, on a :
i) $|x| = 0$ si et seulement si $x = 0$
ii) $|xy| = |x||y|$
iii) $|x + y| \leq |x| + |y|$.

En fait, ces propriétés peuvent être *démontrées* à partir de la définition de la valeur absolue et des propriétés de $+$ et $\leq$ précédemment évoquées. L'étudiant(e) ou le lecteur pourra s'exercer à le faire, peut-être après avoir lu une première fois la dernière partie du cours sur le raisonnement mathématique.

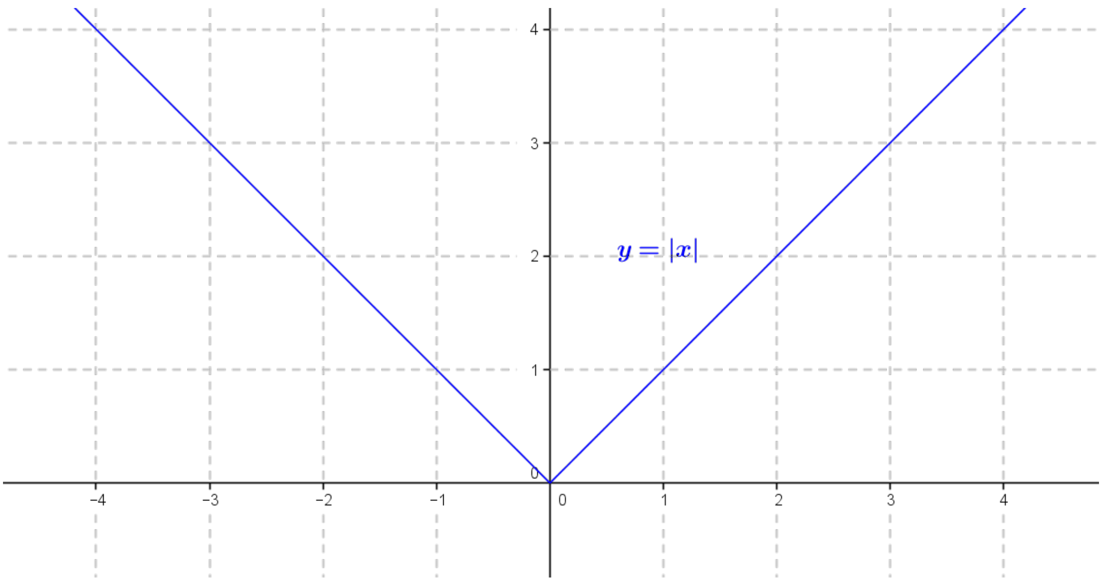


Figure 3.5: Représentation graphique de la fonction valeur absolue $|x|$. Observer la symétrie du graphe.

Exercices de la leçon

Bien que nous n'ayons pas encore abordé les méthodes de démonstration, dans certains exercices nous demandons une démonstration. Il s'agit d'un "argument", comme dans une discussion quotidienne ou philosophique, et l'étudiant(e) ou la lectrice est donc capable, à notre avis, d'argumenter pour établir la véracité d'un fait mathématique simple. C'est une bonne préparation que de s'y exercer avant d'aborder un exposé des méthodes habituelles.

Exercice 3.2.5. i) Écrire les propriétés des puissances entières d'un nombre réel sous forme d'énoncés symboliques.
ii) On rappelle que si $x \in \mathbb{R}_+$, $\sqrt{x}$ est le nombre réel positif dont le carré vaut x. Calculer $((-2)^2)^3$, $(\sqrt{3})^5$ et $(5\pi)^3$.
iii) Soient a et b deux nombres réels, tels que $b > 0$. En utilisant la propriété d'Archimède, expliquer pourquoi il existe un entier naturel n tel que $nb > a$.
iv) Si x, y et z sont trois nombres réels, démontrer que $|x||y + z| \leq |xy| + |xz|$.

3.3 L'ensemble $\mathbb{N}$ des nombres entiers naturels

3.3.1 L'addition et les relations d'ordre

Par définition, 0 est le plus petit entier naturel. Cette propriété se traduit dans l'énoncé P suivant : "pour tout entier naturel n, on a $0 \leq n$", symboliquement "$\forall n \in \mathbb{N},\ 0 \leq n$".
La propriété analogue pour les entiers relatifs, c'est-à-dire P' : "$\forall n \in \mathbb{Z},\ 0 \leq n$" n'est pas vraie, car sa négation $\neg P'$ est vraie : il existe un entier relatif n, tel que $n < 0$ (énoncé logiquement équivalent à $\neg P'$, par les règles évoquées dans le chapitre précédent).
La "position" singulière de 0 dans $\mathbb{N}$ se reformule de la manière suivante comme propriété particulière de l'ensemble $\mathbb{N}$ lui-même :

Propriété 3.3.1. Il existe un entier naturel n, tel que pour tout entier naturel m, on a $n \leq m$, symboliquement : "$\exists n \in \mathbb{N}, \forall m \in \mathbb{N},\ n \leq m$".

A cause de cette propriété, et comme nous l'avons déjà évoqué, l'opération $+$ et les relations $\leq$ et $<$ sont liées dans $\mathbb{N}$ de la manière suivante :

Propriété 3.3.2. Pour tous entiers naturels m et n, on a :
i) $m \leq n$ si et seulement si il existe un entier naturel p tel que $m + p = n$, symboliquement on a $(m \leq n) \Leftrightarrow (\exists p \in \mathbb{N}, m + p = n)$.
ii) $m < n$ si et seulement si il existe un entier naturel non nul p tel que $m + p = n$, symboliquement on a $(m < n) \Leftrightarrow (\exists p \in \mathbb{N},\ p \neq 0 \wedge m + p = n)$.

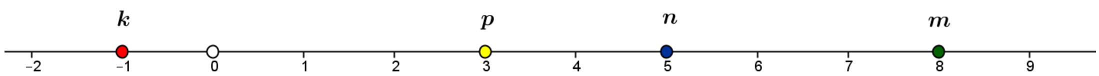


Figure 3.6: 0 n'est pas le plus petit entier relatif : par exemple, il existe $k = -1$ tel que $k < 0$. Le nombre $n = 5$ est strictement inférieur au nombre $m = 8$, et on vérifie qu'il existe un entier strictement positif $p = 3$ tel que $n + p = m$.

3.3.2 La multiplication et la divisibilité

L'arithmétique est cette partie de la mathématique qui traite de la relation de "divisibilité". Cette notion repose sur l'intuition de la multiplication des entiers naturels

: il est habituel de dire qu'un entier naturel n est un *multiple* d'un entier naturel m si la multiplication de m par un "certain entier naturel d" donne comme résultat n. Nous avons déjà vu que mathématiquement, ceci se traduit comme "il existe un entier naturel d, tel que $m.d = n$", ce qui s'écrit symboliquement

$$\exists d \in \mathbb{N},\ m.d = n.$$

Cette expression définit une relation entre les entiers naturels m et n que nous avons déjà introduite précédemment, soit "n est un multiple de m" (ou "m est un diviseur de n"), pour laquelle on utilise une notation spécifique : "$m|n$". On dit encore que m *divise* n. Nous voyons que la définition de cette relation à partir de la multiplication est l'exact analogue *dans* $\mathbb{N}$ de la définition de la relation $\leq$ à partir de l'addition.

Remarque 3.3.3. Attention, même si on peut définir la divisibilité dans $\mathbb{Z}$, ce n'est plus l'analogue de la relation $\leq$, au moins pas dans le sens présent. Nous en reparlerons dans la section suivante.

La *négation* de cette relation, c'est-à-dire "n n'est pas un multiple de m" ou "m ne divise pas n", est écrite symboliquement "$m \nmid n$", et se traduit en toutes lettres par "il n'existe pas d'entier naturel d tel que $m.d = n$". L'inexistence d'un élément d'un ensemble donné ayant une certaine propriété s'exprime également, par la dualité entre les deux quantificateurs, en disant que la propriété est fausse pour tous les éléments de l'ensemble en question, et une traduction mathématique de "$m \nmid n$" est donc la clause équivalente "pour tout entier naturel $d \in \mathbb{N}$, on n'a pas $m.d = n$", ou symboliquement

$$\forall d \in \mathbb{N},\ m.d \neq n,$$

"$m \neq n$" signifiant "m est différent de n" et étant une abréviation, on le rappelle, de "$\neg(m = n)$".
Voici les propriétés élémentaires de la relation de divisibilité dans $\mathbb{N}$:

Propriété 3.3.4. Pour tous entiers naturels m, n, p, on a :
i) $m|0$
ii) $1|m$
iii) si $m|n$ et $n|p$, alors $m|p$
iv) si $m|n$ et $n \neq 0$, alors $m \leq n$
v) si $m|n$ et $n|m$, alors $m = n$.

Ces propriétés aussi se démontrent à partir des définitions; l'étudiant(e) ou le lecteur est invité(e) à essayer de le faire et à y revenir si nécessaire après avoir étudié la dernière section, sur le raisonnement mathématique.

Remarque 3.3.5. Le nombre 1 joue un rôle analogue pour la multiplication au nombre 0 pour l'addition. Cela se reflète dans la divisibilité, puisque pour tout entier naturel n, on a $1|n$. La propriété analogue à la propriété 3.3.1) est donc vérifiée dans $\mathbb{N}$: $\exists n \in \mathbb{N}, \forall m \in \mathbb{N},\ n|m$ ("il existe un plus petit élément pour la relation de divisibilité").
En revanche, alors qu'il n'existe pas de plus grand élément pour la relation $\leq$ (c'est-à-dire un entier plus grand que tous les autres), étant donné que pour tout entier naturel n, on a $n|0$, la propriété "$\exists n \in \mathbb{N}, \forall m \in \mathbb{N},\ m|n$" est vérifiée ("il existe un plus grand élément pour la relation de divisibilité").

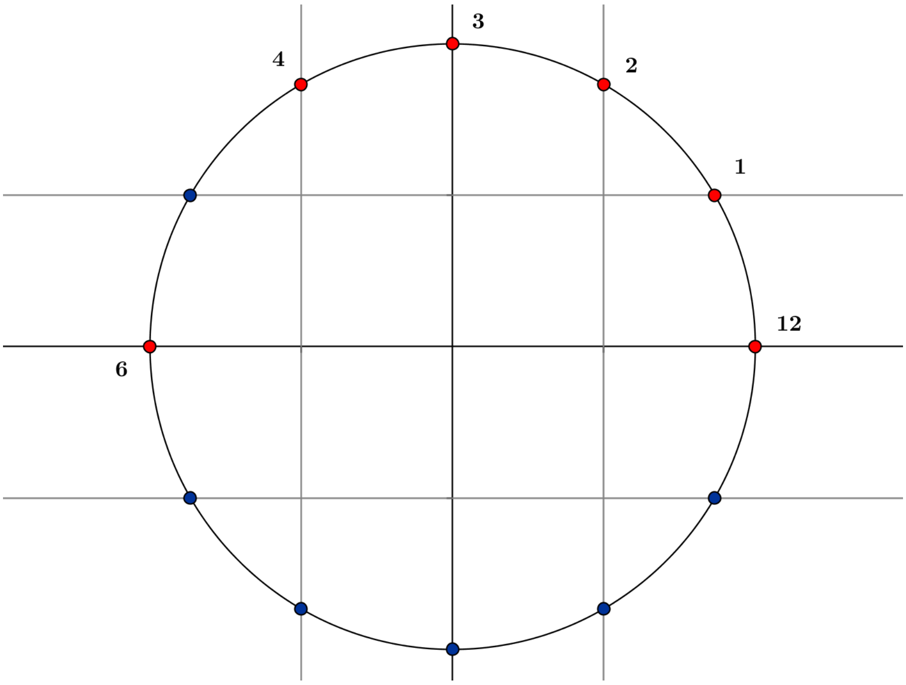


Figure 3.7: Comment diviser un cercle en douze arcs de longueurs égales. En rouge sont représentés tous les nombres entiers naturels qui divisent 12 : on a $12 = 1 \times 12 = 2 \times 6 = 3 \times 4$.

Exercices de la leçon

Exercice 3.3.6. i) Écrire un énoncé équivalent à la négation de la propriété 3.3.1 commençant par un quantificateur universel.
ii) Démontrer les propriétés 3.3.4.
iii) Ecrire un énoncé équivalent à $m < n$ analogue à celui donné dans la leçon en 3.3.2(ii) mais n'utilisant ni la négation, ni la relation $\neq$.
iv) Écrire un énoncé, symbolique ou non, qui exprime qu'il n'existe pas d'entier naturel plus grand que tous les autres.
v) A partir du fait que "0 est un multiple universel" dans $\mathbb{N}$, nous avons évoqué que l'énoncé "$\exists n \in \mathbb{N}, \forall m \in \mathbb{N},\ m|n$" est vrai. Démontrer que l'énoncé "$\exists n \in \mathbb{N}^*, \forall m \in \mathbb{N}^*,\ m|n$" (soit "il existe un plus grand élément pour la divisibilité dans $\mathbb{N}^*$"), est faux. On rappelle que $\mathbb{N}^*$ est l'ensemble des entiers naturels non nuls.

3.4 L'ensemble $\mathbb{Z}$ des nombres entiers relatifs

3.4.1 Les relations d'ordre et l'addition dans $\mathbb{Z}$

Nous avons dit dans la section précédente que la propriété "$\exists n \in \mathbb{N}, \forall m \in \mathbb{N},\ n \leq m$" est vraie dans $\mathbb{N}$ (3.3.1), donc par définition sa négation est fausse.
Nous avons aussi évoqué la propriété analogue obtenue en remplaçant les entiers naturels par les entiers relatifs, autrement dit où les variables m et n dénotent désormais des entiers *relatifs* génériques : cette négation se lit "pour tout entier relatif n, il existe un entier relatif m tel que $m < n$", et traduit l'idée intuitive qu'*il*

n'existe pas de plus petit entier relatif.
Cette propriété est vraie dans $\mathbb{Z}$, puisque si nous choisissons un entier relatif n, alors l'entier $m = n - 1$ est tel que $m < n$. Nous résumons ainsi :

Propriété 3.4.1. Pour tout $n \in \mathbb{Z}$, il existe $m \in \mathbb{Z}$ tel que $m < n$, symboliquement "$\forall n \in \mathbb{Z}, \exists m \in \mathbb{Z},\ m < n$".

A cause de cette propriété, le rapport entre l'addition et les relations $\leq$ et $<$ dans $\mathbb{Z}$ est différent de celui qui existe entre elles dans $\mathbb{N}$.
Par exemple, il n'est plus vrai que si m et n sont deux entiers *relatifs*, on a $m \leq n$ si et seulement si il existe $p \in \mathbb{Z}$ tel que $m + p = n$ (ce qui serait l'énoncé analogue à 3.3.2(i), si les variables dénotent des entiers relatifs). En effet, pour tous nombres $m, n \in \mathbb{Z}$, puisqu'on peut effectuer la soustraction $n-m$, on peut écrire $m+(n-m) = n$, donc l'entier relatif $p = n - m$ convient toujours ! On ne peut plus *définir* la relation $\leq$ dans $\mathbb{Z}$ à partir de la seule addition d'éléments de $\mathbb{Z}$ en général.
Il faut donc modifier différemment la propriété 3.3.2 de la section précédente, en choisissant des variables dans des ensembles différents, pour énoncer une propriété analogue :

Propriété 3.4.2. Pour tous entiers *relatifs* m et n, on a :
i) $m \leq n$ si et seulement si il existe un entier *naturel* p tel que $m + p = n$, symboliquement on a $(m \leq n) \Leftrightarrow (\exists p \in \mathbb{N},\ m + p = n)$
ii) $m < n$ si et seulement si il existe un entier *naturel* p non nul tel que $m + p = n$, symboliquement on a $(m < n) \Leftrightarrow (\exists p \in \mathbb{N},\ p \neq 0 \wedge m + p = n)$.

Remarque 3.4.3. Insistons : l'écriture symbolique de ces deux propriétés est la même que dans 3.3.2, mais il s'agit ici d'une *autre* propriété, puisqu'on la définit sur les entiers *relatifs* et plus sur les entiers *naturels* : la variable auxiliaire quantifiée p est prise dans $\mathbb{N}$, et pas dans $\mathbb{Z}$, donc on n'a pas simplement "transposé" la clause d'un ensemble à l'autre.

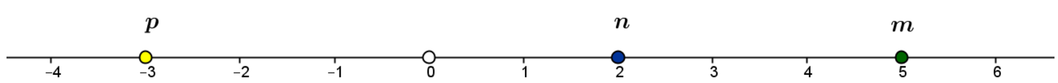


Figure 3.8: L'entier relatif $m = 5$ est strictement supérieur à l'entier relatif $n = 2$, et pourtant il existe un entier relatif $p = -3$ tel que $m + p = n$.

