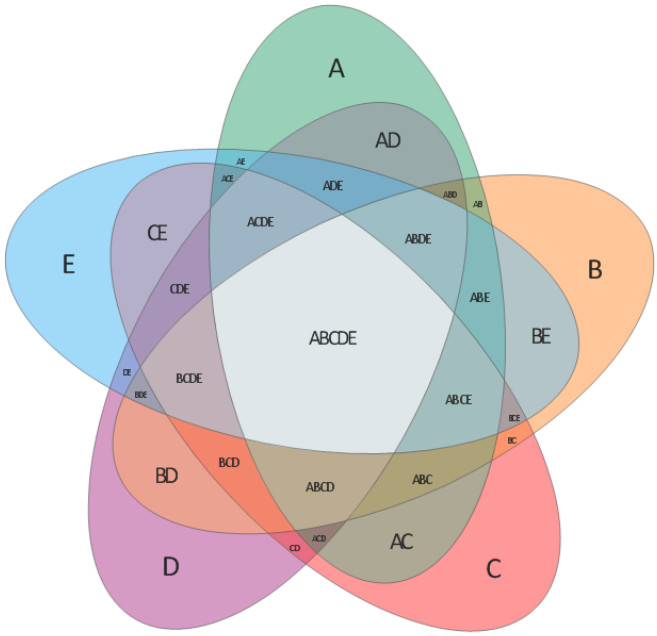
Raisonnement Mathématiques & Preuves

MAT 1762

Hiver 2023



Alistair Savage

Traduit et adapté de l'anglais par Simon Fortier-Garceau

Département de mathématiques et de statistique

Université d'Ottawa

Table des matières

Préface

Voici les notes pour le cours MAT 1762 - *Raisonnement Mathématiques & Preuves* à l'université d'Ottawa. Il s'agit d'une introduction au raisonnement mathématique rigoureux et au concept de preuve en mathématiques. C'est un cours dont l'objet est de préparer les étudiants aux cours de haut niveau en mathématiques, lesquels sont centrés sur les preuves. On abordera la méthode axiomatique et plusieurs méthodes de preuve (preuve par contradiction, l'induction mathématique, etc.). On effectue cela dans un contexte lié à certaines notions fondamentales en mathématiques qui sont cruciales aux cours de mathématiques de haut niveau. Cela inclut les bases de la théorie naïve des ensembles, les fonctions et les relations. On discutera également, de manière précise, les entiers, les entiers modulo n, les nombres rationnels et les nombres réels. Additionnellement, on abordera des concepts liés à la droite réelle, tels que la complétude, les supremums et la définition précise de limite. En général, ce cours est conçu pour donner aux étudiants une fondation théorique solide sur laquelle il est possible d'ériger dans des cours subséquents.

Ce cours devrait être d'intérêt aux étudiants qui ressentent une certaine insatisfaction face aux cours de mathématiques dans lesquels l'accent est mis sur les calculs plutôt que sur les preuves et explications. Dans le cours MAT 1762, on effectuera rarement des calculs basés sur les techniques et algorithmes usuels, comme calculer des dérivés en employant les règles de dérivation en chaîne ou du produit. Au lieu, on mettra l'accent sur *pourquoi* certains énoncés mathématiques sont vrais et *pourquoi* les techniques employées fonctionnent. Cela est bien plus difficile que de suivre un algorithme pour entreprendre un calcul. Toutefois, le résultat de ce travail est bien plus satisfaisant et l'étudiant atteindra un niveau de compréhension beaucoup plus élevé face à la matière.

Remerciement: Une portion significative de ces notes suit de près le livre The Art of Proof par Matthias Beck and Ross Geoghegan [BG10], lequel constitue le manuel officiel pour le cours.

Alistair Savage

Site web du cours (anglais): `https://alistairsavage.ca/mat1362`

Chapitre 1

Entiers

Dans ce chapitre, on aborde les entiers. Quoique vous ayez rencontré les entiers dans plusieurs cours antécédemment, en remontant jusqu'au primaire, vous avez sans doutes pris certaines propriétés pour acquis. Dans ce cours, on débutera avec certains axiomes claires et on déduira d'autres propriétés des entiers en procédant plus rigoureusement.

1.1 Axiomes

On abordera le concept d'un ensemble plus tard, soit au Chapitre 5. Pour l'instant, on emploiera le terme intuitivement. Un ensemble S est une collection de choses, appelées les *éléments* ou *membres* de S. On écrit $a \in S$ pour indiquer que a est un élément de S. Une *opération binaire* sur un ensemble S est une fonction qui reçoit deux éléments de S comme entrées et produit un élément de S comme sortie.

On supposera qu'il existe un ensemble $\mathbb{Z}$, dont les membres seront appelés les *entiers*. Cet ensemble vient avec deux opérations binaires:

- l'*addition*, dénoté $+$, et
- la *multiplication*, dénoté $\cdot$.

On dénotera souvent la multiplication par la *juxtaposition* (i.e. $a \cdot b$ pourra s'écrire ab).

On suppose que $\mathbb{Z}$, en incluant ces opérations, satisfait les cinq axiomes suivants, de même que les Axiomes 2.1 et 2.17 qui seront introduits au Chapitre 2.

Axiome 1.1 (Commutativité, associativité et distributivité)**.**

Pour tous entiers a, b et c, on a

(i) $a + b = b + a$, (*commutativité de l'addition*)

(ii) $(a + b) + c = a + (b + c)$, (*associativité de l'addition*)

(iii) $a \cdot (b + c) = a \cdot b + a \cdot c$, (*distributivité*)

(iv) $a \cdot b = b \cdot a$, (*commutativité de la multiplication*)

(v) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$. (*associativité de la multiplication*)

Axiome 1.2 (Élément neutre additif)**.** Il existe un entier 0 tel que $a+0 = a$ pour tout $a \in \mathbb{Z}$. Cet élément 0 est appelé un *élément neutre additif*, ou un *élément identité de l'addition*.

Axiome 1.3 (Élément neutre multiplicatif)**.** Il existe un entier 1 tel que $1 \neq 0$ et $a \cdot 1 = a$ pour tout $a \in \mathbb{Z}$. L'élément 1 est appelé un *élément neutre multiplicatif*, ou un *élément identité de la multiplication*.

Axiome 1.4 (Inverse additif)**.** Pour chaque $a \in \mathbb{Z}$, il existe un entier, dénoté $-a$, tel que $a + (-a) = 0$. L'élément $-a$ est appelé l'*inverse additif* de a.

Axiome 1.5 (Annulation (multiplicative))**.** Si $a, b, c \in \mathbb{Z}$, $a \cdot b = a \cdot c$ et $a \neq 0$, alors $b = c$. Cela est appelé la *propriété d'annulation* (multiplicative à gauche).