3.4.2 La relation de divisibilité dans $\mathbb{Z}$

Il est souvent utile en arithmétique, même dans la théorie élémentaire des entiers naturels, de faire usage de l'opération de soustraction $-$ sur $\mathbb{Z}$. En fait, l'ensemble $\mathbb{Z}$ s'avère en un sens être un environnement plus approprié pour certaines questions d'arithmétique.
C'est pourquoi la notion de divisibilité, et les notions associées comme la division euclidienne, les nombres premiers, les nombres premiers entre eux... sont étendues dans ce contexte, ce que nous étudierons en détail dans la suite de ce semestre (au

troisième cours).
Ici, nous prenons pour la relation de divisibilité $m|n$ dans $\mathbb{Z}$, comme nous l'avons déjà fait dans la section précédente, *exactement la même définition que dans* $\mathbb{N}$, autrement dit nous dirons pour deux entiers *relatifs* m et n que "m divise n", ce qu'on note "$m|n$", si il existe un entier $d \in \mathbb{Z}$ tels que $n = m.d$, soit "$\exists d \in \mathbb{Z},\ n = m.d$".
Voici les propriétés élémentaires de la relation de divisibilité dans $\mathbb{Z}$, analogues (mais pas identiques) à celles de la divisibilité dans $\mathbb{N}$:

Propriété 3.4.4. Pour tous $m, n, p \in \mathbb{Z}$, on a :
i) $m|0$
ii) $1|m$
iii) si $m|n$ et $n|p$, alors $m|p$
iv) si $m|n$ et $n \neq 0$, alors $|m| \leq |n|$
v) si $m|n$ et $n|m$, alors $m = n$ ou $m = -n$ (c'est-à-dire $|m| = |n|$).

Ici aussi ces propriétés sont des conséquences assez directes de la définition. On pourra les admettre en première lecture, et y revenir après avoir acquis le dernier chapitre.

Remarque 3.4.5. Contrairement à ce que nous avons vu pour l'addition et l'ordre large, il n'est précisément pas possible de caractériser la relation de divisibilité $m|n$ dans $\mathbb{Z}$ par la clause analogue "$\exists d \in \mathbb{N},\ n = d.m$". L'équivalence des deux clauses est fausse (voir les exercices), et c'est exactement l'analogue de la clause qui ne permet *pas* de caractériser l'ordre large dans $\mathbb{Z}$ par rapport à l'addition, que nous avons utilisée pour *définir* la divisibilité dans $\mathbb{Z}$.

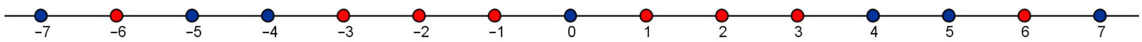


Figure 3.9: En rouge sont représentés tous les diviseurs de 6 (et donc aussi de -6) dans $\mathbb{Z}$.

Exercices de la leçon

Exercice 3.4.6. i) Démontrer que pour tout entier relatif n, on a $-1|n$.
ii) Démontrer les propriétés 3.4.4.
iii) On note $\mathbb{N}^*$ l'ensemble des nombres entiers naturels non nuls. Reformuler la propriété 3.4.2(ii) à l'aide de $\mathbb{N}^*$.
iv) Reformuler la propriété 3.4.2(i) à l'aide d'une variable auxiliaire pour un entier relatif et de la valeur absolue.
v) Montrer que l'équivalence "$(m|n) \Leftrightarrow (\exists d \in \mathbb{N},\ m.d = n)$" est fausse dans $\mathbb{Z}$.

3.5 L'ensemble $\mathbb{Q}$ des nombres rationnels

3.5.1 Opérations et ordre sur les fractions

Rappelons que les éléments de $\mathbb{Q}$ sont désignés par des *fractions*, c'est-à-dire des expressions de la forme $\frac{a}{b}$ (on écrit aussi a/b), pour $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$ (ensemble des

entiers relatifs non nuls), qu'on a $\frac{a}{1} = a$ pour tout entier relatif a, et qu'un nombre rationnel $\frac{a}{b}$ est nul si et seulement si $a = 0$.
Mais attention : plusieurs fractions différentes peuvent représenter le même nombre rationnel. En effet, si $\frac{a}{b}$ et $\frac{c}{d}$ sont deux fractions, alors elles désignent le même nombre rationnel (c'est-à-dire que $\frac{a}{b} = \frac{c}{d}$), lorsque, en réduisant au même dénominateur, on a $\frac{ad}{bd} = \frac{cb}{db}$, ou encore en multipliant par bd, qui est non nul, exactement lorsque $ad = bc$. Énonçons-le proprement :

Propriété 3.5.1. Si $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$, alors on a $\frac{a}{b} = \frac{c}{d}$ si et seulement si $ad = bc$.

Lorsque nous donnerons une *construction* de l'ensemble $\mathbb{Q}$ dans le troisième cours, nous utiliserons en fait cette condition pour représenter les nombres rationnels.

Exemple 3.5.2. Les fractions $\frac{-3}{6}$ et $\frac{1}{-2}$ sont égales, puisque $(-3).(-2) = 6 = 6.1$.

Ceci étant dit, les opérations sur les nombres rationnels et les relations d'ordre entre eux se décrivent comme suit, à partir de la représentation en fractions :

Propriété 3.5.3. Si $\frac{a}{b}$ et $\frac{c}{d}$ sont deux nombres rationnels, on a :
i) $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$
ii) $(\frac{a}{b}).(\frac{c}{d}) = \frac{ac}{bd}$
iii) $(\frac{a}{b})/(\frac{c}{d}) = \frac{ad}{bc}$, si $c \neq 0$
iv) $\frac{a}{b} \leq \frac{c}{d} \Leftrightarrow ad \leq bc$, si $b, d > 0$
v) $\frac{a}{b} < \frac{c}{d} \Leftrightarrow ad < bc$, si $b, d > 0$.

Remarque 3.5.4. i) Dans les clauses (i) et (ii), il faut remarquer que le dénominateur commun bd est toujours non nul, puisque $b, d \neq 0$ et que le produit de deux entiers non nuls est non nul.
ii) Par la clause (iii), on peut toujours diviser un nombre rationnel par un nombre rationnel non nul : c'est l'intérêt des nombres rationnels.
iii) Dans les clauses (iv) et (v), il faut faire attention à choisir des représentations avec un dénominateur strictement positif, car la multiplication par un nombre négatif change le sens des inégalités (voir la propriété 3.1.3 évoquée dans la section 3.1 sur l'ensemble $\mathbb{R}$ des nombres réels). On peut *toujours* choisir une fraction de cette forme pour représenter un nombre rationnel : en effet, si $a/b \in \mathbb{Q}$ et $b < 0$, alors $a/b = -a/-b$, et $-b > 0$.
iv) Si $\frac{a}{b} \in \mathbb{Q}$ et $c \in \mathbb{Z}$, leur produit est $c.\frac{a}{b} = \frac{c}{1}.\frac{a}{b} = \frac{ca}{b}$. En particulier, pour $c = -1$, on a $(-1).\frac{a}{b} = \frac{-a}{b}$, qu'on peut noter $-\frac{a}{b}$, puisque $\frac{a}{b} + \frac{-a}{b} = \frac{0}{b} = 0$: $\frac{-a}{b}$ est l'opposé de $\frac{a}{b}$ pour l'addition.

Exemple 3.5.5. i) On a $\frac{-23}{5} + \frac{7}{41} = (-23.41 + 7.5)/(5.41) = -\frac{908}{205}$.
ii) On a $(\frac{-23}{5}).(\frac{7}{41}) = (-23.7)/(5.41) = \frac{-161}{205}$.
iii) On a $(\frac{-23}{5})/(\frac{7}{41}) = (-23.41)/(7.5) = -\frac{943}{35}$.
iv) On a $\frac{23}{-5} < \frac{-7}{41}$, car $\frac{23}{-5} = \frac{-23}{5}$ et $-23.41 = -943 < -35 = -7.5$.

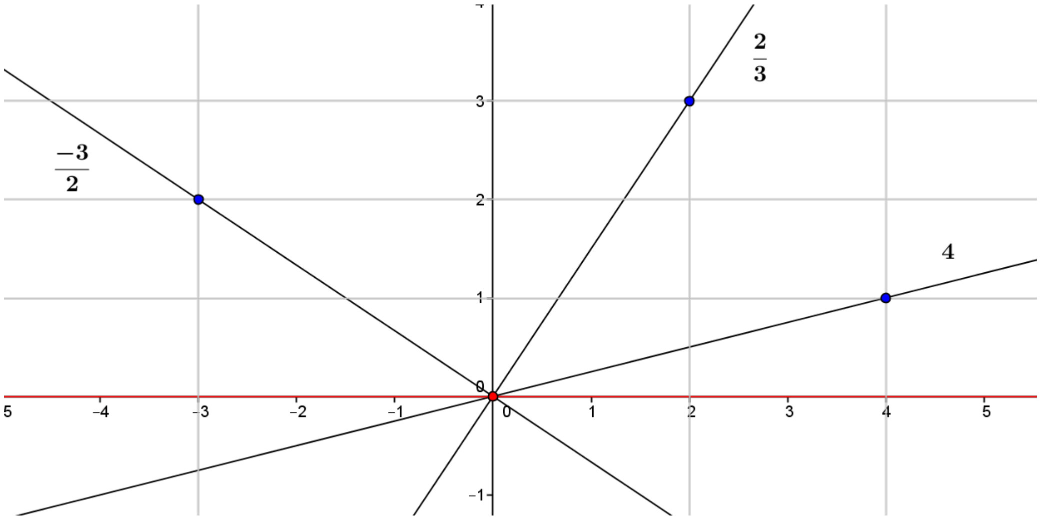


Figure 3.10: Les nombres rationnels peuvent se représenter par les droites du plan passant par des points de coordonnées entières, à l'exception de l'axe des abscisses, et l'ordre sur les rationnels est visible sur ces droites : en partant de la droite en rouge et en tournant dans le sens giratoire (inverse de celui des aiguilles d'une montre), on va des rationnels les plus grands aux plus petits.

3.5.2 La densité de l'ordre linéaire $<$

Reprenons la définition de la relation de divisibilité dans $\mathbb{Z}$: si $m, n \in \mathbb{Z}$, on a $m|n \Leftrightarrow \exists d \in \mathbb{Z},\ m.d = n$. Cette relation n'est pas toujours vérifiée (au moins si $n \neq 0$), c'est pourquoi on l'étudie en détail dans l'arithmétique élémentaire. De plus, si $m = 0$ et $n \neq 0$, elle ne peut jamais être vérifiée : l'intérêt de la relation $m|n$ se limite donc aux entiers m et n tels que $m \neq 0$ ou $n = 0$.
Reprenons la même définition, en changeant les variables pour des nombres rationnels génériques : on obtient, pour $r, s \in \mathbb{Q}$, $r|s \Leftrightarrow \exists x \in \mathbb{Q},\ r.x = s$. Cette relation ne peut pas avoir lieu, comme dans $\mathbb{Z}$, si $r = 0$ et $s \neq 0$. Cependant, *dans tous les autres cas*, elle est *toujours vraie* : en effet, soit $s = 0$ et alors $s = 0 = r.0$, donc $r|s$, soit $r \neq 0$ et alors en écrivant $r = \frac{a}{b}$ et $s = \frac{c}{d}$, on a $a \neq 0$ et par la propriété 3.5.3(iii) de la liste précédente, on peut diviser s par r, d'où $r.(\frac{s}{r}) = s$, donc $r|s$.
Autrement dit, *par construction* la relation $|$ n'a plus d'intérêt dans l'ensemble $\mathbb{Q}$: on ne peut plus distinguer les propriétés arithmétiques des éléments de $\mathbb{Q}$ par cette relation. On se concentre donc plutôt ici sur les relations d'ordre, et particulièrement sur $<$.
La relation d'ordre strict $<$ possède en effet la propriété fondamentale suivante, appelée *densité de l'ordre linéaire sur* $\mathbb{Q}$:

Propriété 3.5.6. Pour tous nombres rationnels r et s tels que $r < s$, il existe un nombre rationnel t tel que $r < t < s$.

Nous allons anticiper la dernière section sur le raisonnement mathématique, dans laquelle nous faisons nos premiers pas dans la démonstration mathématique complexe, en donnant une démonstration de cette propriété, qui en est ici une explication linéaire ne faisant appel à aucune méthode avancée de raisonnement.

Si r, s sont des nombres rationnels tels que $r < s$, écrivons $r = a/b$ et $s = c/d$ comme des fractions : comme précisé avant, on peut toujours choisir a, b, c, d de sorte que $b, d > 0$.
En réduisant les deux fractions au même dénominateur, on obtient $\frac{ad}{bd} < \frac{cb}{bd}$, et donc $ad < bc$. En ajoutant ad aux deux membres (qui sont des entiers relatifs) on obtient alors $2ad < ad + bc$, et en ajoutant cette fois bc aux deux membres on obtient $ad + bc < 2bc$, d'où $2ad < ad + bc < 2bc$.
En divisant alors par 2 dans l'ensemble des nombres rationnels, on obtient $ad < \frac{ad+bc}{2} < bc$. En divisant encore, cette fois-ci par $bd > 0$, on obtient finalement $r = \frac{a}{b} = \frac{ad}{bd} < \frac{ad+bc}{2bd} < \frac{bc}{bd} = \frac{c}{d} = s$. En posant $t = \frac{ad+bc}{2bd}$, on voit qu'on a établi la propriété 3.5.6.

Remarque 3.5.7. i) Nous montrerons plus tard dans ce semestre une propriété analogue, appelée *densité de* $\mathbb{Q}$ *dans* $\mathbb{R}$, à savoir que si $x, y \in \mathbb{R}$ et $x < y$, il existe un nombre rationnel r tel que $x < r < y$.
ii) Le nombre rationnel t n'est rien d'autre que le nombre $\frac{r+s}{2}$, ce qui nous permettra de démontrer également que cette propriété est également valable dans $\mathbb{R}$ dans les exercices, mais la version de la propriété dans $\mathbb{Q}$ ne s'en déduit pas immédiatement comme pour les autres propriétés de $<$ (il faut en plus établir que le nombre t est rationnel, ce qui n'est pas difficile non plus).

Nous verrons dans la dernière partie du cours que la relation $<$ sur $\mathbb{Q}$ et sur $\mathbb{R}$ a une interprétation arithmétique fondamentale.

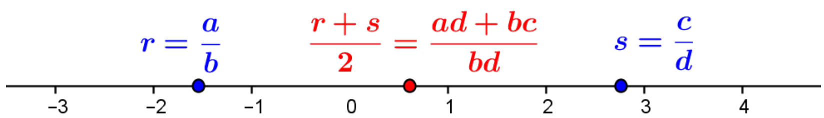


Figure 3.11: Le point d'abscisse $\frac{r+s}{2}$, milieu du segment d'extrémités les points d'abscisses rationnelles $r = \frac{a}{b}$ et $s = \frac{c}{d}$, représente un nombre rationnel strictement compris entre r et s.

Exercices de la leçon

Exercice 3.5.8. i) Écrire deux fractions complexes (avec au moins deux chiffres au numérateur ou au dénominateur), les additionner, les soustraire, les multiplier, et les diviser.
ii) Montrer que si x, y sont des nombres réels et $x < y$, alors on a $x < \frac{x+y}{2} < y$ (le "point" $\frac{x+y}{2}$ est le milieu du segment $[x, y]$); indication : établir que $2x < x+y < 2y$. En déduire que la propriété de densité 3.5.6 est aussi valable dans $\mathbb{R}$.

Chapitre 4

Théorie Élémentaire des Ensembles

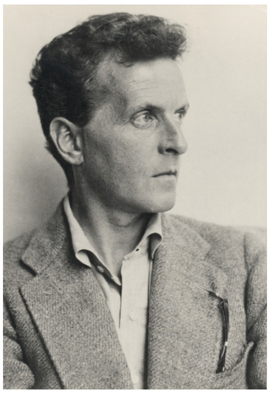
Après avoir introduit les notions de base de la théorie des ensembles (éléments et appartenance, sous-ensembles et inclusion) et les ensembles mathématiques naturels, notamment $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ et $\mathbb{R}$, ainsi que leurs propriétés dans le chapitre précédent, nous allons approfondir les bases de la théorie naïve des ensembles, évoquée dans la première section comme langage conceptuel de la mathématique moderne.
La fécondité de la méthode mathématique repose sur la clarification apportée par cette théorie, conjointement à l'élucidation de la logique mathématique qui lui correspond et que nous avons abordée dans le deuxième chaputre à propos de l'expression mathématique. Il y a ainsi une *articulation naturelle et fondamentale* entre la théorie naïve des ensembles et la logique mathématique naturelle, qui apparaîtra notamment dans les *définitions* ensemblistes.
Rappelons que la théorie naïve des ensembles repose sur l'intuition primitive des *objets*, des *ensembles* et des *entiers naturels*, ce qui signifie que nous ne définirons pas ces notions, mais que nous nous appuierons sur l'intuition que nous en avons.

4.1 Définitions et extensionnalité

4.1.1 Définitions par extension et par intension

Si la théorie naïve des ensembles et la logique mathématique naturelle forment l'armature conceptuelle de la théorie mathématique moderne, le point d'articulation fondamental entre les ensembles et le discours mathématique se situe au niveau des *définitions* des ensembles mathématiques.
En effet, il n'est possible de déployer un discours scientifique qu'à propos de ce dont on sait de quoi on parle... Le philosophe Ludwig Wittgenstein, dans un autre contexte, disait la chose suivante : "Ce qui peut être dit, peut être dit clairement; et ce dont on ne peut parler, il faut le passer sous silence".
Nous avons vu qu'il était possible de se donner des ensembles "naturels", à partir de l'intuition de leurs éléments : nombres entiers, nombres rationnels, nombres réels... et de leurs propriétés, lesquelles sont elles-mêmes exprimées dans un langage qui reflète la théorie des ensembles.

A partir des ensembles définis par des notions primitives ou intuitives, il est alors nécessaire et possible d'en *définir* d'autres, grâce aux méthodes d'expression mathématique étudiées dans la deuxième section.
Il existe deux manières de définir un ensemble - mathématique ou non : la définition par *extension* et la définition par *intension*. Quelle que soit l'approche adoptée, la définition d'un ensemble se fait en utilisant la notation des crochets $\{$ et $\}$.
Un ensemble est défini **par extension** lorsqu'on se donne une liste (exhaustive) de ses éléments; par exemple, l'ensemble $\{0, 3, 5, 6, 8, 15\}$ est défini par extension.
Dans cette situation, on écrit simplement dans la description tous les (noms des) éléments de l'ensemble entre crochets : si $a, b, c, \ldots$ sont les éléments de l'ensemble qu'on cherche à décrire, on écrit $\{a, b, c, \ldots\}$ (ici les points de suspension servent de notation générique, mais la description doit être explicite et finie).
Il peut être utile de répéter le nom d'un objet dans une définition par extension : on décrit cependant le même ensemble. Par exemple, les ensembles $\{1, 8, 2\}$ et $\{1, 8, 2, 8\}$ sont identiques. L'ordre dans lequel on liste les éléments n'a pas non plus d'importance.
Un ensemble est défini **par intension** lorsqu'on se donne une *propriété* qui détermine cet ensemble. C'est à ce niveau que l'expression mathématique spécifique s'articule à la théorie naïve des ensembles.
Par exemple, l'ensemble des entiers naturels pairs, déjà évoqué, est l'ensemble noté $\{n \in \mathbb{N} : \exists d \in \mathbb{N},\ n = 2.d\}$ et est défini par intension comme sous-ensemble de l'ensemble $\mathbb{N}$ des entiers naturels, par la clause "$\exists d \in \mathbb{N},\ n = 2.d$".
En général, un ensemble est défini par intension lorsqu'il s'agit d'un sous-ensemble d'un ensemble déjà introduit ou défini, constitué des éléments ayant une certaine propriété.
On utilise en mathématique les deux types de définitions. Cependant, la définition par extension ne permet par sa nature que de définir des ensembles "finis" (notion que nous définirons proprement dans le cours n^o 2). Pour définir des ensembles "infinis", il est donc naturel de recourir à la définition par intension, qui est donc la définition mathématique *par excellence.*



Le philosophe Ludwig Wittgenstein.

4.1.2 Définitions et clauses

La logique du langage mathématique est étroitement corrélée à l'objet de la science mathématique; ceci apparaîtra lorsque nous décrirons les relations entre certaines "opérations" fondamentales sur les ensembles et les opérations logiques des propriétés qui les définissent.
Lorsque l'on définit un sous-ensemble par intension, c'est-à-dire à partir d'une propriété, on "choisit" à l'aide de cette propriété certains éléments d'un ensemble donné. Pour cela, on utilise une expression mathématique, sous forme symbolique ou non, qui ne contient donc - pour l'instant - qu'une seule variable libre pour les éléments de l'ensemble en question (nous nuancerons lors du deuxième cours).
Plus précisément, si E est un ensemble et qu'on veuille définir un sous-ensemble S par une propriété P, alors P ne peut contenir qu'une seule variable libre x pour les éléments de E, si bien qu'on peut écrire ceci formellement : $S = \{x \in E : P(x)\}$, lire "S est l'ensemble des éléments x de E qui ont la propriété P", plus sommairement "l'ensemble des $x \in X$ tels que P".
Dans le deuxième chapitre, nous avons évoqué la notion de clauses *logiquement équivalentes* : par définition même de cette notion, il faut noter ici que si $P(x)$ et $Q(x)$ sont deux clauses équivalentes avec une variable libre x pour les éléments d'un ensemble E, alors *P et Q définissent le même sous-ensemble de E*, autrement dit les ensembles $\{x \in E : P(x)\}$ et $\{x \in E : Q(x)\}$ sont égaux.
Notons enfin qu'il ne faut pas confondre les définitions de *notions* mathématiques au sens de la deuxième section, et les définitions de *sous-ensembles* par des propriétés.

Exemple 4.1.1. i) Les sous-ensembles $S = \{x \in \mathbb{R} : |x| = x\}$ et $\mathbb{R}_+ = \{x \in \mathbb{R} : x \geq 0\}$ de $\mathbb{R}$ sont égaux.
ii) Si $n \in \mathbb{Z}$, en général le nombre rationnel $n/2$ n'est pas dans $\mathbb{Z}$: c'est le cas si et seulement si n est pair. Ainsi, les sous-ensembles $X = \{n \in \mathbb{Z} : \exists d \in \mathbb{Z},\ 2.d = n\}$ et $Y = \{n \in \mathbb{Z} : n/2 \in \mathbb{Z}\}$ de $\mathbb{Z}$ sont égaux : il s'agit de l'ensemble des entiers relatifs pairs.

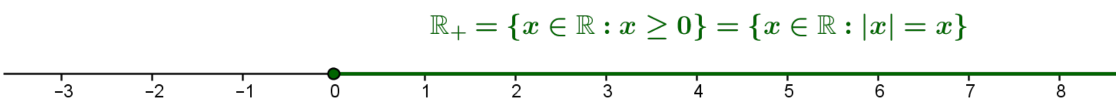


Figure 4.1: En vert est représenté le sous-ensemble de $\mathbb{R}$ des nombres réels positifs, noté $\mathbb{R}_+$, donné par deux descriptions par des clauses équivalentes.

4.1.3 Extensionnalité et inclusion

L'intuition des notions d'ensemble et d'appartenance entraîne que si l'on se donne "deux" ensembles E et F, c'est-à-dire deux descriptions d'ensembles, on a décrit le même ensemble, c'est-à-dire que $E = F$, lorsque E et F ont les mêmes éléments.
On appelle ce principe le principe *d'extensionnalité*, qui au niveau de la théorie naïve des ensembles, est purement "analytique", ce qui signifie qu'il est présent

implicitement dans la notion elle-même.
Lorsque nous avons abordé la notion de sous-ensemble, nous avons défini la relation d'inclusion $E \subseteq F$ par : tout élément de E est élément de F, symboliquement : $\forall x \in E,\ x \in F$. Il s'ensuit que deux ensembles E et F sont égaux exactement lorsque $E \subseteq F$ et $F \subseteq E$.
Pour démontrer l'égalité de deux ensembles E et F donnés formellement, on procède ainsi souvent qu'on démontre que $E \subseteq F$, et que $F \subseteq E$: on dit qu'on procède par *double inclusion*.
Lorsqu'on se donne deux sous-ensembles S et T d'un même ensemble E, définis respectivement par deux propriétés P et Q, S et T sont donc égaux exactement lorsque P et Q définissent le même sous-ensemble, c'est-à-dire lorsque $P(x)$ et $Q(x)$ (où x est une variable pour les éléments de E) sont logiquement équivalentes, par le paragraphe précédent.
Dans cette situation, démontrer la validité universelle de l'implication $P \Rightarrow Q$ (c'est-à-dire la "moitié" de l'équivalence $P \Leftrightarrow Q$) revient alors à démontrer que pour tout élément x de E tel que $P(x)$ est vraie, alors $Q(x)$ est vraie, c'est-à-dire que si $x \in S$, alors $x \in T$, soit encore que $S \subseteq T$.

Figure 4.2: Si P : "n est un multiple de 2", Q : "n est un multiple de 3" et R : "n est un multiple de 6", alors $P \Rightarrow R$ et $Q \Rightarrow R$ sont universellement valides, donc l'ensemble des entiers pairs (en rouge) et l'ensemble des multiples de 3 (en bleu) sont inclus dans l'ensemble des multiples de 6 (en violet).

Exercices de la leçon

Exercice 4.1.2. i) Donner une description par extension de l'ensemble des entiers relatifs impairs dont la valeur absolue est inférieure à 10. Les représenter sur un dessin.
ii) Donner une définition par intension, en utilisant une clause symbolique, de l'ensemble des entiers naturels multiples de 3.
iii) Donner une autre définition par intension de l'ensemble $[-1, 1] = \{x \in \mathbb{R} : -1 \leq x \leq 1\}$ des nombres réels compris entre -1 et 1, en utilisant la valeur absolue.
iv) Donner deux définitions différentes de l'ensemble des entiers naturels impairs.

4.2 Opérations élémentaires sur les ensembles (I)

Nous abordons ici trois opérations fondamentales sur les ensembles : le complément d'un ensemble dans un autre, l'intersection de deux ensembles, et la réunion de deux ensembles.
Ces opérations devront être complétées par d'autres opérations et constructions, mais elles sont suffisantes à ce niveau, et reflètent sur le plan des ensembles les opérations logiques "non" (négation), "et" (conjonction) et "ou" (disjonction), ce qui permet de comprendre l'univocité de l'expression mathématique.

En effet, les clauses élémentaires du discours mathématique expriment des relations qui se ramènent toujours - au moins potentiellement - à l'appartenance d'un objet à un ensemble, et les opérations logiques permises sur les clauses correspondent toujours à des opérations ou constructions parfaitement comprises sur les ensembles.
Les expressions et phrases mathématiques bien formées reflètent donc complètement la structure conceptuelle de l'univers des ensembles, ce qui donne au langage mathématique sa puissance caractéristique : il est "modelé" sur une trame conceptuelle transparente qui est elle-même une forme de langage.
La difficulté dans l'expression mathématique réside donc notamment dans la "traduction" d'idées ou de propriétés intuitives en des propriétés pouvant s'exprimer dans le langage des ensembles et de la logique mathématique.

4.2.1 Complément d'un sous-ensemble

Si E est un ensemble et $S \subseteq E$ un sous-ensemble de E, le *complément de S (dans E)* est l'ensemble noté $C_E(S)$ (ou S^c si l'ensemble ambiant E est clairement identifié dans le contexte), et formé des éléments de E qui ne sont pas éléments de S, symboliquement $C_E(S) = \{x \in E : x \notin S\}$.
Si l'ensemble S est défini comme sous-ensemble de E par une clause P ayant au plus une variable libre x, autrement dit si $S = \{x \in E : P(x)\}$, alors le complément de S est défini par la *négation de P*, c'est-à-dire $S^c = \{x \in E : \neg P(x)\}$. En effet, dire que $x \in E$ n'est pas élément de S, c'est dire dans ce cas que $P(x)$ n'est pas vraie, autrement dit que $\neg P(x)$ est vraie.

Exemple 4.2.1. i) Le complément de l'ensemble $P = \{n \in \mathbb{Z} : \exists d \in \mathbb{Z},\ n = 2.d\}$ des entiers relatifs pairs est l'ensemble $I = \{n \in \mathbb{Z} : \exists d \in \mathbb{Z},\ n = 2.d + 1\}$ des entiers relatifs impairs, car la négation de la propriété "n est un multiple de 2" est (équivalente à) la propriété "$n - 1$ est un multiple de 2".
ii) Le complément de l'ensemble $\mathbb{R}_+ = \{x \in \mathbb{R} : x \geq 0\}$ des nombres réels positifs est l'ensemble $\mathbb{R}_-^* = \{x \in \mathbb{R} : x < 0\}$ des nombres réels strictement négatifs, car la négation de la propriété "$x \geq 0$" est la propriété "$x < 0$".
iii) Par *définition*, le complément du sous-ensemble $\mathbb{Q}$ des nombres rationnels dans l'ensemble $\mathbb{R}$ des nombres réels est appelé *l'ensemble des nombres irrationnels.*

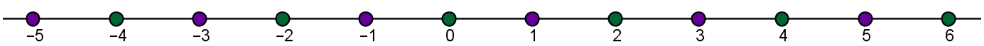


Figure 4.3: En vert, (une partie de l') ensemble des entiers pairs; en violet, (une partie de) son complémentaire, l'ensemble des entiers impairs.

4.2.2 Intersection de deux ensembles

Si E et F sont deux ensembles, *l'intersection de E et F* est l'ensemble noté $E \cap F$ et dont les éléments sont les objets qui sont à la fois éléments de E et éléments de F.
Si E et F sont deux sous-ensembles d'un ensemble X, respectivement définis par

des clauses $P(x)$ et $Q(x)$ dépendant d'un élément générique x de X (x est la seule variable libre dans P et Q), de sorte que $E = \{x \in X : P(x)\}$ et $F = \{x \in X : Q(x)\}$, alors l'intersection $E \cap F$ est définie par la *conjonction* de P et Q, autrement dit $E \cap F = \{x \in X : (P \wedge Q)(x)\}$. En effet, dire qu'un élément x de X est à la fois élément de E et F, c'est dans ce cas dire qu'à la fois $P(x)$ et $Q(x)$ sont valides.

Exemple 4.2.2. i) L'intersection de l'ensemble P des entiers naturels pairs et de l'ensemble I des entiers naturels impairs est l'ensemble $P \cap I = \emptyset$, car aucun entier naturel n'est à la fois pair et impair.
ii) L'intersection de l'ensemble $\mathbb{Q}$ des nombres rationnels et de l'ensemble $\mathbb{R}_+$ des nombres réels positifs est l'ensemble noté $\mathbb{Q}_+$ des rationnels positifs.
iii) L'intersection de l'ensemble E des entiers relatifs multiples de 3 et de l'ensemble F des entiers relatifs multiples de 5 est l'ensemble des entiers relatifs multiples de 15 (nous le démontrerons en général dans le cours d'arithmétique du premier semestre).

4.2.3 Réunion de deux ensembles

De manière analogue, la *réunion de E et F* (on dit aussi *union de E et F*) est l'ensemble noté $E \cup F$ et dont les éléments sont les objets qui appartiennent soit à E, soit à F (et possiblement aux deux).
Si comme avant E et F sont définis comme sous-ensembles d'un ensemble X par des propriétés respectives $P(x)$ et $Q(x)$, alors $E \cup F = \{x \in X : (P \vee Q)(x)\}$. En effet, dans ce cas un élément x de X est dans $E \cup F$ si et seulement si $P(x)$ est vraie ou $Q(x)$ est vraie.

Exemple 4.2.3. i) La réunion de l'ensemble P des entiers naturels pairs et de l'ensemble I des entiers naturels impairs est l'ensemble $\mathbb{N}$ de tous les entiers naturels, car un entier naturel est soit pair, soit impair.
ii) La réunion de l'ensemble $\mathbb{Q}_+^*$ des rationnels strictement positifs et de l'ensemble $\mathbb{Q}_-^*$ des rationnels strictement négatifs est l'ensemble $\mathbb{Q}^*$ des rationnels non nuls.
iii) La réunion de l'ensemble E des entiers relatifs pairs et de l'ensemble F des entiers relatifs multiples de 5 est la réunion des ensembles $\{0, 2, 4, 5, 6, 8, 10, 12, 14, 15, 16, 18, 20, \ldots\}$ et $\{-2, -4, -5, -6, -8, -10, -12, -14, -15, -16, -18, -20, \ldots\}$, décrit par intension comme $\{n \in \mathbb{Z} : \exists d \in \mathbb{Z},\ (2.d = n) \vee (5.d = n)\}$.

Remarque 4.2.4. i) Dans l'exemple (iii), la description par extension des deux ensembles de nombres est *impropre*, puisqu'on ne donne pas la liste de tous les éléments.
ii) E et F sont deux ensembles, alors $E \cap F$ est toujours un sous-ensemble de $E \cup F$, car tout objet qui est élément à la fois de E et de F est élément de $E \cup F$!
Symboliquement : on a toujours $E \cap F \subseteq E \cup F$.