Le symbole "=" veut dire *égal*. Quand on écrit $a = b$ pour des éléments a et b d'un ensemble S (e.g. $\mathbb{Z}$), on veut dire que a et b sont *le même élément*. Ce symbole admet les propriétés que, pour tous objets a, b et c d'un ensemble S,

(i) $a = a$. (*réflexivité de l'égalité*)

(ii) Si $a = b$, alors $b = a$. (*symétrie de l'égalité*)

(iii) Si $a = b$ et $b = c$, alors $a = c$. (*transitivité de l'égalité*)

(iv) Si $a = b$, alors a peut être remplacé (substitué) par b dans tout énoncé ou expression, sans changer le sens de l'énoncé ou de l'expression. Par exemple, si $a, b, c \in \mathbb{Z}$ et $a = b$, alors on peut remplacer a par b dans une expression comme $a + c$ et déduire que $a + c = b + c$. On appelle cela la propriété de *substitution*.

Le symbole $\neq$ veut dire *n'est pas égal à*. Lorsqu'on écrit $a \neq b$ pour $a, b \in \mathbb{Z}$, on veut dire que a et b ne sont pas les mêmes éléments de $\mathbb{Z}$ (ils sont des éléments distincts). Notez les faits suivants:

(i) Le symbole $\neq$ n'est pas réflexif: on n'a jamais $a \neq a$.

(ii) Le symbole $\neq$ est symétrique: si $a, b \in \mathbb{Z}$ et $a \neq b$, alors $b \neq a$.

(iii) Le symbole $\neq$ n'est pas transitif: par exemple, $1 \neq 2$ et $2 \neq 1$, mais il est faux que $1 \neq 1$ (ce qu'impliquerait la transitivité).

Le symbole $\notin$ veut dire *n'est pas un élément de*.

1.2 Premières conséquences des axiomes

Pour le moment, on suppose *seulement* les Axiomes 1.1–1.5. C'est-à-dire, qu'à priori, on n'utilisera aucune autre propriété des entiers que vous pourriez avoir apprise lors de cours antécédents en mathématiques. On déduira des propriétés des entiers *à partir* des axiomes, et une fois que l'on aura démontré qu'un énoncé est vrai, on aura le droit de s'en servir pour des démonstrations de propriétés subséquentes. En général, on veut supposer un minimum d'axiomes et démontrer que, en soi, elles *impliquent* un grand nombre de propriétés additionnelles. Notez, par exemple, que l'on a *pas* encore introduit l'opération de soustraction. (On verra cela à la Section 1.3.)

Proposition 1.6. *Pour tous $a, b, c \in \mathbb{Z}$, $(a+b)c = ac + bc$.*

Preuve. Considérons (n'importe quels) $a, b, c \in \mathbb{Z}$. Alors, nous avons

$$\begin{aligned} (a+b)c &= c(a+b) && \text{Axiome 1.1(iv) (comm. de la mult.)} \\ &= ca + cb && \text{Axiome 1.1(iii) (distributivité)} \\ &= ac + bc. && \text{Axiome 1.1(iv) (comm. de la mult.)} \end{aligned}$$

□

Proposition 1.7. *Pour tout $a \in \mathbb{Z}$, $0 + a = a$ et $1 \cdot a = a$.*

Preuve. La preuve de cette proposition est laissée en exercice (Exercice 1.2.1). □

Proposition 1.8. *Pour tout $a \in \mathbb{Z}$, $(-a) + a = 0$.*

Preuve. La preuve de cette proposition est laissée en exercice (Exercice 1.2.2). □

Proposition 1.9. *Pour tous $a, b, c \in \mathbb{Z}$, si $a + b = a + c$, alors $b = c$.*

Preuve. Soient $a, b, c \in \mathbb{Z}$. Supposons que $a + b = a + c$. Alors,

$$\begin{aligned} & a + b = a + c \\ \implies & (-a) + (a + b) = (-a) + (a + c) && \text{propriété de substitution} \\ \implies & ((-a) + a) + b = ((-a) + a) + c && \text{Axiome 1.1(ii) (assoc. de +)} \\ \implies & 0 + b = 0 + c && \text{Proposition 1.8} \\ \implies & b = c. && \text{Proposition 1.7} \end{aligned}$$

□

Ci-haut, on a employé le symbole $\implies$. Si P et Q sont deux énoncés, alors $P \implies Q$ veut dire que P *implique* Q, c'est-à-dire que Q suit logiquement de P. On peut également lire "si P, alors Q".

Proposition 1.10 (Unicité de l'inverse additif)**.** *Si $a, b \in \mathbb{Z}$ et $a + b = 0$, alors $b = -a$. En d'autres mots, l'élément $-a$ mentionné par l'Axiome 1.4 est l'*unique *inverse additif de a (i.e. tout entier admet* exactement un *inverse additif).*

Preuve. Supposons que $a, b \in \mathbb{Z}$. Alors on a

$$\begin{aligned} & a + b = 0 \\ \implies & (-a) + (a + b) = (-a) + 0 && \text{propr.de subst.} \\ \implies & (-a) + (a + b) = -a && \text{Axiome 1.2 (élém. neutre de +)} \\ \implies & ((-a) + a) + b = -a && \text{Axiome 1.1(ii) (assoc. de +)} \\ \implies & 0 + b = -a && \text{Proposition 1.8} \\ \implies & b = -a. && \text{Proposition 1.7} \end{aligned}$$

□

La Proposition 1.10 est un bon exemple de la façon dont on a cherché à minimiser les axiomes pour les entiers. On aurait pu formulé l'Axiome 1.4 en énonçant que tout entier admet un *unique* inverse additif. Toutefois, la Proposition 1.10 démontre que l'axiome plus faible d'exiger *au moins un* inverse additif est suffisant, i.e. l'unicité de l'inverse additif découle des axiomes.

Proposition 1.11. *Supposons que $a, b, c, d \in \mathbb{Z}$. Alors*

(i) $(a+b)(c+d) = (ac+bc)+(ad+bd)$,

(ii) $a+(b+(c+d)) = (a+b)+(c+d) = ((a+b)+c)+d$,

(iii) $a+(b+c) = (c+a)+b$,

(iv) $a(bc) = c(ab)$,

(v) $a(b+(c+d)) = (ab+ac)+ad$,

(vi) $(a(b+c))d = (ab)d+a(cd)$.

Preuve. On démontre la partie (v) et on laisse les autres parties en exercice (Exercice 1.2.3).

Prenons $a, b, c, d \in \mathbb{Z}$. On obtient

$$\begin{aligned} a(b+(c+d)) &= ab+a(c+d) && \text{Axiome 1.1(iii) (distrib.)} \\ &= ab+(ac+ad) && \text{Axiome 1.1(iii) (distributivity)} \\ &= (ab+ac)+ad. && \text{Axiome 1.1(ii) (assoc. de +)} \end{aligned}$$

□

Proposition 1.12 (Unicité de l'élément neutre additif)**.** *Soit $a \in \mathbb{Z}$. Si a satisfait la propriété $b+a = b$ pour tout $b \in \mathbb{Z}$, alors $a = 0$. En d'autres mots, l'élément neutre additif est unique.*

Preuve. Supposons que $a \in \mathbb{Z}$ satisfait la propriété $b+a = b$ pour tout $b \in \mathbb{Z}$. En particulier, en choisissant $b = 0$, on obtient

$$\begin{aligned} & 0+a = 0 \\ \implies\ & a = 0. && \text{Proposition 1.7} \end{aligned}$$