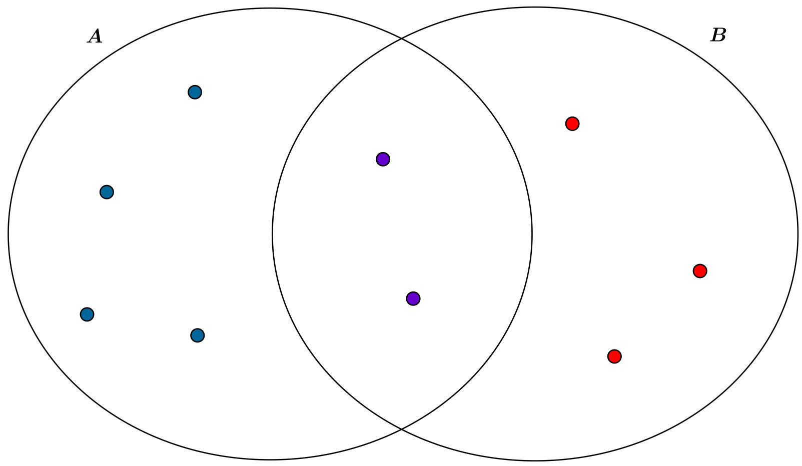


Figure 4.4: L'intersection des ensembles A et B est formée des objets représentés en violet. La réunion de ces ensembles est formée de tous les objets.

4.2.4 Calcul booléen et opérations ensemblistes

Les lois du calcul Booléen sur les clauses, évoquées dans la seconde partie du cours, ont une contrepartie ensembliste naturelle. Lorsque les ensembles sont définis comme sous-ensembles par des clauses, ces lois se traduisent alors comme des opérations analogues sur les ensembles que ces clauses définissent.

Autrement dit, si E et F sont deux sous-ensembles d'un ensemble X, on a :

i) $(E^c)^c = E$ (correspond à l'équivalence entre P et $\neg\neg P$: si $E = \{x \in X : P(x)\}$, alors $(E^c)^c = \{x \in X : \neg(\neg P)(x)\}$ par définition)

ii) $(E \cap F)^c = E^c \cup F^c$ (correspond à la première loi de De Morgan : $(E \cap F)^c = \{x \in X : \neg(P(x) \wedge Q(x))\} = \{x \in X : \neg P(x) \vee \neg Q(x)\} = \{x \in X : \neg P(x)\} \cup \{x \in X : \neg Q(x)\} = E^c \cup F^c$)

iii) $(E \cup F)^c = E^c \cap F^c$ (correspond à la seconde loi de De Morgan : $(E \cup F)^c = \{x \in X : \neg(P(x) \vee Q(x))\} = \{x \in X : \neg P(x) \wedge \neg Q(x)\} = \{x \in X : \neg P(x)\} \cap \{x \in X : \neg Q(x)\} = E^c \cap F^c$).

Il est important de noter que ces lois booléennes sur les ensembles peuvent se démontrer directement (voir les exercices de la leçon) ou alors comme application de la définition de sous-ensembles par des clauses : en effet, on a $E = \{x \in X : x \in E\}$ et $F = \{x \in X : x \in F\}$ donc on peut appliquer la relation entre opérations sur les clauses et opérations sur les ensembles à ces clauses triviales.

Exercices de la leçon

Exercice 4.2.5. o) Si E est un ensemble et F, G, H sont trois sous-ensembles de E, expliquer pourquoi $F \cap (G \cup H) = (F \cap G) \cup (F \cap H)$ et $F \cup (G \cap H) = (F \cup G) \cap (F \cup H)$ (voir aussi l'exercice analogue 2.2.9(iv)).

i) Quel est le complément dans $\mathbb{R}$ de l'ensemble des nombres irrationnels ?

ii) Soient E l'ensemble des nombres rationnels de la forme $a/2$ ($a \in \mathbb{Z}$) et F l'ensemble des nombres rationnels de la forme $a/3$ ($a \in \mathbb{Z}$) : donner une description de même type de l'intersection $E \cap F$.

iii) Soient E l'ensemble des entiers relatifs multiples de 5 et F l'ensemble des entiers relatifs multiples de 35. Quel est l'ensemble $E \cup F$?
iv) Si E et F sont deux sous-ensembles d'un ensemble X, démontrer sans utiliser les équivalences logiques que $(E^c)^c = E$, $(E \cap F)^c = E^c \cup F^c$ et $(E \cup F)^c = E^c \cap F^c$.
v) Si E est un ensemble et F et G sont deux sous-ensembles de E tels que $F \subseteq C_E(G)$, établir que $G \subseteq C_E(F)$.

4.3 Les parties d'un ensemble

4.3.1 L'ensemble $\mathscr{P}(E)$ des parties d'un ensemble E

Dans le premier chapitre nous avons introduit la relation d'inclusion entre ensembles, correspondant à la notion de partie ou de sous-ensemble d'un ensemble.
Dans la théorie naïve des ensembles, on admet l'existence, c'est-à-dire la consistance logique, pour chaque ensemble E, d'un *ensemble des parties de* E. Autrement dit, on admet dans l'univers conceptuel de cette théorie qu'on peut toujours considérer de manière fondée un ensemble, noté $\mathscr{P}(E)$, dont les *éléments* sont les *parties* de E.
Il faut donc prendre garde que si E et X sont deux ensembles, X est une partie de E si et seulement si $X \subseteq E$, si et seulement si $X \in \mathscr{P}(E)$. Nous connaissons déjà pour tout ensemble E deux éléments très particuliers de $\mathscr{P}(E)$, à savoir l'ensemble vide $\emptyset$ et E lui-même. L'ensemble $\emptyset$ est inclus dans tout sous-ensemble de E, donc il est le "plus petit", tandis que E est le "plus grand" sous-ensemble de lui-même, puisqu'il contient par définition tout sous-ensemble.
Cette "opération", qui consiste à "prendre" l'ensemble des parties d'un ensemble, peut être itérée à nouveau : puisque $\mathscr{P}(E)$ est un ensemble, on peut considérer l'ensemble des parties de $\mathscr{P}(E)$, qu'on note $\mathscr{P}(\mathscr{P}(E))$.
Ceci devient vite illisible et impraticable, mais en pratique on a rarement à considérer plus de deux fois l'itération de $\mathscr{P}$ et pendant cette première année nous l'utiliserons peu. L'important dans ce genre de situation est d'être capable de revenir aux définitions, comme toujours, pour retrouver son chemin.

Exemple 4.3.1. i) Si $X \subseteq E$, l'ensemble $\mathscr{P}_X(E)$ des parties de E qui contiennent X, décrit symboliquement comme $\mathscr{P}_X(E) = \{Y \in \mathscr{P}(E) : X \subseteq Y\}$, est un sous-ensemble de $\mathscr{P}(E)$. C'est donc un élément de $\mathscr{P}(\mathscr{P}(E))$.
ii) Un sous-ensemble de $\mathbb{Z}$ formé des multiples d'un entier relatif n donné, soit un ensemble de la forme $n\mathbb{Z} = \{m \in \mathbb{Z} : \exists d \in \mathbb{Z},\ m = dn\}$ est appelé un *idéal* (voir le cours du second semestre sur les structures algébriques élémentaires). L'ensemble des idéaux de $\mathbb{Z}$ est un sous-ensemble de $\mathscr{P}(\mathbb{Z})$.
iii) Un *segment* de $\mathbb{R}$ est par définition un sous-ensemble de $\mathbb{R}$ de la forme $[a, b] = \{x \in \mathbb{R} : a \leq x \leq b\}$, pour $a, b \in \mathbb{R}$. L'ensemble des segments de $\mathbb{R}$ est un élément de $\mathscr{P}(\mathscr{P}(\mathbb{R}))$.

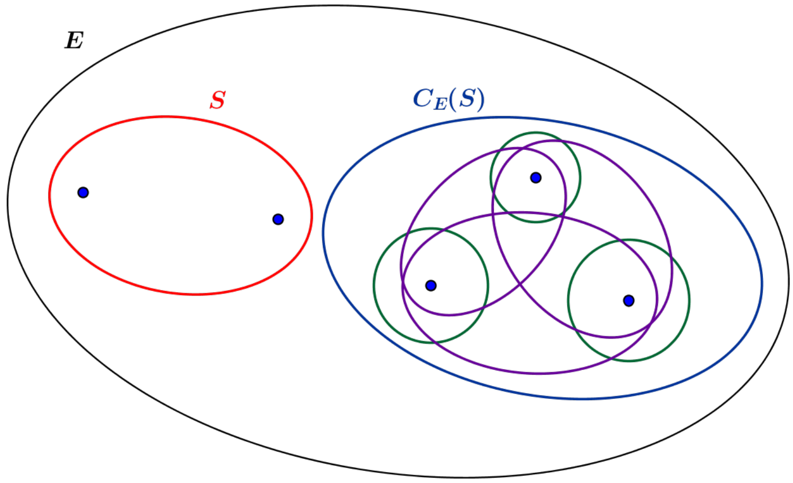


Figure 4.5: Représentation de l'ensemble des parties d'un ensemble E qui sont disjointes d'un sous-ensemble S : ses éléments sont les sous-ensembles de $C_E(S)$, représentés en bleu, en vert et en violet.

4.3.2 Singletons

Parmi les sous-ensembles d'un ensemble E, certains ne contiennent qu'un seul élément de E : ils sont en quelque sorte une "copie" de E dans $\mathscr{P}(E)$, ce que nous aurons l'occasion de préciser dans le second cours (sur les ensembles et la numération).
Un tel sous-ensemble est appelé un *singleton* (de l'anglais "singleton", qui signifie "célibataire"...), et ne possédant qu'un seul élément, par exemple a, et il est décrit par extension comme $\{a\}$.
Si $a, b \in E$, dans le cas où $a \neq b$, les singletons $\{a\}$ et $\{b\}$ sont différents : en effet, ils n'ont pas "les mêmes éléments", et par extensionnalité ils sont différents. Mais il faut garder à l'esprit que des notations différentes peuvent désigner le même objet. Ainsi, il se peut que $\{a\} = \{b\}$, précisément lorsque $a = b$.
Chaque singleton étant une partie de E, l'ensemble des singletons de E est un sous-ensemble de $\mathscr{P}(E)$.

Exemple 4.3.2. i) Pour tout entier naturel n, le singleton $\{n\}$ est un élément de $\mathscr{P}(\mathbb{N})$, mais aussi de $\mathscr{P}(\mathbb{Z})$, de $\mathscr{P}(\mathbb{Q})$ et de $\mathscr{P}(\mathbb{R})$.
ii) Si E est un ensemble, pour tout $X \subseteq E$, le singleton $\{X\}$ est un élément de $\mathscr{P}(\mathscr{P}(E))$ (à méditer).

Figure 4.6: Le segment $[a, b]$ et le singleton $\{c\}$ sont des parties de la droite réelle, donc des éléments de $\mathscr{P}(\mathbb{R})$.

Exercices de la leçon

Exercice 4.3.3. i) Si $X \subseteq E$, nous avons défini $\mathscr{P}_X(E)$; définir à partir de X un autre sous-ensemble de $\mathscr{P}(E)$.
ii) Quels sont les éléments de l'ensemble $\{\emptyset, \{\emptyset\}\}$? Quelles sont ses parties ?
iii) Les ensembles $\{a\}$ et $\{\{a\}\}$ sont-ils égaux ? Décrire $\mathscr{P}(\{a\})$ et $\mathscr{P}(\{\{a\}\})$.

4.4 Opérations élémentaires sur les ensembles (II)

4.4.1 Différence de deux ensembles

Si E et F sont deux ensembles, la *différence de* E *et* F est l'ensemble noté $E - F$ ou $E \backslash F$ de tous les objets qui sont éléments de E mais ne sont pas éléments de F, symboliquement : $E - F = \{x \in E : x \notin F\}$.
Autrement dit, la différence de E et F est l'ensemble $C_E(E \cap F)$, puisque $E \cap F$ est un sous-ensemble de E : effet, un élément de E qui n'est pas élément de F est exactement un élément de E qui n'est pas élément de $E \cap F$.
Inversement et pour les mêmes raisons, si F est un sous-ensemble de E, le complément de F dans E est $E - F$ puisque $F = E \cap F$ dans ce cas : les notions de différence et de complément sont donc définissables l'une à partir de l'autre.
La différence entre les deux notions réside dans le point de vue adopté, puisque contrairement au complément, dans la différence on ne se préoccupe pas de ce que F soit un sous-ensemble de E. La différence est donc ce qu'on appelle une *généralisation du complément*, au sens où le complément d'un ensemble dans un autre est *un cas particulier* de la différence de deux ensembles.
Si E et F sont deux sous-ensembles d'un ensemble X, respectivement définis par des clauses $P(x)$ et $Q(x)$ (x désigne un élément générique de X), alors $E - F$ est le sous-ensemble de X défini par la négation de $P \Rightarrow Q$; autrement dit, on a $E - F = \{x \in X : \neg(P \Rightarrow Q)(x)\}$.
Vérifions-le : un élément x de X est élément de $E - F$ si et seulement si il est dans E mais pas dans F, c'est-à-dire si et seulement si $P(x)$ est vraie et $Q(x)$ est fausse, ou encore si $(P \wedge \neg Q)(x)$ est vraie, laquelle clause est équivalente à la négation de $(\neg P \vee Q)(x)$, soit de $(P \Rightarrow Q)(x)$ par définition.

Exemple 4.4.1. i) La différence de $\mathbb{Q}$ et de $\mathbb{R}_+$ est l'ensemble $\mathbb{Q} - \mathbb{R}_+$ des nombres rationnels qui ne sont pas des réels positifs, autrement dit des nombres rationnels strictement négatifs, soit l'ensemble $\mathbb{Q}_-^* = \{x \in \mathbb{Q} : x < 0\}$.
ii) La différence de $\mathbb{N}$ et de l'ensemble noté $7\mathbb{Z}$ des entiers relatifs qui sont multiples de 7, est l'ensemble $\mathbb{N} \backslash 7\mathbb{Z}$ des entiers naturels qui ne sont pas multiples de 7, soit l'ensemble $\{n \in \mathbb{N} : 7 \nmid n\}$.
iii) Si E est un ensemble et F est un sous-ensemble de E, soit $\mathscr{P}_F(E)$ l'ensemble des parties de E qui contiennent F, symboliquement $\mathscr{P}_F(E) = \{X \subseteq E : F \subseteq X\}$. L'ensemble $\mathscr{P}(E) - \mathscr{P}_F(E)$ est le complémentaire de $\mathscr{P}_F(E)$ dans $\mathscr{P}(E)$, soit l'ensemble des sous-ensembles X de E qui ne contiennent pas F.

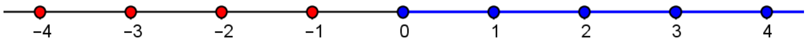


Figure 4.7: En bleu, on a représenté l'ensemble $\mathbb{R}_+$ des nombres réels positifs et les points représentent les entiers relatifs. Les points rouges sont donc les éléments de l'ensemble $\mathbb{Z} - \mathbb{R}_+$.

4.4.2 Différence symétrique de deux ensembles

Si E et F sont deux ensembles, la *différence symétrique de E et F* est l'ensemble $(E - F) \cup (F - E)$, noté $E \Delta F$ (lire "E Delta F"), c'est-à-dire l'ensemble des objets qui sont éléments de E mais pas éléments de F, ou bien éléments de F mais pas éléments de E. On a "symétrisé" la différence entre E et F.
Cette opération correspond à ce qui est connu des informaticiens et des automaticiens comme ce qu'on appelle le "ou exclusif" : un élément de $E\Delta F$, c'est un objet qui est élément de E ou de F, mais pas des deux à la fois.
Une autre façon de concevoir la différence symétrique, c'est de l'écrire $(E \cup F) - (E \cap F)$. En effet, si $x \in E$ et $x \notin F$, alors $x \in E \cup F$ et $x \notin E \cap F$, et de même si $x \in F$ et $x \notin E$, donc $E\Delta F \subseteq (E \cup F) - (E \cap F)$; inversement, si $x \in (E \cup F) - (E \cap F)$, alors soit $x \in E$ (car $x \in E \cup F$) et alors $x \notin F$ (car $x \notin E \cap F$), soit $x \in F$ et alors $x \notin E$ (pour les mêmes raisons), d'où $(E \cup F) - (E \cap F) \subseteq E\Delta F$, et finalement $E\Delta F = (E \cup F) - (E \cap F)$ par double inclusion (voir la section 4.1 sur l'extensionnalité).
Si E et F sont deux sous-ensembles d'un ensemble X, respectivement définis par des clauses $P(x)$ et $Q(x)$ comme précédemment, par le paragraphe précédent la différence symétrique $E\Delta F$ est définie par la disjonction de $\neg(P \Rightarrow Q)$ et $\neg(Q \Rightarrow P)$ (lesquelles définissent respectivement $E - F$ et $F - E$), soit $E\Delta F = (E - F) \cup (F - E) = \{x \in X : \neg(P \Rightarrow Q)(x)\} \cup \{x \in X : \neg(Q \Rightarrow P)(x)\} = \{x \in X : (\neg(P \Rightarrow Q) \vee \neg(Q \Rightarrow P))(x)\}$.
Or, nous avons vu, en traitant de l'équivalence logique, que la clause $(\neg(P \Rightarrow Q)) \vee (\neg(Q \Rightarrow P))$ est équivalente à la négation de la clause $P \Leftrightarrow Q$. Il s'ensuit que le sous-ensemble $E\Delta F$ de X est défini par la clause $\neg(P \Leftrightarrow Q)$, autrement dit $E\Delta F = \{x \in X : \neg(P \Leftrightarrow Q)(x)\}$. La clause $\neg(P \Leftrightarrow Q)$ est donc la version mathématique du "ou exclusif".

Exemple 4.4.2. i) L'ensemble $\mathbb{Z}\Delta\mathbb{Q}_+$ est la réunion de l'ensemble des entiers relatifs strictement négatifs et de l'ensemble des rationnels positifs non entiers.
ii) L'ensemble $2\mathbb{N}\Delta 3\mathbb{Z}$ est la réunion de l'ensemble des entiers naturels pairs non multiples de 3 ($\{2, 4, 8, 10, 14, 16, \ldots\}$), de l'ensemble des entiers naturels impairs, non nuls et multiples de 3 ($\{3, 9, 15, 21, 27, \ldots\}$ et de l'ensemble des entiers relatifs strictement négatifs multiples de 3 ($\{\ldots, -18, -15, -12, -9, -6, -3\}$).
iii) Si E est un ensemble quelconque, alors $E - E = \emptyset$ et $E\Delta E = \emptyset$. De plus, si E est un sous-ensemble d'un ensemble F, on a $E\Delta C_F(E) = F$, ce qui montre que cette "différence" peut donner des ensembles "plus gros" que les ensembles de départ !
iv) En genéral, si E et F sont deux ensembles disjoints (c'est-à-dire tels que $E \cap F = \emptyset$), on a $E\Delta F = E \cup F$.

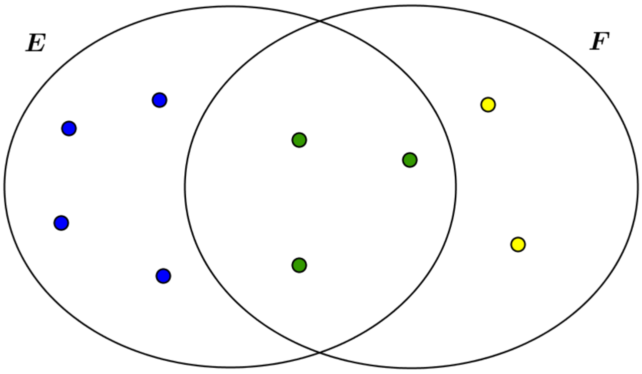


Figure 4.8: La différence $E - F$ est l'ensemble constitué des objets de couleur bleue. La différence symétrique $E\Delta F$ est l'ensemble des objets qui ne sont pas de couleur verte.

La différence de deux ensembles, et la différence symétrique dans une moindre mesure, doivent être connues au même titre que les trois opérations fondamentales. Cependant, nous en ferons un usage moins extensif que ces autres opérations, et surtout à des étapes plus avancées du cursus.

Exercices de la leçon

Exercice 4.4.3 (Différence de deux ensembles)*.* i) Si $\mathbb{Q}_+ = \mathbb{Q}\cap\mathbb{R}_+$ désigne l'ensemble des rationnels positifs, donner une définition par intension de l'ensemble $\mathbb{Z} - \mathbb{Q}_+$.
ii) Donner une définition de l'ensemble $\mathbb{N} - 2\mathbb{Z}$.
iii) Dans l'exemple 4.4.1(iii), donner une description explicite des éléments de $\mathscr{P}_F(E)$ par une propriété utilisant l'appartenance.
iv) Si E, F et G sont trois ensembles tels que $E - F \subseteq G$, établir que $E - G \subseteq F$.
v) Si E et F sont deux ensembles, démontrer que $E = (E - F) \cup (E \cap F)$.

Les exercices sur la différence symétrique sont un peu plus difficiles. Ici comme ailleurs, l'important est de les chercher et de savoir identifier le point où l'on ne peut plus avancer (même si c'est au début !), quitte à y revenir ultérieurement.

Exercice 4.4.4 (Différence symétrique)*.* i) Si E et F sont deux ensembles, démontrer que $E \cup F = (E\Delta F) \cup (E \cap F)$.
ii) Si E est un ensemble et F est un sous-ensemble de E, supposons que $X \subseteq E$ et que $F\Delta X = \emptyset$: démontrer que $X = F$ (on dit que F est le *seul* sous-ensemble de E tel que $F\Delta X = \emptyset$). Indication : si $F\Delta X = \emptyset$, alors $F \cup X \subseteq F \cap X$.
iii) Dans la même configuration que (ii), montrer que $C_E(F)$ est le seul sous-ensemble X de E tel que $F\Delta X = E$, c'est-à-dire que si $X \subseteq E$ et $F\Delta X = E$, alors $X = C_E(F)$. Indication : si $F\Delta X = E$, alors $F \cap X = \emptyset$.
iv) Décrire l'ensemble $\mathbb{Q}_- = \{x \in \mathbb{Q} : x \leq 0\}$ des rationnels négatifs comme la différence symétrique de deux autres ensembles.

Chapitre 5

Le Raisonnement Mathématique

Après avoir esquissé le panorama des ensembles mathématiques naturels, introduit l'expression mathématique naturelle et symbolique, décrit les propriétés élémentaires des ensembles $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ et $\mathbb{R}$, et posé les bases de la théorie naïve des ensembles, dans ce dernier chapitre nous abordons le dernier "bloc" de connaissances essentielles à l'acquisition de la mathématique supérieure moderne.
Dans les dernières sections, nous avons acquis des bases fondamentales en théorie naïve des ensembles, et nous avons établi un lien essentiel entre cette théorie et la logique mathématique naturelle, à travers la notion de définition d'un sous-ensemble par une clause.
La théorie des ensembles et la logique mathématique, au niveau où nous nous plaçons dans ce cours introductif, sont les deux ingrédients conceptuels indissociables qui donnent à la mathématique sa puissance d'expression et sa rigueur.
Dans le deuxième chapitre, nous avons précisé l'usage du langage naturel en mathématique, et introduit le symbolisme typique de notre science, et nous avons appris à nous exprimer rigoureusement.
Dans ce cinquième et dernier chapitre, nous abordons l'autre "articulation" du langage mathématique, ou le "deuxième volet" de l'expression mathématique, celui de la "grammaire" des arguments mathématiques, c'est-à-dire des démonstrations.
Argumenter fait partie de l'usage courant du langage : tout le monde y est habitué, depuis l'enfant qui discute les instructions de ses parents jusqu'au commerçant qui défend la valeur du produit qu'il vend.
Il ne s'agit donc pas tant ici d'apprendre à argumenter, que d'apprendre à le faire en mathématique, c'est-à-dire en utilisant les conventions de l'expression mathématique spécifique.

5.1 Règles, propositions et arguments

5.1.1 Un jeu de règles fini et une proto-théorie des ensembles naturels

Il s'agit ici d'aborder les principaux types de raisonnement mathématique, qui sont en nombre fini, et même très restreint. Il n'est pas du tout évident *a priori* qu'un nombre fini de règles suffise à écrire tous les raisonnements mathématiques dont

nous avons besoin ! Et il n'est pas non plus évident que ce nombre soit si restreint qu'on puisse en donner une liste accessible à ce niveau. C'est pourtant le cas, et l'étudiant(e) ou la lectrice qui travaillera soigneusement ce cours jusqu'au bout aura posé des fondements solides pour la construction de son savoir mathématique.
Nous n'allons pas présenter ces règles comme un simple "catalogue", mais nous allons présenter au mieux les exemples sur lesquels nous les illustrons comme les éléments d'une "proto-théorie" des ensembles $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ et $\mathbb{R}$. Non seulement cela présente l'avantage d'être plus intéressant et d'approfondir la connaissance de ces ensembles et de leurs opérations et relations fondamentales, mais aussi ces quelques résultats établissent des relations subtiles entre ces ensembles, qui illustrent une continuité sous-jacente, mystérieuse, entre arithmétique et géométrie.
Ces différentes règles ou types de raisonnement sont au nombre de cinq : le raisonnement direct, le raisonnement par (disjonction de) cas, le raisonnement par contraposition, le raisonnement par l'absurde et le raisonnement par récurrence.

5.1.2 Les propositions mathématiques

Contrairement au vocabulaire grammatical naturel, en mathématique **une *proposition*** désigne en général (tout du moins hors d'un contexte de logique formelle) **un énoncé *vrai***. Rappelons que cette notion de "véracité" (ou "validité") d'un énoncé demeure intuitive, et est intrinsèquement liée à la relation qu'entretiennent la théorie naïve des ensembles et le langage mathématique naturel.
Il n'en demeure pas moins vrai qu'en principe, cette notion est rigoureuse et que le but de l'activité créatrice en mathématique, est d'énoncer et de *démontrer* des propositions, c'est-à-dire des énoncés vrais, lesquels émergent souvent d'une intuition à propos d'un "état de choses (c'est-à-dire un fait) mathématique", qui demande à être établie rigoureusement, et qu'on appelle une *conjecture*. C'est précisément par une *démonstration* qu'on établit la véracité d'une conjecture, qui peut alors être considérée comme une proposition.
On appelle aussi classiquement *théorème* un énoncé vrai, ce que nous avons appelé ici "proposition". Il n'y a pas de différence de nature entre une proposition et un théorème, mais il est d'usage de réserver le terme "théorème" à une proposition d'importance capitale dans un texte mathématique. Il va sans dire qu'il s'agit là d'une affaire de jugement ou de goût... Mais certaines propositions simples ou accessoires ne seront pas appelées "théorèmes". Le terme "proposition" est donc un terme générique.
Par ailleurs, on dispose également d'autres noms pour certaines propositions. Un *lemme* est une proposition auxiliaire, qu'on utilise pour démontrer une proposition plus importante; souvent, on traite de parties entières de théorèmes complexes dans des lemmes "préparatoires" ou "auxiliaires", qui permettent de clarifier la démonstration du théorème. Un *corollaire* est une conséquence, relativement directe, d'une proposition ou d'un théorème; si on a bien choisi la terminologie, un théorème apporte en effet une connaissance substantiellement nouvelle avec plusieurs retombées.
En somme, le "lemme" prépare et précède une proposition importante, le "corollaire" la suit, et la proposition capitale est un "théorème". Il existe d'autres termes utilisés

occasionnellement, et qui relèvent de la tradition mathématique et philosophique, mais le présent vocabulaire est standard.

$$\textit{Lemme} \quad \longrightarrow \quad \textit{Théorème} \quad \longrightarrow \quad \textit{Corollaire}$$

Figure 5.1: Différents types de propositions mathématiques et leur enchaînement classique.

5.1.3 Les arguments mathématiques

Enfin, si l'on cherche à démontrer des énoncés vrais, il nous faut une *méthode* de démonstration.
Lorsque nous avons abordé l'expression mathématique, nous avons caractérisé celle-ci comme une variante du discours naturel, marquée par sa référence particulière aux objets mathématiques et à la théorie des ensembles, et nous avons vu qu'un petit nombre de règles de syntaxe "logique" permettait de décrire la "grammaire" des clauses mathématiques.
Il en va de même de la démonstration mathématique : il s'agit d'une variante du discours naturel, lequel est également susceptible de démonstration et d'argumentation, et la spécificité du discours mathématique permet d'isoler des modes de raisonnement mathématiques propres.
Comme nous l'avons déjà évoqué, les règles essentielles en usage dans les démonstrations mathématiques de tout niveau sont en très petit nombre, et accessibles à un niveau élémentaire. Nous allons les exposer en les illustrant par quelques résultats sur les ensembles naturels $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ et $\mathbb{R}$, ce qui fournira à l'étudiant(e) ou le lecteur une "théorie élémentaire des ensembles naturels", et une bonne introduction au semestre et à l'ensemble du cursus.

5.2 Le raisonnement direct

Principe du raisonnement direct

Les énoncés mathématiques dont on cherche à démontrer la validité se présentent souvent comme une conclusion qui découle d'une hypothèse. Autrement dit, démontrer une proposition mathématique revient en général à établir la véracité d'un énoncé de la forme $P \Rightarrow Q$, ou la validité universelle d'une clause de la forme $P \Rightarrow Q$.
La méthode "directe" consiste donc à supposer P, et à chercher à démontrer Q "directement" à partir de l'analyse des hypothèses contenues dans P, par une suite de déductions simples ou de calculs.
Il n'est pas toujours possible de procéder aisément ainsi, mais quand c'est le cas, une telle démonstration a l'avantage de la clarté. Les autres types de raisonnement sont "indirects", en ce qu'ils utilisent un ou plusieurs raisonnements accessoires ou élaborés, d'une autre forme.
Nous présenterons deux exemples de démonstrations par un raisonnement direct.

5.2.1 Entiers impairs

Nous allons commencer doucement, par un résultat simple, pas si intuitif que cela : le carré d'un entier relatif impair est impair. On peut essayer avec les premiers entiers naturels : $1^2 = 1$, $3^2 = 9$, $5^2 = 25$, $7^2 = 49$, $9^2 = 81$; la propriété se vérifie sur ces quelques valeurs, mais il ne suffit pas en mathématique d'une vérification expérimentale sur un nombre fini, même grand, de valeurs : il faut l'établir pour tout nombre entier relatif, et il faut donc pour cela raisonner de manière "générique".
Nous avons déjà vu que la notion de multiple d'un nombre entier est valable pour les entiers relatifs; on rappelle que c'est cette notion qu'on utilise pour définir rigoureusement ce qu'est un entier relatif pair : il s'agit d'un *multiple de* 2.
Autrement dit, par définition un entier relatif m est pair si et seulement si il existe $n \in \mathbb{Z}$ tel que $m = 2n$. On peut alors définir un entier impair comme un entier m qui n'est pas pair, ce qui équivaut (voir les exercices) à ce qu'il existe un entier $n \in \mathbb{Z}$ tel que $m = 2n + 1$.
La proposition suivante, démontrée par un raisonnement direct, nous sera utile pour démontrer l'irrationalité de la racine carrée de 2 (Proposition 5.4.7), ce qui était une tragédie pour les mathématiciens grecs de l'Antiquité, car cela signifiait que certaines grandeurs géométriques ne pouvaient se mesurer par les nombres rationnels. Puisque nous l'utiliserons comme résultat accessoire, nous l'appelons un *lemme*.

Lemme 5.2.1. *Pour tout entier relatif impair n, l'entier relatif n^2 est impair.*

Démonstration. Comme n est impair, par ce qui précède il existe un entier $m \in \mathbb{Z}$ tel que $n = 2m + 1$. On peut alors écrire $n^2 = (2m + 1)^2 = (2m + 1).(2m + 1) = 4m^2 + 4m + 1$ (en développant) $= 2(2m^2 + 2m) + 1$, ce qui montre bien que n^2 est impair. □

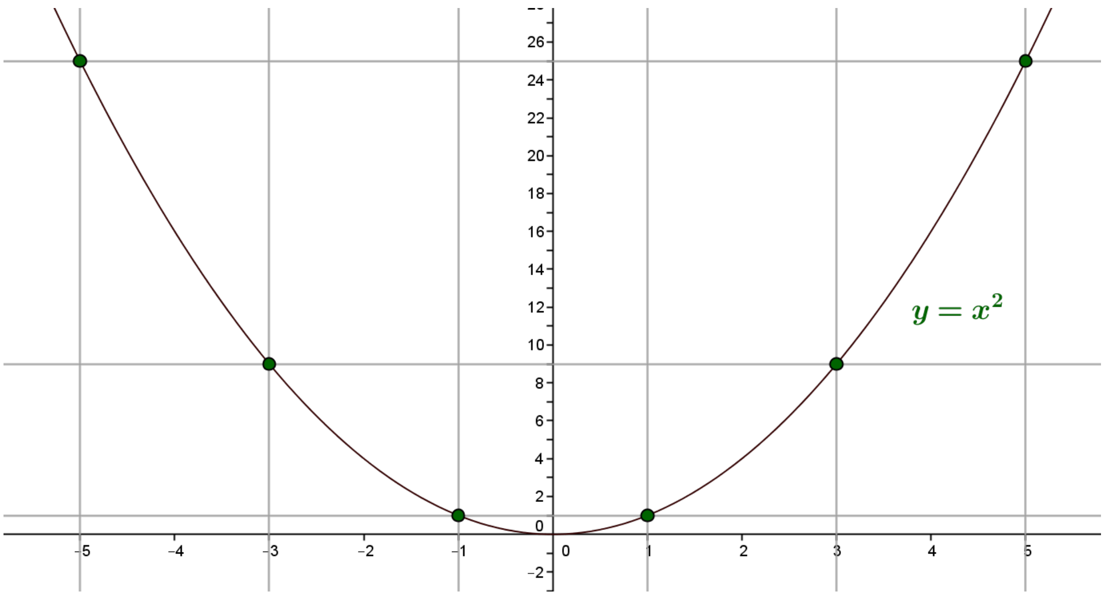


Figure 5.2: Le carré d'un entier relatif impair est un entier (naturel) impair.