□

Proposition 1.13. *Soit $a \in \mathbb{Z}$. Si a satisfait la propriété $b+a = b$ pour un* certain *$b \in \mathbb{Z}$, alors $a = 0$.*

Preuve. Supposons que $a \in \mathbb{Z}$ satisfait la propriété $b+a = b$ pour un $b \in \mathbb{Z}$. Par l'Axiome 1.4, b admet un inverse additif $-b \in \mathbb{Z}$. Donc

$$\begin{aligned} & b+a = b \\ \implies\ & (-b)+(b+a) = (-b)+b && \text{propr. de subst.} \end{aligned}$$

$$\begin{aligned}
&\implies ((-b)+b)+a=(-b)+b && \text{Axiome 1.1(ii) (assoc. de +)}\\
&\implies 0+a=0 && \text{Proposition 1.8}\\
&\implies a=0. && \text{Proposition 1.7}
\end{aligned}$$

□

Notez la différence entre les Propositions 1.12 et 1.13. Dans la Proposition 1.12, l'équation $b+a=b$ est supposée vraie pour *tout* $b\in\mathbb{Z}$, tandis que dans la Proposition 1.13, elle est supposée vraie pour un *certain* $b\in\mathbb{Z}$.

Proposition 1.14. *Si $a\in\mathbb{Z}$, alors $a\cdot 0=0=0\cdot a$.*

Preuve. Soit $a\in\mathbb{Z}$. On a

$$\begin{aligned}
&0=0+0 && \text{Axiome 1.2 (élém. neutre de +)}\\
&\implies a\cdot 0=a\cdot(0+0) && \text{substitution}\\
&\implies a\cdot 0=a\cdot 0+a\cdot 0 && \text{Axiome 1.1(iii) (distributivité)}\\
&\implies a\cdot 0+\big(-(a\cdot 0)\big)=(a\cdot 0+a\cdot 0)+\big(-(a\cdot 0)\big) && \text{substitution}\\
&\implies a\cdot 0+\big(-(a\cdot 0)\big)=a\cdot 0+\Big(a\cdot 0+\big(-(a\cdot 0)\big)\Big) && \text{Axiome 1.1(ii) (assoc. de +)}\\
&\implies 0=a\cdot 0+0 && \text{Axiome 1.4 (inverse additif)}\\
&\implies 0=a\cdot 0 && \text{Axiome 1.2 (élém. neutre additif).}
\end{aligned}$$

L'égalité $0=0\cdot a$ suit de l'Axiome 1.1(iv) (comm. de la mult.). □

Pour $a,b\in\mathbb{Z}$, on dit que a *est divisible par* b (ou que b *divise* a) s'il existe $c\in\mathbb{Z}$ tel que $a=bc$. On écrira $b\mid a$ pour indiquer que a est divisible par b et $b\nmid a$ pour indiquer que a n'est pas divisible par b.

Comment peut-on définir un entier pair? Bien, comme vous l'avez appris au primaire, un entier *pair* est un entier qui est divisible par 2. Mais qu'est-ce que 2? Aucun des axiomes ou des énoncés que nous avons démontrées ne dit quoi que soit sur l'entier 2. Toutefois, on peut *définir* 2 comme étant l'entier $1+1$.

Proposition 1.15. *Si a et b sont des entiers pairs, alors $a+b$ et ab sont également pairs.*

Preuve. Supposons que a et b sont des entiers pairs, i.e. que $2\mid a$ et $2\mid b$. Alors, par définition, il existe $j,k\in\mathbb{Z}$ tels que $a=2j$ et $b=2k$. Ainsi

$$\begin{aligned}
a+b&=2j+2k && \text{propr. de subst.}\\
&=2(j+k) && \text{Axiome 1.1(iii) (distrib.)}
\end{aligned}$$

Puisque $j+k\in Z$, alors $a+b$ est divisible par 2, c'est-à-dire qu'il est pair.

La preuve que ab est pair est laissée en exercice (Exercice 1.2.4). □

Proposition 1.16.

(i) 0 *est divisible par tout entier.*

(ii) Si $a \in \mathbb{Z}$ *et* $a \neq 0$*, alors* $0 \nmid a$*.*

Preuve. (i) Soit $m \in \mathbb{Z}$. On a $0 = m \cdot 0$ par la Proposition 1.14. Ainsi, selon la définition de divisibilité, 0 est divisible par m.

(ii) Soit $a \in \mathbb{Z}$. Supposons que a est divisible par 0. Alors, par la définition de divisibilité, il existe $k \in \mathbb{Z}$ tel que $a = 0 \cdot k$. Mais, $0 \cdot k = 0$ par la Proposition 1.14. Donc $a = 0$. Ainsi, on a démontré que le seul nombre divisible par zéro est zéro lui-même. Il s'ensuit que, si $a \neq 0$, alors $0 \nmid a$.

□

Proposition 1.17 (Unicité de l'élément neutre multiplicatif)**.** *Si* $a \in \mathbb{Z}$ *a la propriété que* $ba = b$ *pour tout* $b \in \mathbb{Z}$*, alors* $a = 1$*.*

Preuve. La preuve de cette proposition est laissée en exercice (Exercice 1.2.5). □

Proposition 1.18. *Si* $a \in \mathbb{Z}$ *a la propriété que, pour un entier* $b \neq 0$*,* $ba = b$*, alors* $a = 1$*.*

Preuve. Supposons qu'un $a \in \mathbb{Z}$ a la propriété en question. Donc, il existe un $b \in \mathbb{Z}$ non nul tel que $ba = b$. Prenons un tel $b \in \mathbb{Z}$.

$$\begin{aligned} & ba = b \\ \implies & b \cdot a = b \cdot 1 && \text{Axiome 1.3 (élém neutre mult.)} \\ \implies & a = 1. && \text{Axiome 1.5 (annulation)} \end{aligned}$$

□

Proposition 1.19. *Pour tous $a, b \in \mathbb{Z}$, $(-a)b = -(ab)$.*

Preuve. Considérons $a, b \in \mathbb{Z}$. Alors

$$\begin{aligned}
& a + (-a) = 0 && \text{Axiome 1.4 (inverse additif)} \\
\implies & (a + (-a))b = 0 \cdot b && \text{prop. de subst.} \\
\implies & (a + (-a))b = 0 && \text{Prop. 1.14} \\
\implies & ab + (-a)b = 0 && \text{Prop. 1.6} \\
\implies & (-a)b = -(ab). && \text{Prop. 1.10}
\end{aligned}$$

□

Proposition 1.20.

(i) Pour tout $a \in \mathbb{Z}$, $-(-a) = a$.

(ii) $-0 = 0$.