Remarque 5.2.2. Nous avons utilisé une caractérisation d'un nombre impair que nous n'avons pas démontrée, et qui est renvoyée aux exercices, lesquels proposent de l'établir à l'aide du théorème qui suit. Cette façon de faire, un peu circulaire dans le texte lui-même, ne pose pas de problème tant qu'on n'utilise pas un résultat qu'on est censé démontrer avec celui qu'on est en train de démontrer ! C'est le cas ici, et cela nous permet d'exposer les choses dans un ordre qui nous plaît mieux; c'est un excellent exercice que de s'assurer qu'on n'introduit pas ici de circularité logique.

5.2.2 Division euclidienne des entiers naturels

Une propriété essentielle des entiers naturels, qui s'étend aux entiers relatifs, est la possibilité d'effectuer ce qu'on appelle la *division euclidienne.* L'idée simple mais fondamentale sous-jacente est que deux entiers naturels a et b étant donnés, a n'est pas toujours un multiple de b, autrement dit, le nombre rationnel a/b n'est pas toujours un entier : il n'est pas toujours possible de diviser de manière exacte a par b.

Par la division euclidienne on cherche alors le "nombre maximal de fois que b se trouve dans a" : intuitivement, il existe un "plus grand multiple" de b inférieur ou égal à a. Sur le plan des *quantités*, l'intuition est que si l'on dispose d'un ensemble de a objets, on pourra les rassembler en un nombre maximal de sous-ensembles contenant chacun b objets parmi ceux-ci, et il en restera éventuellement quelques-uns, mais toujours strictement moins que b (sinon, on peut toujours former un nouveau sous-ensemble de b objets).

Le *quotient* de la division de a par b est en quelque sorte le "nombre maximal de paquets de b objets qu'on peut faire avec a objets", et le *reste* de cette division est le nombre d'objets qui reste une fois qu'on a "mis de côté" ces paquets et qu'on ne peut plus en former, parce qu'il ne reste pas assez d'objets.

Nous allons énoncer et démontrer rigoureusement qu'il existe un quotient et un reste uniques, en utilisant un raisonnement direct. Rappelons qu'un *multiple* d'un entier naturel b est un entier naturel m tel que $b|m$, autrement dit tel qu'il existe un entier naturel d pour lequel $m = b.d$. Les multiples de b sont donc *tous* les entiers naturels m qui s'écrivent sous la forme $b.d$, pour $d \in \mathbb{N}$.

Nous admettons le principe intuitif suivant, qui sera justifié dans le cours suivant : si E est un sous-ensemble non vide de $\mathbb{N}$ tel qu'il existe $n \in \mathbb{N}$ pour lequel $E \subseteq \{0, \ldots, n\}$ (un sous-ensemble "fini"), alors il existe un "plus grand élément" dans E, c'est-à-dire un entier naturel $m \in E$ tel que $x \leq m$ pour tout $x \in E$.

Théorème 5.2.3. *Pour tous entiers naturels a et b tels que $b \neq 0$, il existe deux entiers naturels q et r uniques tels que $a = bq + r$ et $r < b$. Les nombres q et r sont appelés respectivement le* quotient *et le* reste *de la division Euclidienne de a par b.*

Démonstration. On considère l'ensemble $D = \{d \in \mathbb{N} : b.d \leq a\}$, qui n'est pas vide puisque $0 \in D$: en effet, on a $b.0 = 0 \leq a$. Comme aussi $b > 0$, d'après les propriétés de $<$ (propriété 3.1.3(iv)), on a $a < (a+1)b$ puisque $a < a+1$, donc pour tout entier naturel $d \geq a+1$, on a $b.d > a$. Nous venons d'établir que l'ensemble $X = \{n \in \mathbb{N} : n \geq a+1\}$ est inclus dans l'ensemble $\mathbb{N} - D$, et par les propriétés élémentaires sur les ensembles (voir l'exercice 4.2.5) il s'ensuit que l'ensemble D est inclus dans l'ensemble $\mathbb{N} - X = \{n \in \mathbb{N} : n \leq a\}$. Comme D n'est pas vide, par le principe évoqué avant l'énoncé il possède un plus grand élément, qu'on appelle q.

On a alors $bq \leq a < b(q+1)$, puisque $q \in D$ mais $q+1 \notin D$. Écrivons $r = a - bq$: en soustrayant bq (dans $\mathbb{Z}$) de l'inégalité précédente, grâce aux propriétés de la relation $<$ par rapport à l'addition on obtient $0 = bq - bq \leq r = a - bq < b(q+1) - bq = b$, donc on peut écrire

$$a = b.q + r,$$

avec $0 \leq r < b$: nous avons démontré l'*existence* de q et de r. Supposons que q' et r' sont des entiers naturels avec la même propriété, c'est-à-dire que $a = b.q' + r'$, avec $r' < b$: on a $b.q + r = b.q' + r'$, et en ajoutant $-b.q' - r$ à chaque membre de cette égalité, on obtient $b.q - b.q' = r' - r$ $(*)$. Comme $r \leq b - 1$ et $r' \leq b - 1$, on a d'abord $1 - b \leq -r \leq 0$, d'où $-b + 1 \leq r' - r \leq b - 1$, c'est-à-dire $-b < r' - r < b$, d'où $|r' - r| < b$ par définition de la valeur absolue, et en remplaçant $r' - r$ par sa valeur à partir de $(*)$, on obtient $-b < b(q - q') < b$, c'est-à-dire $|b||q - q'| < |b|$; en divisant chaque membre par $|b| = b > 0$, on ne change pas le sens des inégalités et on obtient $|q - q'| < 1$, ce qui signifie que $q = q'$. Il s'ensuit alors que $0 = a - a = (b.q + r') - (b.q + r) = r' - r$, donc $r = r'$ et finalement, q et r sont uniques. On a démontré l'existence et l'unicité de q et r, et la démonstration est terminée. $\square$

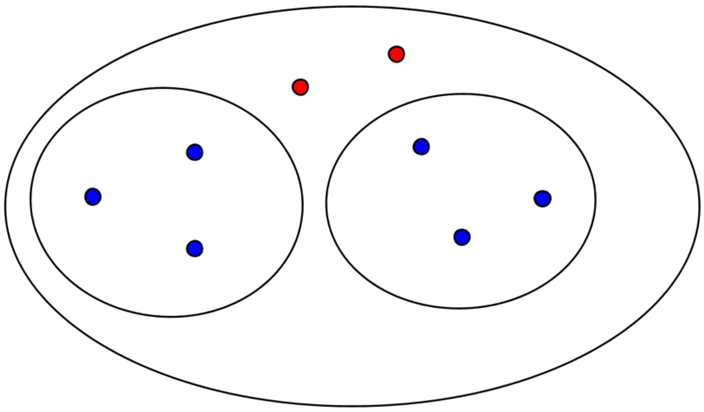


Figure 5.3: Le quotient et le reste de la division de 11 par 3 sont respectivement 2 et 2 : on peut faire au maximum 2 paquets de 3 objets dans un ensemble de 8 objets, et il reste alors 2 objets.

Remarque 5.2.4. i) La division Euclidienne fait un lien essentiel entre les quatre ensembles fondamentaux $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ et $\mathbb{R}$. En effet, son énoncé porte sur les entiers naturels, et la démonstration utilise la différence dans l'ensemble des entiers relatifs ainsi que la valeur absolue. Elle permet aussi d'écrire le nombre rationnel a/b sous la forme $a/b = (bq + r)/b = q + (r/b)$ avec $0 \leq r/b < 1$, ce qui est la meilleure approximation de a/b par un entier qui lui est inférieur ou égal, et sera généralisé à la "partie entière"d'un nombre réel.
ii) En utilisant un raisonnement sur les complémentaires des ensembles, nous avons évité au début de la démonstration, pour établir que $D \subseteq \{0, \ldots, a\}$, un raisonnement dit *par contraposée*, que nous introduirons dans la suite.
iii) Cette démonstration est complexe. L'étudiant(e) ou la lectrice trouvera du profit

à en faire "l'exégèse", c'est-à-dire à l'analyser en détail pour en comprendre les parties, les articulations, et chaque argument individuel.
iv) Nous donnerons dans la leçon suivante une extension de ce théorème à la division euclidienne d'un entier relatif par un entier naturel non nul.

Exercices de la leçon

Exercice 5.2.5. i) Soit $n \in \mathbb{N}$. En effectuant la division euclidienne de n par 2, montrer que si n est impair, alors on peut écrire $n = 2m + 1$, pour un certain $m \in \mathbb{N}$.
ii) Soit $n \in \mathbb{Z}$, $n < 0$. En appliquant la question précédente à $-n \in \mathbb{N}$, démontrer que si n est impair, alors il existe $m \in \mathbb{Z}$ tel que $n = 2m + 1$.
iii) Démontrer que si $n \in \mathbb{Z}$ s'écrit sous la forme $n = 2m + 1$, avec $m \in \mathbb{Z}$, alors n est impair (réciproque de l'exercice précédent). En conclure que les entiers impairs sont les nombres de la forme $2m + 1$, pour $m \in \mathbb{Z}$.
iv) Démontrer que le produit de deux entiers relatifs impairs est impair.
v) Effectuer la division euclidienne de 83 par 7.

5.3 Le raisonnement par (disjonction des) cas

5.3.1 Principe du raisonnement par cas

Le raisonnement par cas consiste, pour démontrer un énoncé de la forme $P \Rightarrow Q$ (ou la validité universelle d'une clause de la forme $P \Rightarrow Q$), à "décomposer" P en deux ou plusieurs cas.
Autrement dit, si P est une clause équivalente à une disjonction $P_1 \vee P_2$ (les deux cas), on se ramène à démontrer la clause équivalente $(P_1 \vee P_2) \Rightarrow Q$, qui par définition est $\neg(P_1 \vee P_2) \vee Q$, logiquement équivalente par les règles élémentaires à $(\neg P_1 \wedge \neg P_2) \vee Q$, à son tour équivalente à $(\neg P_1 \vee Q) \wedge (\neg P_2 \vee Q)$, c'est-à-dire, par définition, $(P_1 \Rightarrow Q) \wedge (P_2 \Rightarrow Q)$!
En reformulant encore, on se ramène à démontrer *à la fois* $P_1 \Rightarrow Q$ *et* $P_2 \Rightarrow Q$ (et autant d'implications que de cas lorsqu'on distingue plus de cas); il y a donc autant d'étapes dans la démonstration que de cas à traiter.
Cette approche est utile lorsque distinguer des situations différentes sous l'hypothèse P conduit à adopter des stratégies différentes pour démontrer Q.

5.3.2 Division euclidienne des entiers relatifs

Une première application féconde du raisonnement par cas est l'extension de la division euclidienne des entiers naturels aux entiers relatifs. Ici, les deux cas de base à distinguer seront celui d'un entier naturel, et celui d'un entier relatif strictement négatif.

Corollaire 5.3.1. *Si a et b sont deux entiers relatifs tels que $b > 0$, alors il existe des entiers relatifs q et r uniques tels que $a = bq + r$ et $0 \leq r < b$.*

Démonstration. Distinguons deux cas, selon que $a \in \mathbb{N}$ ou bien que $a \in \mathbb{Z} - \mathbb{N}$. Si $a \in \mathbb{N}$, la conclusion de l'énoncé découle de la division euclidienne des entiers naturels (théorème 5.2.3). Si $a < 0$, démontrons d'abord l'existence de q et r. Effectuons la division euclidienne de $-a$ par b, puisque $-a \in \mathbb{N}$: il existe des entiers naturels uniques q_0 et r_0 tels que $-a = bq_0 + r_0$ et $0 \leq r_0 < b$. On peut donc écrire, en multipliant par -1, $a = -bq_0 - r_0$. Distinguons à nouveau deux cas, selon que $r_0 = 0$ ou non. Si $r_0 = 0$, alors on a $a = b.(-q_0)$, donc $q = -q_0$ et $r = 0$ conviennent. Si $r_0 > 0$, $-r_0$ ne peut pas être un reste, mais comme $r_0 < b$ on peut écrire à la place de l'égalité précédente $a = -bq_0 - b + b - r_0 = b(-q_0 + 1) + (b - r_0)$. Comme $-b < -r_0 < 0$ par les propriétés des inégalités (on a multiplié l'inégalité $0 < r_0 < b$ par -1), il vient $0 = b - b < b - r_0 < b$, si bien que $q = -q_0 + 1$ et $r = b - r_0$ conviennent. Par disjonction des cas, l'existence de q et r est démontrée pour $a < 0$. L'unicité de q et r se démontre alors exactement comme dans le théorème 5.2.3; par disjonction des cas, le corollaire est démontré. $\square$

Remarque 5.3.2. i) C'est un bon exercice que de démontrer l'unicité de q et r pour le cas où $a < 0$ (ou pour tout entier relatif a en général), c'est-à-dire de se convaincre que l'argument déjà utilisé à la leçon précédente pour le cas $a \geq 0$ convient pour tout entier relatif.
ii) Nous aurions pu choisir comme cas $a \geq 0$ d'une part et $a \leq 0$ d'autre part, avec la même démonstration : il n'est pas nécessaire que les cas soient exclusifs, mais il faut par contre qu'ils épuisent toutes les situations possibles.

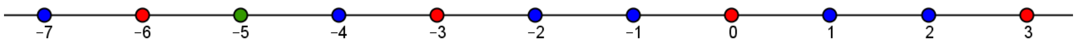


Figure 5.4: Même si -5 est un entier strictement négatif, son reste dans la division euclidienne par 3 est 1.

5.3.3 Mesure des grandeurs réelles dans une unité

Un autre exemple de raisonnement par cas est donné dans la conséquence fondamentale suivante de la propriété d'Archimède vue dans le Chapitre 3 (axiome 1), énonçant en termes mathématiques ce qu'est la "mesure" d'une grandeur réelle x, positive ou négative, relativement à une "unité de mesure", qui est un réel strictement positif :

Proposition 5.3.3 ("Propriété de la mesure")**.** *Si a est un nombre réel strictement positif, alors pour tout nombre réel x il existe un unique entier relatif k tel que $ka \leq x < (k+1)a$.*

Démonstration. Nous démontrons d'abord l'existence de k et pour cela nous distinguons deux cas : soit $x \geq 0$, soit $x < 0$. Si $x \geq 0$, comme $a > 0$ on a aussi $x/a \geq 0$, et par la propriété d'Archimède il existe un entier naturel n tel que $n > x/a$. On considère l'ensemble E des entiers naturels m tels que $m \leq x/a$: comme $0 \leq x/a$, l'ensemble E n'est pas vide (il contient 0), et pour tout $m \in E$ on a $m \leq n$, donc E

possède comme dans la section précédente un plus grand élément, que nous appelons k. Par définition, on a alors $k \leq x/a < k+1$, et en multipliant cette double inégalité par $a > 0$, on ne change pas le sens des inégalités et on obtient $ka \leq x < (k+1)a$.
Si $x < 0$, alors $-x/a > 0$ et par la propriété d'Archimède à nouveau il existe un entier naturel n tel que $-x/a < n$, d'où $-n < x/a$ en multipliant l'inégalité par -1. L'ensemble E des entiers relatifs m tels que $-n \leq m \leq x/a$ n'est donc pas vide, et possède un plus grand élément, qu'on note k : par définition, on a $k \leq x/a < k+1$, d'où à nouveau $ka \leq x < (k+1)a$, et *l'existence* de k est démontré dans les deux cas.
En ce qui concerne l'unicité, supposons que l est un entier relatif tel que $la \leq x < (l+1)a$; en particulier, on a $ka \leq x < (l+1)a$, et en divisant par $a > 0$ on obtient $k \leq x/a < l+1$, d'où $k \leq l$; en échangeant les rôles de k et de l on a aussi $l \leq k$, d'où $k = l$, et k est unique avec cette propriété : la proposition est démontrée. □

Remarque 5.3.4. i) Dans le cas où $x < 0$, l'existence du plus grand élément k repose sur un principe analogue à celui de l'existence d'un plus grand élément pour un sous-ensemble borné de $\mathbb{N}$, que nous n'avons pas précisé ici.
ii) Noter l'analogie avec la division euclidienne : il existe un entier relatif k unique et un nombre réel positif r tel que $r < a$ unique, tels que $x = k.a + r$. Nous verrons dans le paragraphe suivant qu'on peut en fait interpréter la division euclidienne à travers cette propriété.

La démonstration précédente illustre une stratégie habituelle pour prouver l'existence d'un unique objet ayant une propriété donnée, que nous avons déjà rencontrée dans la démonstration du théorème 5.2.3 : on montre d'abord *l'existence* de l'objet en question (ici, c'est dans cette phase que nous avons appliqué le raisonnement par cas), puis on montre *l'unicité* de l'objet, en montrant que si deux objets partagent la propriété en question, il sont nécessairement égaux. Il est important de remarquer que les deux étapes de cette stratégie peuvent être réalisées dans l'autre ordre : il n'est pas nécessaire de savoir que l'objet en question existe, pour pouvoir démontrer que *si* il existe, il est alors unique !

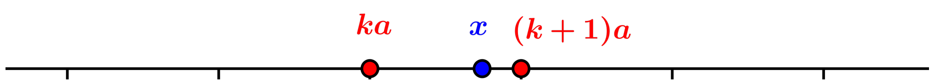


Figure 5.5: Mesure d'une grandeur réelle x dans une unité $a > 0$: la mesure de x est k, car $ka \leq x < (k+1)a$.

5.3.4 Un pont entre l'arithmétique et la géométrie

Revenant à la proposition 5.3.3, il devrait apparaître à l'étudiant(e) ou le lecteur attentif(ve) l'analogie entre sa démonstration et la démonstration de l'existence du quotient dans la division euclidienne pour les entiers relatifs. Il existe en fait un lien profond entre ces deux résultats, que nous allons expliciter à l'aide de la notion fondamentale suivante.

Définition 5.3.5. En choisissant $a = 1$ dans la proposition 5.3.3 précédente, pour tout nombre réel x il existe un unique entier relatif n tel que $n \leq x < n+1$. L'entier n est appelé la *partie entière de* x et noté $E(x)$.

La partie entière d'un nombre réel est un concept mathématique très important, qui n'a pas fini de livrer ses secrets. Une conséquence des plus intéressantes de la "propriété de la mesure" est le corollaire suivant, qui entremêle la division euclidienne des entiers relatifs avec l'ordre naturel de la droite réelle, en utilisant les nombres rationnels et la partie entière comme "pont" entre l'arithmétique et la géométrie.

Corollaire 5.3.6. *Si $r = a/b$ est un nombre rationnel et $b > 0$, alors $E(r)$ est le quotient, et $a - bE(r)$ est le reste, de la division Euclidienne de a par b.*

Démonstration. Par définition, on a $E(r) \leq r < E(r) + 1$, d'où $bE(r) \leq br < bE(r) + b$, car $b > 0$, donc nous obtenons $a = br = bE(r) + (a - bE(r))$, avec $a - bE(r) = br - bE(r) = b(r - E(r)) < b$. Il s'ensuit que $E(r)$ est le quotient et $a - bE(r)$ est le reste, de la division Euclidienne de a par b, par définition et unicité de ceux-ci (corollaire 5.3.1). □

Rappelons que l'hypothèse sur b n'est pas restrictive puisque tout nombre rationnel possède une représentation de cette forme; le corollaire est donc valable pour tout nombre rationnel. Ce type de considération donne lieu au *développement des nombres réels* dans une base numérique donnée, que nous aborderons dans la suite du semestre.

Exercices de la leçon

Exercice 5.3.7. i) Démontrer l'unicité du quotient et du reste dans la division euclidienne des entiers relatifs.
ii) Redémontrer qu'un entier relatif impair n s'écrit sous la forme $2m+1$ en utilisant la division euclidienne des entiers relatifs.
iii) Démontrer que pour tout nombre réel x, on a $|x| = \sqrt{x^2}$ (on rappelle que la racine carrée $\sqrt{y}$ d'un nombre réel positif y est l'unique nombre réel positif z tel que $z^2 = y$). Indication : utiliser un raisonnement par cas en revenant à la définition de $|x|$.
iv) En simplifiant la démonstration de la proposition 5.3.3, montrer directement que pour tout $x \in \mathbb{R}$, il existe un unique entier relatif $k \in \mathbb{Z}$ tel que $k \leq x < k + 1$ (définition de la partie entière).

5.4 Les raisonnements classiques par la négation

5.4.1 Le raisonnement par contraposition

Le raisonnement par contraposition (ou contraposée) consiste, pour démontrer $P \Rightarrow Q$, à démontrer plutôt $(\neg Q) \Rightarrow (\neg P)$. En effet, ces deux énoncés (ou deux clauses en général) sont équivalents : par définition, le second est $\neg(\neg Q) \vee \neg P$, équivalent à $Q \vee \neg P$ par les propriétés de la négation, lui-même équivalent à $\neg P \vee Q$, c'est-à-dire $P \Rightarrow Q$ par définition. On utilise ce procédé dans le cas où il est plus simple de

raisonner de cette façon que de chercher à démontrer Q en supposant P. La clause $(\neg Q) \Rightarrow (\neg P)$ est appelée la *contraposée* de la clause $P \Rightarrow Q$.
Dans les deux exemples suivants, on raisonne par contraposée parce qu'il est plus commode de démontrer une égalité qu'une inégalité.

Proposition 5.4.1. *Pour tout entier relatif non nul n, si $d, d' \in \mathbb{Z}$ et $d \neq d'$, alors $dn \neq d'n$.*

Démonstration. On raisonne par contraposée, en supposant que $dn = d'n$: on peut écrire $dn - d'n = 0$, et en factorisant par n on obtient $(d - d')n = 0$. Comme n n'est pas nul, on peut diviser par n dans $\mathbb{Q}$, et on obtient $d - d' = ((d - d')n)/n = 0/n = 0$, soit $d = d'$. Par contraposée, si $d \neq d'$ on a $dn \neq d'n$. □

Remarque 5.4.2. On peut aussi faire une démonstration par cas (en distinguant les cas $d < d'$ et $d > d'$), mais la contraposée est plus simple (voir les exercices).

Les deux exemples suivants sont tirés de *Algèbre 1ère année*, de F. Liret et D. Martinais (Dunod, Paris, 1997).

Proposition 5.4.3. *Si x, y sont des nombres réels tels que $x \neq y$, alors $(x+1)(y-1) \neq (x-1)(y+1)$.*

Démonstration. On raisonne par contraposition, en supposant que $(x+1)(y-1) = (x-1)(y+1)$. En développant, on obtient l'égalité $xy - x + y - 1 = xy + x - y - 1$, et en ajoutant $1 - xy$ aux deux membres, on obtient $-x + y = x - y$, d'où $2(x - y) = 0$, et en divisant par 2, on conclut que $x - y = 0$, soit $x = y$. Par contraposée, si $x \neq y$, on a bien $(x+1)(y-1) \neq (x-1)(y+1)$. □

Remarque 5.4.4. Comme pour l'exemple précédent, on peut démontrer cette proposition par cas, mais la démonstration est plus simple par contraposée. De plus, ici le raisonnement par cas fait directement apparaître les éléments du raisonnement par contraposée.

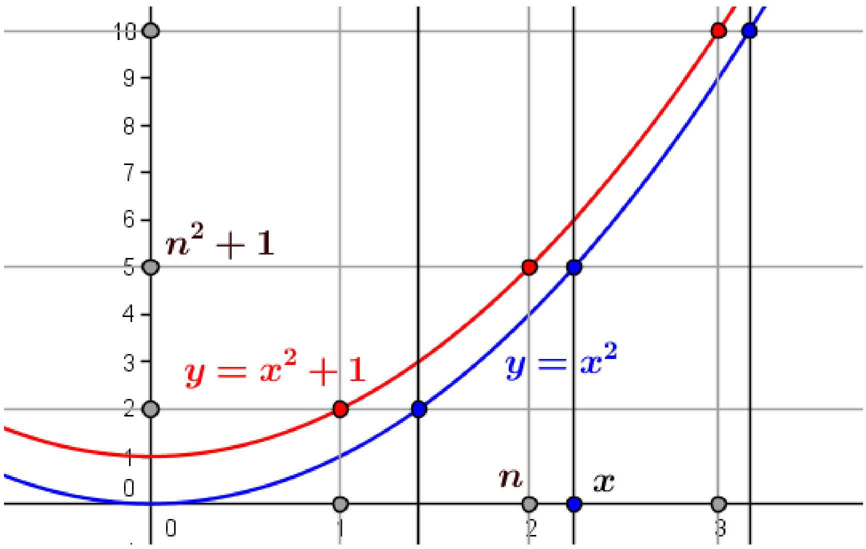


Figure 5.6: Si $n > 0$ est entier, alors $n^2 + 1$ n'est pas un carré : l'abscisse du point de la courbe $y = x^2$ d'ordonnée $n^2 + 1$ n'est pas un entier, autrement dit $n^2 + 1$ n'est pas le carré d'un entier.

5.4.2 Le raisonnement par l'absurde

Le raisonnement par l'absurde, ou par *reductio ad absurdum* en latin, consiste, pour démontrer la véracité d'un énoncé P, à supposer que P est faux (c'est-à-dire que $\neg P$ est vrai), et à en tirer une contradiction. Autrement dit, on cherche à démontrer $(\neg P) \Rightarrow \bot$, où $\bot$ est un symbole qui désigne un énoncé faux.
Par définition, ce dernier énoncé est $\neg(\neg P) \vee \bot$, équivalent par double négation à $P \vee \bot$, équivalent lui-même à P, par définition de la disjonction, puisque $\bot$ n'est pas vrai !
On utilise habituellement ce type de raisonnement lorsqu'on "tourne en rond" avec un autre type de raisonnement. Ce mode de raisonnement est peut-être le plus célèbre, à la fois par sa puissance (certains théorèmes n'ont de démonstration connue que par l'absurde) et par son caractère mystérieux (il paraît étrange de pouvoir démontrer quelque chose de vrai en établissant quelque chose d'absurde). Nous allons l'illustrer par deux résultats, dont un joli théorème sur l'irrationalité de la racine carrée de 2.

Proposition 5.4.5. *Si n est un entier naturel strictement positif, alors n^2+1 n'est pas un carré.*

Démonstration. On raisonne par l'absurde : on suppose que l'énoncé est faux, autrement dit qu'il est faux que "pour tout entier naturel $n > 0$, n^2+1 n'est pas un carré". La négation de cet énoncé est donc "il existe un entier naturel $n > 0$ tel que n^2+1 est un carré", et on suppose qu'elle est vraie, pour chercher une contradiction. Dans ce cas, il existe un entier naturel $n > 0$ qui est un carré, donc il existe aussi un entier naturel a tel que $n^2+1 = a^2$, ce qu'on peut réécrire $a^2 - n^2 = 1$, ou encore $(a+n)(a-n) = 1$. En particulier, aucun des deux entiers relatifs $a+n$ et $a-n$ ne sont nuls (sinon, en raisonnant par cas, $(a+n)(a-n) = 0$). Comme $a \in \mathbb{N}$, on a aussi $a+n \geq n > 0$, donc $a+n$ est un entier positif, si bien que $a-n$ lui-même est un entier positif (sinon, on a $1 = (a+n)(a-n) < 0$, ce qui est faux : par l'absurde, on a $a-n \geq 0$). Il s'ensuit que $a+n = a-n = 1$, d'où $n = -n$, c'est-à-dire $n = 0$, ce qui contredit l'hypothèse que $n > 0$. Par *reductio ad absurdum*, on en conclut que si $n > 0$, le nombre n^2+1 n'est pas un carré. $\square$

Remarque 5.4.6. Dans cette preuve, on a un autre raisonnement par l'absurde "imbriqué" : il s'agit de l'argument qui établit que $a-n > 0$. Lorsque des raisonnements très courts et très simples sont nécessaires, on omet, selon le niveau du lecteur, de l'auditeur ou de l'interlocuteur, de préciser les détails de ces raisonnements. Dans la preuve, on a encore un autre raisonnement par l'absurde imbriqué : où se trouve-t-il ?

Si p est un nombre premier (notion définie dans l'exemple 2.4.8) et n un entier relatif quelconque, *l'exposant de p dans n* est par définition le plus grand entier naturel r tel que p^r divise n (si $p \nmid n$, alors $r = 0$, et si $p|n$, il n'existe qu'un nombre fini d'entiers naturels s tels que $p^s|n$, et on prend le plus grand, selon un principe évoqué précédemment).
Par exemple, comme $72 = 8 \times 9 = 2^3.3^2$, l'exposant de 2 dans 72 est 3, et l'exposant de 3 est 2. De même, comme $20 = 4 \times 5 = 2^2.5$, l'exposant de 2 dans 20 est 2, et

celui de 5 est 1. L'exposant des nombres premiers ne divisant pas un nombre donné est nul.
On peut le reformuler comme suit : l'exposant de p dans n est l'unique entier naturel r tel que l'on peut écrire $n = p^r.m$, avec $p \nmid m$. Avec cette notion, on peut démontrer par l'absurde le fameux théorème suivant, qui s'interprète géométriquement grâce au théorème de Pythagore en disant que la longueur de la diagonale d'un carré de côté 1 n'est pas un nombre rationnel :

Théorème 5.4.7. *Il n'existe pas de nombre rationnel r tel que $r^2 = 2$.*

Démonstration. Supposons, par l'absurde, qu'il existe au contraire un nombre rationnel r tel que $r^2 = 2$, et écrivons $r = a/b$, avec $b \in \mathbb{N}$, ce qui est toujours possible. Soit s l'exposant du nombre premier 2 dans b : par définition, on peut écrire $b = 2^s.c$, avec $2 \nmid c$, d'où $b^2 = (2^s.c)^2 = (2^s)^2.c^2 = 2^{2s}.c^2$. Comme le carré d'un entier impair est un entier impair par la proposition 5.2.1, on peut aussi dire que $2 \nmid c^2$, si bien que l'exposant de 2 dans b^2 est pair, égal à $2s$. De même, l'exposant de 2 dans a^2 est pair et on a $a^2 = 2b^2 = 2.(2^{2s}).c = 2^{2s+1}.c$. Comme $2 \nmid c$ par définition de c, on conclut que l'exposant de 2 dans a^2 est $2s + 1$, ce qui contredit le fait qu'il est pair. Par *reductio ad absurdum*, on en conclut qu'il n'existe aucun nombre rationnel r tel que $r^2 = 2$. □

Remarque 5.4.8. Ici, la contradiction à laquelle nous aboutissons, est que l'exposant de 2 dans a^2 est à la fois pair et impair, ce qui est absurde (c'est-à-dire un énoncé faux).

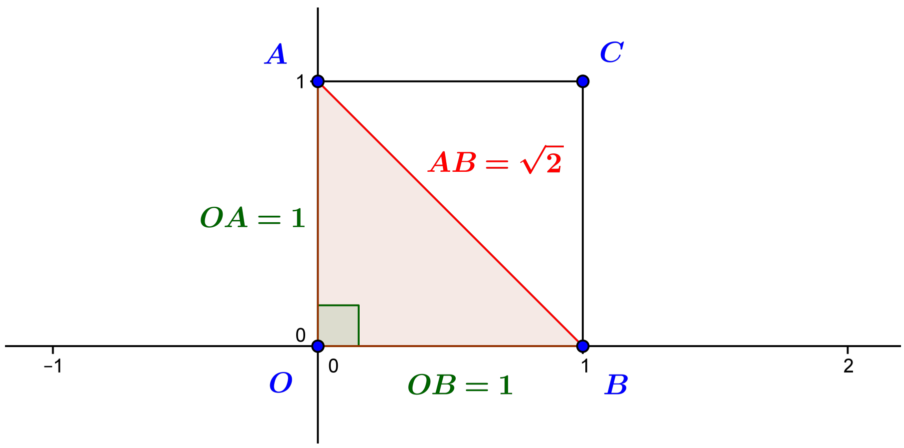


Figure 5.7: Par le théorème de Pythagore appliqué au triangle AOB rectangle en O, on a $AB^2 = OA^2 + OB^2 = 2$, donc $AB = \sqrt{2}$: la longueur de la diagonale AB du carré $OBCA$ n'est pas un nombre rationnel.

Exercices de la leçon

Exercice 5.4.9. i) Démontrer la proposition 5.4.1 en utilisant un raisonnement par cas ($d < d'$ ou $d' < d$).
ii) Démontrer la proposition 5.4.3 par disjonction des cas, en distiguant $x < y$ et $y < x$. Indication : si $x < y$, poser $z = y - x > 0$ et remplacer $y - x$ par z dans

$(x+1)(y-1)$ et $(x-1)(y+1)$.
iii) On admet que si p est un nombre premier, a un entier naturel et $p \nmid a$, alors $p \nmid a^2$. Démontrer qu'il n'existe pas de nombre rationnel r tel que $r^2 = p$.
iv) Expliquer comment la proposition 5.4.5 peut être démontrée par contraposée.