Preuve. (i) On a

$$\begin{aligned}
& (-a) + -(-a) = 0 && \text{Axiome 1.4 (inverse additif)} \\
\implies & 0 = (-a) + a && \text{Prop. 1.8} \\
\implies & (-a) + -(-a) = (-a) + a && \text{transitivité de l'égalité} \\
\implies & -(-a) = a. && \text{Prop. 1.9}
\end{aligned}$$

(ii) On a

$$\begin{aligned}
& 0 + 0 = 0 && \text{Axiome 1.2 (élément neutre add.)} \\
\implies & 0 = -0. && \text{Proposition 1.10}
\end{aligned}$$

□

Proposition 1.21. *Pour tous $a, b \in \mathbb{Z}$, $(-a)(-b) = ab$. En particulier, $(-1)(-1) = 1$.*

Preuve. Supposons que $a, b \in \mathbb{Z}$. Alors

$$\begin{aligned}
(-a)(-b) &= -\big(a(-b)\big) && \text{Prop. 1.19} \\
&= -((-b)a) && \text{Axiome 1.1(iv) (comm. de la mult.)} \\
&= -(-(ba)) && \text{Prop. 1.19} \\
&= -(-(ab)) && \text{Axiome 1.1(iv) (comm. de la mult.)} \\
&= ab. && \text{Prop. 1.20(i)}
\end{aligned}$$

□

Proposition 1.22. *Supposons que $a, b \in \mathbb{Z}$. Alors, il existe un unique $c \in \mathbb{Z}$ tel que $a + c = b$.*

Notez que la Proposition 1.22 affirme l'existence d'*un et un seul* c avec la propriété en question. Donc, cet énoncé affirme deux choses: il *existe* un tel c (la partie "existence" de l'énoncé), et deux éléments satisfaisant la propriété en question doivent être égaux (la partie "unicité" de l'énoncé). Plus tard, une fois que l'on aura abordé la soustraction, l'élément c de la Proposition 1.22 sera dénoté $b - a$.

Preuve de la Proposition 1.22. Soient a, b des entiers. Pour démontrer la partie existence de l'énoncé, il suffit de trouver un élément avec la propriété. On a déjà a et b à notre disposition pour le construire et, en fait, $(-a) + b$ nous donne un tel élément, car

$$\begin{aligned} a + \big((-a) + b\big) &= \big(a + (-a)\big) + b && \text{Axiom 1.1(ii) (assoc. de +)} \\ &= 0 + b && \text{Axiome 1.4 (inverse additif)} \\ &= b. && \text{Proposition 1.7} \end{aligned}$$

Il reste à démontrer l'unicité. Supposons que c_1 et c_2 sont deux éléments avec la propriété en question. On obtient donc

$$a + c_1 = b = a + c_2 \implies c_1 = c_2,$$

où l'implication résulte de la Proposition 1.9. □

Proposition 1.23. *Si $a \in \mathbb{Z}$ satisfait $a \cdot a = a$, alors $a = 0$ ou $a = 1$.*

Preuve. La preuve de cette proposition est laissée en exercice (Exercice 1.2.6). □

Proposition 1.24. *Pour tous $a, b \in \mathbb{Z}$, on a*

(i) $-(a + b) = (-a) + (-b)$,

(ii) $-a = (-1)a$, *et*

(iii) $(-a)b = a(-b) = -(ab)$.

Preuve. La preuve de cette proposition est laissée en exercice (Exercice 1.2.7). Notez qu'une partie de (iii) a déjà été démontré à la Proposition 1.19. □

Remarque 1.25. En mathématiques, le mot "ou", sans d'autres qualificatifs, s'interprète toujours inclusivement. Par exemple, de dire que "P ou Q" est vrai veut dire que "P" est vrai, ou "Q" est vrai, ou les deux.

Proposition 1.26. *Si $a, b \in \mathbb{Z}$ satisfont $ab = 0$, alors $a = 0$ ou $b = 0$.*

Preuve. Supposons qu'on a des entiers a, b satisfaisant $ab = 0$. Alors

$$a \cdot b = 0 = a \cdot 0.$$

On sépare la preuve en deux cas exhaustifs: $a = 0$ et $a \neq 0$.

Cas 1: Si $a = 0$, alors l'énoncé "$a = 0$ ou $b = 0$" est vrai, et on a terminé.

Cas 2: Si $a \neq 0$, alors, par l'Axiome 1.5, on peut conclure $b = 0$. Ainsi, l'énoncé "$a = 0$ ou $b = 0$" est vrai.

Dans tous les cas possibles, on a établit que "$a = 0$ ou $b = 0$" est vrai. Donc, c'est vrai (peu importe le cas).

□

Exercices.

1.2.1. Démontrez la Proposition 1.7.

1.2.2. Démontrez la Proposition 1.8.

1.2.3. Démontrez les parties restantes de la Proposition 1.11.

1.2.4. Complétez la preuve de la Proposition 1.15.

1.2.5. Démontrez la Proposition 1.17.

1.2.6. Démontrez la Proposition 1.23. *Indice*: Séparez la preuve en deux cas: $a = 0$ et $a \neq 0$.

1.2.7. Démontrez la Proposition 1.24.

1.3 Soustraction

Quoique vous soyez familiers avec la soustraction des entiers, nous n'avons pas encore abordé ce concept: il n'est pas mentionné dans les axiomes et dans les résultats démontrés jusqu'ici. On peut maintenant définir précisément le concept de soustraction.

Définition 1.27 (Soustraction)**.** Étant donné $a, b \in \mathbb{Z}$, on définit $a - b$ par $a + (-b)$. Cette nouvelle opération binaire $-$ est appelée la *soustraction*.

Proposition 1.28. *Pour tous $a, b, c, d \in \mathbb{Z}$, on a*

(i) $(a - b) + (c - d) = (a + c) - (b + d)$,

(ii) $(a - b) - (c - d) = (a + d) - (b + c)$,

(iii) $(a - b)(c - d) = (ac + bd) - (ad + bc)$,

(iv) $a - b = c - d$ *si et seulement si* $a + d = b + c$,

(v) $(a - b)c = ac - bc$.

Preuve. La preuve de la partie (i) se trouve dans [BG10, Prop. 1.27]. On démontre la partie (iii) ici et on laisse la preuve des autres en exercice (Exercice 1.3.1). On a

$$\begin{aligned}
(a-b)(c-d) &= \big(a+(-b)\big)\big((c+(-d))\big) && \text{définition de soustraction}\\
&= \big(ac+(-b)c\big)+\big(a(-d)+(-b)(-d)\big) && \text{Prop. 1.11(i)}\\
&= \big(ac+\big((-b)c+a(-d)\big)\big)+(-b)(-d) && \text{Prop. 1.11(ii)}\\
&= \big(ac+\big((-b)c+a(-d)\big)\big)+bd && \text{Prop. 1.21}\\
&= bd+\big(ac+\big((-b)c+a(-d)\big)\big) && \text{Axiome 1.1(i) (comm. de +)}
\end{aligned}$$

$$
\begin{aligned}
&= (bd + ac) + \big((-b)c + a(-d)\big) && \text{Axiome 1.1(ii) (assoc. de +)} \\
&= (bd + ac) + \big(-(bc) + (-(ad))\big) && \text{Prop. 1.24(iii)} \\
&= (bd + ac) + \big(-(bc + ad)\big) && \text{Prop. 1.24(i)} \\
&= (bd + ac) - (bc + ad) && \text{définition de soustraction} \\
&= (ac + bd) - (ad + bc). && \text{Axiome 1.1(i) (comm. de +)}
\end{aligned}
$$

□

Comme on peut le voir, écrire une preuve en détails, en citant tous les axiomes et les résultats, peut prendre une certaine ampleur. Au fur et à mesure qu'on se familiarise avec les propriétés, on omettra souvent les étapes évidentes, afin que l'on qu'on puisse mettre l'accent sur les nouvelles idées importantes de la preuve, plutôt que sur les aspects techniques mineurs ayant surgit de manière récurrente lors d'arguments antécédents. Or, il est important de réaliser que l'on *pourrait* fournir tous les détails, en justifiant chaque étape si on le voulait.