5.5 Le raisonnement par récurrence

5.5.1 Principe du raisonnement par récurrence

Si le raisonnement par l'absurde est possiblement le plus connu, le raisonnement par récurrence est possiblement le plus emblématique de la science mathématique, et celui qui fascine et déconcerte le plus.
Il est aussi appelé raisonnement *par induction*, par analogie avec l'induction scientifique qui consiste à "étayer" une hypothèse par la multiplication d'observations, et est utilisé lorsqu'on cherche à démontrer une propriété P (qui dépend) des entiers naturels, autrement dit un énoncé de la forme $\forall n \in \mathbb{N}, P(n)$.
Notons bien qu'un tel énoncé porte souvent sur bien d'autres relations entre objets connexes autres que les entiers naturels, implicites dans la formule $P(n)$, qui dénote une clause pouvant être complexe et mentionnant des termes et quantifications pour des objets particuliers ou génériques quelconques.
Par exemple, la clause $P(n)$: "$\forall x \in \mathbb{R}_+, \forall y \in \mathbb{R}_+,\ x \leq y \Rightarrow x^n \leq y^n$", où n désigne un entier naturel générique, est une propriété de n, mais elle mentionne des nombres réels génériques (nous démontrerons la véracité de $\forall n \in \mathbb{N}, P(n)$ dans le lemme 5.5.4).
Le raisonnement par récurrence consiste à démontrer $P(0)$, c'est-à-dire la propriété P pour la valeur $n = 0$ (ce qu'on appelle *l'amorce de la récurrence*), et en supposant que $P(n)$ est vraie (ce qu'on appelle *l'hypothèse de récurrence*) à démontrer que $P(n+1)$ est vraie c'est ce qu'on appelle *l'étape de récurrence.* De "proche en proche", cela entraîne que $P(n)$ est vrai pour tout entier naturel n.
Dans l'exemple choisi, la propriété $P(0)$ est "$\forall x \in \mathbb{R}_+, \forall y \in \mathbb{R}_+,\ x \leq y \Rightarrow 1 \leq 1$", puisque $x^0 = 1$ pour tout nombre réel x. L'étape de récurrence consiste alors à démontrer $P(n+1)$, c'est-à-dire "$\forall x \in \mathbb{R}_+, \forall y \in \mathbb{R}_+,\ x \leq y \Rightarrow x^{n+1} \leq y^{n+1}$", en supposant $P(n)$.
On raisonne de cette manière car, l'ensemble $\mathbb{N}$ étant intuitivement "infini", il n'est pas possible de démontrer la propriété $P(n)$ pour tous les entiers naturels n individuellement, soit $P(0)$, $P(1)$, $P(2)$, ...
La justification de ce type d'argument repose sur le *principe de récurrence*, propriété axiomatique fondamentale de l'ensemble $\mathbb{N}$, et que nous étudierons précisément dans les deuxième et troisième cours de ce semestre.
Sur le plan de l'intuition, le raisonnement par récurrence pourrait se comparer à l'ascension d'une échelle infinie : on ne peut pas compter le nombre de barreaux à franchir pour aboutir en haut de l'échelle, mais si nous savons que nous pouvons franchir le premier barreau, et que nous pourrons toujours passer d'un barreau au barreau suivant, nous croyons que nous pourrons aller jusqu'en haut.
Certains aiment aussi le comparer à un jeu de dominos : il faut faire tomber le premier domino, puis chaque fois qu'un domino tombe, il entraîne dans sa chute

le domino suivant et de proche en proche, tous les dominos tombent. De même, il faut démontrer la propriété pour le premier entier, puis de proche en proche, chaque fois qu'elle est démontrée pour un entier, elle sera vraie pour l'entier suivant, *si du moins* on peut démontrer le passage d'une étape à l'autre, ce qui est souvent l'effort sur lequel porte la démonstration.
Ce qui rend les choses possibles, c'est qu'on ne démontre par chaque étape de récurrence individuellement, mais de manière "générique". Nous illustrerons l'usage du raisonnement par récurrence dans la démonstration de plusieurs propriétés numériques fondamentales.

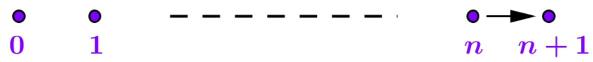


Figure 5.8: Principe du raisonnement par récurrence : on démontre la propriété à l'étape 0, puis on la démontre à l'étape $n+1$ à partir de l'étape n, laquelle est l'hypothèse de récurrence. On peut commencer le raisonnement à une autre étape que 0, par exemple à 1 pour démontrer une propriété valable pour tout entier $n \geq 1$.

5.5.2 La somme des n premiers entiers naturels non nuls

L'expression suivante est très importante, il faut savoir s'en souvenir ou la retrouver quand c'est nécessaire.

Proposition 5.5.1. *Pour tout entier naturel n, la somme $1+2+\ldots+n$ des n premiers entiers naturels non nuls est égale à* $\dfrac{n(n+1)}{2}$.

Démonstration. Nous procédons par récurrence sur n. Si $n = 0$ (amorce de la récurrence), par convention la somme $1+2+\ldots+n$, qui ne possède "aucun terme", vaut 0, tandis que $n(n+1) = 0(0+1) = 0$, donc la propriété est vérifiée au rang $n = 0$. Supposons qu'elle le soit au rang n, c'est-à-dire que pour un certain $n \in \mathbb{N}$, nous avons l'égalité $1+2+\ldots+n = \frac{n(n+1)}{2}$ (hypothèse de récurrence) : nous voulons montrer que cette égalité est valide au rang $n+1$ (étape de récurrence), c'est-à-dire en remplaçant n par $n+1$, autrement dit que $(1+2+\ldots+n)+(n+1) = \frac{(n+1)(n+2)}{2}$. Par hypothèse de récurrence, on peut remplacer $1+2+\ldots+n$ par sa valeur, soit $\frac{n(n+1)}{2}$, pour écrire $1+2+\ldots+n+(n+1) = \frac{n(n+1)}{2}+n+1 = \frac{n(n+1)}{2} + \frac{2(n+1)}{2}$ (par réduction au même dénominateur) $= \frac{n(n+1)+2n+2}{2} = \frac{n^2+n+2n+2}{2} = \frac{n^2+3n+2}{2}$. D'un autre côté, le second membre de l'équation à vérifier est $\frac{(n+1)(n+2)}{2} = \frac{n^2+2n+n+2}{2} = \frac{n^2+3n+2}{2}$, et finalement on obtient $1+2+\ldots+n+(n+1) = \frac{(n+1)(n+2)}{2}$, ce qui est la propriété au rang $n+1$. Par le principe de récurrence, l'égalité est valable pour tout $n \in \mathbb{N}$, et la proposition est démontrée. □

Remarque 5.5.2. i) Puisque l'étape-clef du raisonnement par récurrence consistant à établir $P(n+1)$ à partir de $P(n)$, il est important dans la pratique de bien écrire ces deux propriétés pour identifier un moyen de passer de l'une à l'autre.

ii) Lorsqu'on utilise l'hypothèse de récurrence, c'est-à-dire qu'on suppose que la propriété à démontrer est vérifiée à "l'étape" ou au "rang" n, l'entier n est temporairement "fixé", c'est-à-dire choisi, dans le flot du raisonnement, mais il est générique, c'est-à-dire quelconque.

5.5.3 Définitions par récurrence

Nous avons défini intuitivement, dans le troisième chapitre, la puissance n-ième d'un nombre réel comme le produit de ce nombre par lui-même "n fois". Il faudrait rigoureusement *définir* ce que cela signifie. Ceci est possible grâce aux *définitions par récurrence.*
Si l'on peut, en effet, faire des démonstrations par récurrence, on peut également faire des définitions, de certaines expressions par exemple, par récurrence. Il s'agit, comme pour la démonstration, de définir une expression (un terme) $f(n)$, en une variable libre n pour un entier naturel disons, en définissant $f(0)$, et, supposant établie la définition de $f(n)$, en définissant $f(n+1)$.
Le principe de ce procédé sera partiellement justifié au troisième cours avec celui de la démonstration par récurrence, pour l'instant nous l'illustrons par la définition de la puissance d'un nombre réel et nous en découvrirons l'intérêt dans les démonstrations par récurrence qui suivent.

Définition 5.5.3. Si a est un nombre réel et n un entier naturel, définissons par récurrence l'expression "a^n" : on pose $a^0 = 1$, et supposant que a^n est défini, on pose $a^{n+1} := a^n.a$.

On comprend bien, intuitivement, qu'à la n-ième étape, on multiple le résultat obtenu par a, ce qui traduit bien l'idée que a^n est la multiplication de a par lui-même, n fois.

Lemme 5.5.4. *Pour tous nombres réels positifs a et b tels que $a \leq b$ et tout entier naturel n, on a $a^n \leq b^n$.*

Démonstration. On procède par récurrence sur n. Si $n = 0$, alors $a^n = a^0 = 1 = b^0 = b^n$ par convention, donc l'inégalité tient pour $n = 0$. Supposons qu'elle soit vérifiée pour un entier n, autrement dit que $a^n \leq b^n$: on a alors $a^{n+1} = a^n.a$ (par définition) $\leq a^n.b$ (car $a \leq b$ et $b^n \geq 0$) $\leq b^n.b$ (en appliquant l'hypothèse de récurrence et la multiplication par $b \geq 0$) $= b^{n+1}$ (par définition), donc la propriété est vérifiée au rang $n+1$, et par le principe de récurrence, elle est vérifiée pour tout $n \in \mathbb{N}$. $\square$

Remarque 5.5.5. i) On voit bien dans cette démonstration comment la définition et le raisonnement par récurrence vont de pair. Si on est encore gêné par l'idée de définition par récurrence, on peut temporairement s'appuyer sur l'intuition à partir de laquelle on a défini a^n.
ii) Nous avons admis dans la démonstration que $b^n \geq 0$ pour tout n. Il faudrait le démontrer, par récurrence, ce qui est un bon moyen de vérifier qu'on a compris le principe de la démonstration (voir les exercices).

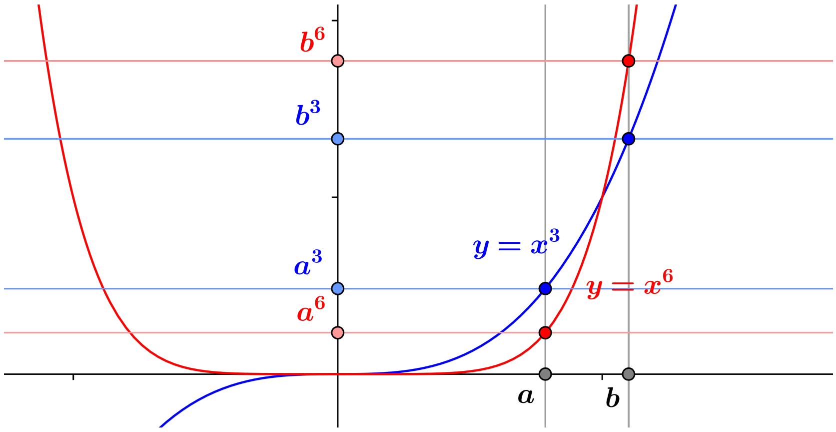


Figure 5.9: Si $a, b \in \mathbb{R}_+$ et $a \leq b$, alors $a^n \leq b^n$: illustration avec $n = 3$ et $n = 6$. On devine que la comparaison de a^n et b^n pour $a, b \in \mathbb{R}_-$ fait intervenir la parité de n.

5.5.4 Factorielle et puissance

La proposition suivante illustre comment le raisonnement par récurrence permet d'établir rigoureusement une propriété qui paraît "évidemment vraie", mais qu'on ne peut établir par un raisonnement direct.

En effet, si $n \geq 1$ on rappelle que par définition le nombre $n!$ (appelé "factorielle n") vaut $1 \times 2 \times \ldots \times n$, soit le produit des n premiers entiers naturels non nuls, et comme chaque facteur, strictement positif, de ce produit, est inférieur à n, le produit est "évidemment" inférieur ou égal au produit de n facteurs chacun égal à n. Autrement dit, on a $n! \leq n^n$ pour tout entier naturel n; mais comment le démontrer ?

Nous allons passer là aussi par des définitions par récurrence. En ce qui concerne la factorielle, par convention on pose $0! = 1$ et $n!$ étant supposé défini, on pose $(n+1)! = n!(n+1)$.

De même, pour définir n^n nous devrions faire un peu attention : l'expression a^n a bien été définie pour un nombre réel a, mais alors le nombre a était constant ! Ici, nous devons considérer d'une part n comme le nombre réel de base (c'est-à-dire a), d'autre part comme exposant entier, donc considérer la définition de a^m par récurrence sur m, et l'appliquer au cas où $m = n$ et où $a = n$. Cela ne pose pas de problème dans la proposition suivante, où seule la définition par récurrence de $n!$ est utilisée directement dans le raisonnement.

Proposition 5.5.6. *Pour tout entier naturel n, on a $n! \leq n^n$.*

Démonstration. Nous procédons par récurrence sur n. Si $n = 0$, alors par convention $n! = 0! = 1$ et $n^n = 0^0 = 1$, donc l'inégalité est vérifiée pour $n = 0$. Supposons qu'elle le soit pour un entier n, c'est-à-dire que $n! \leq n^n$, et montrons qu'elle l'est pour $n+1$. Par définition, on a $(n+1)! = n!(n+1)$, et par hypothèse de récurrence, comme $n+1 \geq 0$ on a $(n+1)! \leq n^n.(n+1)$. D'autre part, on a aussi $n \leq n+1$, donc $n^n \leq (n+1)^n$ par le lemme 5.5.4 (appliqué à $a = n$ et $b = n+1$), si bien que $n^n.(n+1) \leq (n+1)^n(n+1) = (n+1)^{n+1}$, et en mettant ensemble ces inégalités on obtient $(n+1)! \leq n^n.(n+1) \leq (n+1)^{n+1}$, ce qui est l'inégalité au rang $n+1$. Par le principe de récurrence, l'inégalité est vérifiée pour tout $n \in \mathbb{N}$, et la proposition est démontrée. $\square$

Remarque 5.5.7. i) La définition par récurrence de a^n est utilisée indirectement sous la forme de la référence au lemme 5.5.4.
ii) Dans toutes ces démonstrations nous n'écrivons pas tous les détails, sans quoi elles seraient beaucoup trop longues, ce qui paradoxalement nuirait à leur clarté. Il appartient toujours au lecteur d'une démonstration mathématique d'en compléter les détails, notamment les modalités d'application d'un lemme à une proposition, comme c'est ici le cas : nous n'avons pas expliqué en détail pourquoi le lemme peut s'appliquer, c'est à l'étudiant(e) ou la lectrice de le faire. L'essentiel est de ne pas laisser sans explication les points essentiels et les points difficiles de la démonstration.

L'expression $n!$ est définie pour des entiers naturels. On peut toutefois la prolonger à une fonction (notion abordée dans le second cours) notée Γ sur l'ensemble des nombres complexes privé des entiers négatifs (soit sur $\mathbb{C} - \mathbb{Z}_-$), au sens où pour tout $n \in \mathbb{N}^*$, on a $\Gamma(n) = (n-1)!$, et appelée "fonction Gamma d'Euler", du nom de l'illustre mathématicien qui l'a découverte, et qui est liée à la fameuse Hypothèse de Riemann, problème mathématique formidable qui n'a pas encore (à ce jour) reçu de démonstration.
Nous terminons ce cours par une égalité essentielle et ubiquitaire, dont la démonstration constituera un des exercices de la leçon. Il s'agit d'une expression donnant la somme des $n+1$ premières puissances d'un nombre complexe a, le cas $a = 1$ étant considéré comme "évident", ou "trivial" comme on dit en mathématique.
Pour être rigoureux, il faut définir cette somme, qu'on note $1 + a + \ldots + a^n$, où l'on sous-entend que $1 = a^0$. L'expression a^n étant définie comme pour les nombres réels, on définit par récurrence la somme $1 + a + \ldots + a^n$ comme suit : si $n = 0$, alors la somme commence à 1 et s'arrête à 1, donc elle vaut 1. Supposons qu'elle soit définie au rang n, on pose alors $1 + a + \ldots + a^n + a^{n+1} = (1 + a + \ldots + a^n) + a^{n+1}$. Cela paraît inutile parce qu'évident, il faut se convaincre (peut-être plus tard !) qu'il n'en est rien.

Théorème 5.5.8. *Soit a un nombre complexe.*
i) Si $a = 1$, alors on a $1 + a + \ldots + a^n = n + 1$.
ii) Si $a \neq 1$, alors on a $1 + a + a^2 + \ldots + a^n = \dfrac{1 - a^{n+1}}{1 - a}$.

Remarque 5.5.9. Les énoncés de propositions mathématiques peuvent se présenter, comme ici, comme une liste de propriétés. Il faut alors bien entendu démontrer chacune d'entre elles.

Exercices de la leçon

Les exercices suivant puisent éventuellement, comme d'habitude, dans les connaissances et exercices abordés dans les sections précédentes.

Exercice 5.5.10. o) Démontrer que pour tout nombre réel $x \geq 0$, et pour tout entier naturel n, on a $x^n \geq 0$.

i) Démontrer par induction que pour tout $n \in \mathbb{N}$, on a $n < 2^n$.
ii) Démontrer par récurrence que pour tout entier relatif impair n et tout entier naturel m, l'entier n^m est impair.

Problème 5.5.11. Démontrer le théorème 5.5.8.

Index