Remarque 1.29. On a vu dans ce chapitre que l'arithmétique des entiers, telle que définie par nos axiomes, se comporte telle que nous l'avons vu au primaire. À partir de ce point, on commencera à employer librement les propriétés démontrées dans ce chapitre, souvent en omettant certaines des justifications. En particulier, à la Proposition 1.11(ii), on voit qu'il est admissible de déplacer les parenthèses comme on le veut lorsqu'on additionne plusieurs entiers, laissant le résultat inchangé. De ce fait, si $a, b, c, d \in \mathbb{Z}$, on peut écrire sans ambiguïté des expressions comme

$$a + b + c + d,$$

puisque le résultat de l'addition est le même, peu importe comment on regroupe les termes.

Exercices.

1.3.1. Démontrez les parties restantes de la Proposition 1.28.

Chapitre 2

Nombres naturels et induction

Dans ce chapitre, on introduit les nombres naturels et l'ordre sur les entiers. Puis, on voit aussi les principes importants de l'induction mathématique et du bon ordre.

2.1 Nombres naturels

Dans le Chapitre 1, on a introduit les entiers. Or, vous avez peut-être remarqué qu'aucun de nos axiomes et résultats jusqu'ici ne s'est référé aux nombres *positifs* ou *négatifs*, ni même aux relations "plus grand que" ou "plus petit que". On introduit un autre axiome pour établir ces notions.

Axiome 2.1 (Nombres naturels)**.** Il existe un sous-ensemble $\mathbb{N}$ de $\mathbb{Z}$ avec les propriétés suivantes:

(i) Si $a, b \in \mathbb{N}$, alors $a + b \in \mathbb{N}$. (Le sous-ensemble $\mathbb{N}$ est fermé sous l'addition.)

(ii) Si $a, b \in \mathbb{N}$, alors $ab \in \mathbb{N}$. (Le sous-ensemble $\mathbb{N}$ est fermé sous la multiplication.)

(iii) $0 \notin \mathbb{N}$.

(iv) Pour tout $a \in \mathbb{Z}$, $a \in \mathbb{N}$ ou $a = 0$ ou $-a \in \mathbb{N}$.

On appelle les membres de $\mathbb{N}$ les *nombres naturels* ou *entiers positifs*. Un *entier négatif* est un entier qui n'est ni positif ni zéro.

Remarque 2.2. Il est important de constater que certaines références emploient le symbole $\mathbb{N}$ pour désigner un sous-ensemble de $\mathbb{Z}$ légèrement différent de celui présenté ci-haut. Plus spécifiquement, elles incluent le 0 dans l'ensemble des nombres naturels. Gardez cela à l'esprit lorsque vous consulté d'autres sources, pour éviter toute confusion.

La preuve de la prochaine proposition emploie la méthode de *preuve par contradiction*. Cette technique s'agence comme suit: Disons que l'on veut démontrer qu'un certain énoncé P est vrai. Au lieu de le faire directement, on peut montrer que l'hypothèse adverse (i.e. que P est faux) mène à une contradiction logique (tel que $1 = 0$). On utilise implicitement le *principe du tiers exclu*, lequel énonce que P doit être vrai ou faux. Donc, si l'hypothèse que P est faux mène à une contradiction, alors P doit être vrai.

Proposition 2.3. *Pour $a \in \mathbb{Z}$, un et un seul des énoncés suivants est vrai:*

- $a \in \mathbb{N}$,
- $-a \in \mathbb{N}$,
- $a = 0$.

Preuve. Soit $a \in \mathbb{Z}$. Par l'Axiome 2.1(iv), au moins un de ces énoncés est vrai. Il suffit donc de démontrer qu'*au plus* un de ces énoncés est vrai à l'égard de a.

Tout d'abord, supposons que $a = 0$. Alors, par l'Axiome 2.1(iii), $a \notin \mathbb{N}$. Aussi, par la Proposition 1.20(ii), il est vrai que $-a = -0 = 0$. De ce fait, par l'Axiome 2.1(iii), $-a \notin \mathbb{N}$ non plus.

Il reste à démontrer que, si $a \neq 0$, alors a et $-a$ ne peuvent pas tous les deux être dans $\mathbb{N}$. On effectue cela avec une preuve par contradiction. Ainsi, on suppose que l'énoncé

$$a \text{ et } -a \text{ ne sont pas tous les deux dans } \mathbb{N} \tag{2.1}$$

est faux. Cela est équivalent à faire l'hypothèse que l'énoncé

$$a \in \mathbb{N} \text{ et } -a \in \mathbb{N} \tag{2.2}$$

est vrai. En supposant cela, l'Axiome 2.1(i), nous dit que

$$a + (-a) \in \mathbb{N}.$$

Toutefois, par l'Axiome 1.4, nous avons $a + (-a) = 0$. Donc, $0 \in \mathbb{N}$. Mais cela contredit l'Axiome 2.1(iii). Ainsi, l'hypothèse (2.2) doit être fausse. Conséquemment, l'énoncé (2.1) doit être vrai, tel que voulu. □

Proposition 2.4. *On a $1 \in \mathbb{N}$.*

Preuve. Puisque $1 \neq 0$ (par l'axiome de l'élément neutre multiplicatif, l'Axiome 1.3), un et un seul de $1 \in \mathbb{N}$ et $-1 \in \mathbb{N}$ peut être vrai par la Proposition 2.3. Si $-1 \in \mathbb{N}$, alors par la fermeture de $\mathbb{N}$ sous la multiplication (l'Axiome 2.1(ii)), on aurait $1 = (-1)(-1) \in \mathbb{N}$, ce qui contredirait la Proposition 2.3. Donc, $1 \in \mathbb{N}$. □

2.2 Ordre sur les entiers

Maintenant que nous avons introduit les nombres naturels $\mathbb{N}$, nous sommes en mesure d'introduire une relation d'ordre sur les entiers.

Définition 2.5 (Ordre sur les entiers)**.** Étant donné $a, b \in \mathbb{Z}$, on écrit $a < b$ (et on dit que a est *plus petit que* b) ou $b > a$ (et on dit que b est *plus grand que* a) si et seulement si

$$b - a \in \mathbb{N}.$$

On écrit $a \leq b$ (et on dit que a est *plus petit ou égal à* b) ou $b \geq a$ (et on dit que b est *plus grand ou égal à* a) si et seulement si

$$a < b \quad \text{ou} \quad a = b.$$

Proposition 2.6 (Transitivité de $<$)**.** *Supposons que $a, b, c \in \mathbb{Z}$. Si $a < b$ et $b < c$, alors $a < c$. (En d'autres mots, la relation $<$ est transitive.)*

Preuve. Considérons $a, b, c \in \mathbb{Z}$ tels que $a < b$ et $b < c$. Alors, par définition, on a $b - a \in \mathbb{N}$ et $c - b \in \mathbb{N}$. Puis, par l'Axiome 2.1(i)

$$c - a = (c - b) + (b - a) \in \mathbb{N}.$$

Ainsi, $a < c$. □

Proposition 2.7 ($\mathbb{N}$ n'a pas de plus grand élément)**.** *Pour tout $a \in \mathbb{N}$, il existe un $b \in \mathbb{N}$ tel que $b > a$.*

Preuve. La preuve de cette proposition est laissée en exercice (Exercice 2.2.1). □

Proposition 2.8. *Si $a, b \in \mathbb{Z}$ satisfont $a \leq b \leq a$, alors $a = b$.*

Preuve. Supposons que $a, b \in \mathbb{Z}$ satisfont $a \leq b \leq a$. Supposons, en vue d'une contradiction, que $a \neq b$. Alors $a < b < a$. Par définition, cela veut dire que

$$b - a \in \mathbb{N} \quad \text{et} \quad a - b \in \mathbb{N}.$$

Alors, par l'Axiome 2.1(i),

$$0 = (a - b) + (b - a) \in \mathbb{N}.$$

Cela contredit l'Axiome 2.1(iii). Étant donné que l'hypothèse $a \neq b$ mène à une contradiction, on doit avoir $a = b$. □

Proposition 2.9. *Soient $a, b, c, d \in \mathbb{Z}$.*

(i) Si $a < b$, alors $a + c < b + c$.

(ii) Si $a < b$ et $c \leq d$, alors $a + c < b + d$.

(iii) Si $0 < a < b$ et $0 < c \leq d$, alors $ac < bd$.

(iv) Si $a < b$ et $c < 0$, alors $bc < ac$.

Preuve. La preuve de la partie (iii) se trouve dans [BG10, Prop. 2.7]. On va démontrer la partie (iv) et on laisse la preuve des autres parties en exercice (Exercice 2.2.2).

Supposons que $a, b, c \in \mathbb{Z}$ satisfont $a < b$ et $c < 0$. Donc, $b - a \in \mathbb{N}$ et

$$-c = 0 + (-c) = 0 - c \in \mathbb{N}.$$

Puis, par l'Axiome 2.1(ii),

$$(b - a)(-c) \in \mathbb{N}.$$

Or,

$$(b - a)(-c) = b(-c) - a(-c) = ac - bc.$$

Il s'ensuit que $ac - bc \in \mathbb{N}$, et donc $bc < ac$. □

Proposition 2.10. *Soient $a, b \in \mathbb{Z}$. Alors exactement un des énoncés suivants est vrai:*

- $a < b$,
- $a = b$,
- $a > b$.

Preuve. La preuve de cette proposition est laissée en exercice (Exercice 2.2.3). □

Proposition 2.11. *Si $a \in \mathbb{Z}$ et $a \neq 0$, alors $a^2 \in \mathbb{N}$. (Ici, a^2 veut dire $a \cdot a$.)*

Preuve. La preuve de cette proposition est laissée en exercice (Exercice 2.2.4). □

Proposition 2.12. *Il n'y a pas de $a \in \mathbb{Z}$ satisfaisant $a^2 = -1$.*

Preuve. On démontre cela avec une preuve par contradiction. Supposons qu'un tel $a \in \mathbb{Z}$ existe avec $a^2 = -1$. Par la Proposition 2.3, on peut séparer la preuve en trois cas:

Cas 1: $a = 0$. Alors $a^2 = 0 \cdot 0 = 0$, et donc $0 = -1$. En ajoutant 1 de chaque côté, on obtient $1 = 0$, ce qui contredit l'Axiome 1.3.

Cas 2: $a \in \mathbb{N}$. Dans ce cas, on a $-1 = a^2 \in \mathbb{N}$ par la fermeture de $\mathbb{N}$ sous la multiplication (Axiome 2.1(ii)). Par la Proposition 2.3, on conclut que $1 \notin \mathbb{N}$, ce qui contredit la Proposition 2.4.

Cas 3: $-a \in \mathbb{N}$. Alors, par la fermeture de $\mathbb{N}$ sous la multiplication (Axiome 2.1(ii)), on obtient $-1 = a^2 = (-a)(-a) \in \mathbb{N}$. Et comme dans le cas précédent, cela est impossible.

Dans tous les cas possibles, on parvient à une contradiction. Cela termine la preuve par contradiction. □

Proposition 2.13. *Si $a \in \mathbb{N}$ et $b \in \mathbb{Z}$ satisfont $ab \in \mathbb{N}$, alors $b \in \mathbb{N}$.*

Preuve. La preuve de cette proposition est laissée en exercice (Exercice 2.2.5). □

Proposition 2.14. *Supposons que $a, b, c, d \in \mathbb{Z}$.*

(i) $-a < -b$ *si et seulement si* $a > b$.

(ii) Si $c > 0$ *et* $ac < bc$, *alors* $a < b$.

(iii) Si $c < 0$ *et* $ac < bc$, *alors* $b < a$.

(iv) Si $a \leq b$ *et* $0 \leq c$, *alors* $ac \leq bc$.

Preuve. On démontre la partie (iv) et on laisse les autres en exercice (Exercice 2.2.6). Supposons que $a \leq b$ et $0 \leq c$. On sépare la preuve en trois cas.

Cas 1: $c = 0$. Alors $ac = 0$ et $bc = 0$. Donc $ac \leq bc$ car $0 \leq 0$.

Cas 2: $c > 0$ et $a = b$. Alors $ac = bc$, et donc $ac \leq bc$ est vrai.

Cas 3: $c > 0$ et $a < b$. Alors on a $c \in \mathbb{N}$ et $b - a \in \mathbb{N}$. Puis,

$$bc - ac = (b - a)c \in \mathbb{N},$$

par la fermeture de $\mathbb{N}$ sous la multiplication (Axiome 2.1(ii)). Ainsi, $ac \leq bc$. □

Si A et B sont des ensembles, on écrit $A \subseteq B$ pour dire que A est un sous-ensemble de B. Plus spécifiquement, $A \subseteq B$ se définit à travers

$$x \in A \implies x \in B.$$

Deux ensembles A et B sont *égaux*, dénoté $A = B$, si

$$A \subseteq B \quad \text{et} \quad B \subseteq A.$$

On définit $A = B$ formellement à travers

$$x \in A \iff x \in B.$$

(Si P et Q sont des énoncés, alors "$P \iff Q$" veut dire "$P \implies Q$ *et* $Q \implies P$".) On peut également écrire $A \subsetneq B$ pour dire

$$A \subseteq B \quad \text{et} \quad A \neq B.$$

Notez que cela *diffère* du symbole $\not\subseteq$, lequel veut dire "n'est pas un sous-ensemble de". De ce fait $A \not\subseteq B$ si et seulement s'il existe au moins un élément de A qui n'est pas un élément de B.

Il est préférable d'éviter le symbole $\subset$ en raison de son ambiguïté: certains auteurs emploient $\subset$ au sens de $\subseteq$, alors que d'autres l'emploient au sens de $\subsetneq$.

Proposition 2.15. *L'ensemble* $\mathbb{N} = \{n \in \mathbb{Z} : n > 0\}$.

Preuve. Soit m. On a

$$m \in \{n \in \mathbb{Z} : n > 0\} \iff m \in \mathbb{Z} \text{ et } m > 0 \iff m \in \mathbb{Z} \text{ et } m = m - 0 \in \mathbb{N} \iff m \in \mathbb{N}.$$

□

Exercices.

2.2.1. Démontrez la Proposition 2.7.

2.2.2. Démontrez les parties restantes de la Proposition 2.9.

2.2.3. Démontrez la Proposition 2.10.

2.2.4. Démontrez la Proposition 2.11.

2.2.5. Démontrez la Proposition 2.13. *Indice*: Considérez les trois cas: $b < 0$, $b = 0$ et $b > 0$.

2.2.6. Démontrez les parties restantes de la Proposition 2.14.

2.3 Induction

Dans cette section on introduit une méthode de preuve importante: *l'induction mathématique*. Cette méthode est basée sur les nombres naturels, et il nous faut introduire un dernier axiome sur les entiers avant d'en discuter. Or, avant d'énoncer cet axiome, on commence avec une proposition.

Proposition 2.16.

(i) $1 \in \mathbb{N}$.

(ii) $n \in \mathbb{N} \implies n+1 \in \mathbb{N}$.

Preuve. La preuve de la proposition est laissée en exercice (Exercice 2.3.1). Notez que la partie (i) a déjà été démontrée à la Proposition 2.4. □

Le nouvel axiome énonce que $\mathbb{N}$ est le plus petit ensemble de $\mathbb{Z}$ satisfaisant la Proposition 2.16.

Axiome 2.17 (Axiome d'induction)**.** Supposons qu'un sous-ensemble $A \subseteq \mathbb{Z}$ satisfait les propriétés suivantes:

(i) $1 \in A$,

(ii) $n \in A \implies n+1 \in A$.

Alors $\mathbb{N} \subseteq A$.

Proposition 2.18. *Supposons que* $B \subseteq \mathbb{N}$ *satisfait:*

(i) $1 \in B$,

(ii) $n \in B \implies n+1 \in B$.

Alors $B = \mathbb{N}$.

Preuve. Par hypothèse, $B \subseteq \mathbb{N}$, et l'Axiome 2.17 nous donne $\mathbb{N} \subseteq B$. Donc $B = \mathbb{N}$. □

La Proposition 2.18 est la base du principe d'induction.

Théorème 2.19 (Principle d'induction mathématique: première forme)**.** *Supposons que, pour tout* $k \in \mathbb{N}$*, on a un énoncé* $P(k)$*. De plus, supposons que*

(i) $P(1)$ *est vrai, et*

(ii) pour tout $n \in \mathbb{N}$, $P(n) \implies P(n+1)$.

Alors $P(k)$ *est vrai pour tout* $k \in \mathbb{N}$.

Preuve. Supposons que (i) et (ii) sont vrais. Prenons

$$B := \{k \in \mathbb{N} : P(k) \text{ est vrai}\}.$$

Alors $1 \in B$ par (i) et $n \in B \implies n+1 \in B$ par (ii). Ainsi, par la Proposition 2.18, $B = \mathbb{N}$. En d'autres mots, $P(k)$ est vrai pour tout $k \in \mathbb{N}$. □

Les preuves qui emploient le Théoréme 2.19 sont appelées *preuves par induction*. Dans une preuve par induction, l'énoncé (i) est souvent appelé le *cas de base* et l'énoncé (ii) est souvent appelé l'*étape inductive*. En démontrant l'étape inductive, on commence typiquement par choisir un $n \in \mathbb{N}$ arbitraire, puis à émettre l'hypothèse que $P(n)$ est vrai pour ce n. Ensuite, on montre que $P(n+1)$ découle de cette hypothèse. Pour cette étape, $P(n)$ est appelé l'*hypothèse d'induction*.

Pour être en mesure de donner des exemples intéressant de preuve par induction, il nous faut des noms pour désigner les entiers. On définit les *chiffres*

$$\begin{aligned} 2 &:= 1+1, \\ 3 &:= 2+1, \\ &\vdots \\ 9 &:= 8+1. \end{aligned}$$

On peut ensuite définir les nombres écrit en notation à base dix, e.g. 11 et 56, tel qu'on l'a appris au primaire. Cela fait l'objet d'une discussion détaillée dans [BG10, Ch. 7], mais on omettra cette discussion pour ce cours.

Exemple 2.20. Nous allons démontrer par induction que $11^n - 6$ est divisible par 5 pour tout $n \in \mathbb{N}$. Posons $P(k)$ comme étant l'énoncé

$$11^k - 6 \text{ est divisible par } 5.$$

(Nous allons définir plus précisément les puissances à la Section 4.1. Pour l'instant, il nous faut simplement les propriétés que $11^1 = 11$ et que $11^{n+1} = 11^n \cdot 11$ pour tout $n \in \mathbb{N}$.)

Cas de base: $P(1)$ est l'énoncé que $11^1 - 6$ est divisible par 5. Puisque $11^1 - 6 = 5 = 5 \cdot 1$, cela est vrai.

Étape inductive: Prenons un $n \in \mathbb{N}$. Supposons que $P(n)$ est vrai pour ce n, c'est-à-dire que $11^n - 6$ est divisible par 5. Par définition de divisibilité, il existe un $m \in \mathbb{Z}$ tel que

$$11^n - 6 = 5m.$$

On veut montrer que l'énoncé $P(n+1) :=$"$11^{n+1} - 6$ est divisible par 5" est vrai. Or, on a

$$\begin{aligned} 11^{n+1} - 6 &= 11 \cdot 11^n - 6 \\ &= 11(5m+6) - 6 && \text{(par l'hypothèse d'induction)} \\ &= 55m + 66 - 6 \\ &= 55m + 60 \end{aligned}$$

$$= 5(11m + 12).$$

Ainsi, $11^{n+1} - 6$ est divisible par 5. En d'autres mots, $P(n+1)$ est vrai. Cela termine la preuve de la partie inductive.

Par le Principe d'induction (Théorème 2.19), on peut conclure que $5 \mid 11^k - 6$ pour tout $k \in \mathbb{N}$.

Proposition 2.21. *Pour tout $a \in \mathbb{N}$, $a \geq 1$.*

Preuve. On démontre cela par induction sur a. Soit $P(a)$ l'énoncé

$$a \geq 1.$$

Cas de base: Le cas de base $P(1)$ est vrai car $1 \geq 1$.

Étape inductive: Supposons que $P(m) := m \geq 1$ est vrai pour un certain $m \in \mathbb{N}$. (On veut montrer que $P(m+1) := m + 1 \geq 1$ est vrai.) Puisque $m \geq 1$, alors soit $m = 1$, soit $m > 1$. Si $m = 1$, alors

$$(m + 1) - 1 = m = 1 \in \mathbb{N},$$

et donc $m + 1 > 1$; i.e. $m + 1 \geq 1$. D'une autre part, si $m > 1$, alors $m - 1 \in \mathbb{N}$, et donc

$$(m + 1) - 1 = (m - 1) + 1 \in \mathbb{N}$$

par la Proposition 2.16(ii). Ainsi $m + 1 > 1$, et donc $m + 1 \geq 1$.

Dans les deux cas possibles ($m = 1$ ou $m > 1$), on a démontré que $m + 1 \geq 1$, i.e. $P(m + 1)$ est vrai. Par le Principe d'induction, $a \geq 1$ pour tout $a \in \mathbb{N}$. □

Proposition 2.22. *Il n'a pas d'entier a satisfaisant $0 < a < 1$.*

Preuve. Supposons, en vue d'une contradiction, qu'il existe un entier a satisfaisant $0 < a < 1$. Considérons un tel a. Puisque $a > 0$, alors nous avons $a \in \mathbb{N}$. Puis, selon la Proposition 2.21, nous avons $a \geq 1$. Étant donné que $a < 1$ implique $a \leq 1$, alors

$$1 \leq a \leq 1.$$

Par la Proposition 2.8, on obtient $a = 1$. Mais $a < 1$, donc on obtient l'inégalité $1 < 1$, lequel veut dire $0 = 1 - 1 \in \mathbb{N}$. Cela contredit l'Axiome 2.1(iii). Donc, notre hypothèse initiale est fausse. Ainsi, il n'y a pas d'entier a satisfaisant $0 < a < 1$. □

Corollaire 2.23. *Soit $b \in \mathbb{Z}$. Alors, il n'y a pas d'entier a satisfaisant $b < a < b + 1$.*

Preuve. La preuve de ce corollaire est laissée en exercice (Exercice 2.3.3). □

Proposition 2.24. *Soient $a, b \in \mathbb{N}$. Si $b \mid a$, alors $b \leq a$.*

Preuve. On démontre cela avec une preuve par contradiction. Prenons $a, b \in \mathbb{N}$, puis supposons que $b \mid a$, et que $b > a$. Par définition de la division, il existe $c \in \mathbb{Z}$ tel que $a = bc$. En substituant a par bc dans $b > a$, on obtient $b > bc$ (et donc $b \cdot 1 > bc$). On a $b > 0$ et, par la Proposition 2.14(ii), il s'ensuit que $1 > c$. Alors, les Proposition 2.22 et 2.10 impliquent que $c \leq 0$.

Cas 1: $c = 0$. Dans ce cas, nous avons $a = b \cdot 0 = 0$, ce qui contredit l'hypothèse $a \in \mathbb{N}$ (par l'Axiome 2.1(iii)).

Cas 2: $c < 0$. Dans ce cas $-c = 0 - c \in \mathbb{N}$. Ainsi,

$$-a = -(bc) = b(-c) \in \mathbb{N},$$

et cela contredit l'hypothèse que $a \in \mathbb{N}$ (par la Proposition 2.3).

Dans tous les cas, on parvient à une contradiction, donc cela complète la preuve. □

Proposition 2.25. *Si $a \in \mathbb{N}$, alors $a^2 + 1 > a$.*

Preuve. On démontre le résultat par induction sur a. Le cas de base est $a = 1$, lequel est vrai car $1^2 + 1 = 2 > 1$.

Pour l'étape inductive, supposons que $n^2+1 > n$ pour un certain $n \in \mathbb{N}$. Alors, $n^2+1-n \in \mathbb{N}$. Puis, on a

$$(n+1)^2 + 1 - (n+1) = n^2 + n + 1 = (n^2 + 1 - n) + 2n \in \mathbb{N}.$$

Ainsi, $(n+1)^2 + 1 > n + 1$, et cela complète l'étape inductive. □

Parfois, on veut démarrer l'induction à un entier autre que 1.

Théorème 2.26 (Principe d'induction mathématique: première forme revisité)**.** *Supposons que m est un entier fixé et que, pour tout $k \in \mathbb{Z}$ avec $k \geq m$, on a un énoncé bien défini $P(k)$. De plus, supposons que*

(i) $P(m)$ est vrai, et

(ii) pour tout $n \geq m$, $P(n) \implies P(n+1)$.

Alors, $P(k)$ est vrai pour tout $k \geq m$.

Preuve. En écrivant $Q(k) := P(k + m - 1)$ pour tout $k \in \mathbb{N}$, alors ce théorème revient au cas du Théorème 2.19. Voir [BG10, Th. 2.25] pour les détails. □

Exemple 2.27. Nous allons démontrer que

$$3k^2 + 15k + 19 \geq 0 \text{ pour tout entier } k \geq -2.$$

Cas de base: Lorsque $k = -2$, nous avons $3(-2)^2 + 15(-2) + 19 = 12 - 30 + 19 = 1 > 0$. Donc l'énoncé est vrai pour $k = -2$.

Étape inductive: Supposons que l'énoncé est vrai pour un certain $k \geq -2$. Alors

$$\begin{aligned} 3(k+1)^2 + 15(k+1) + 19 &= 3(k^2 + 2k + 1) + 15k + 15 + 19 \\ &= (3k^2 + 15k + 19) + (6k + 18) \\ &\geq 0 + 6k + 18 = 6k + 18, \end{aligned}$$

Mais, nous avons

$$\begin{aligned} k \geq -2 &\implies 6k \geq -12 && \text{(par la Prop. 2.14(iv))} \\ &\implies 6k + 18 \geq 6 \geq 0 && \text{(par la Prop. 2.9(i)).} \end{aligned}$$

Alors

$$3(k+1)^2 + 15(k+1) + 19 \geq 0, \quad \text{(par la transitivité de } \leq)$$

ce qui complète l'étape inductive.

Exercices.

2.3.1. Démontrez la Proposition 2.16(ii).

2.3.2 ([BG10, Prop. 2.18]). Démontrez les énoncés suivants.

(i) Pour tout $k \in \mathbb{N}$, $k^3 + 2k$ est divisible par 3.

(ii) Pour tout $k \in \mathbb{N}$, $k^4 - 6k^3 + 11k^2 - 6k$ est divisible par 4.

(iii) Pour tout $k \in \mathbb{N}$, $k^3 + 5k$ est divisible par 6.

2.3.3. Démontrez le corollaire 2.23.

2.3.4 ([BG10, Prop. 2.27]). Démontrez que, pour tout entier $k \geq 2$, on a $k^2 < k^3$.

2.4 Le principe du bon ordre

Définition 2.28 (Plus petit et plus grand éléments)**.** Supposons que $A \subseteq \mathbb{Z}$ est non vide. S'il existe un $m \in A$ tel que

$$m \leq a \text{ pour tout } a \in A,$$

alors on dit que m est un *plus petit élément* de A et on écrit $m = \min(A)$. S'il existe un $M \in A$ tel que

$$M \geq a \text{ pour tout } a \in A,$$

alors on dit que M est un *plus grand élément* de A et on écrit $M = \max(A)$.

Proposition 2.29. *Supposons que $A \subseteq \mathbb{Z}$ est non vide.*

(i) Si A admet un plus petit élément, alors cet élément est unique. En d'autres termes, A admet au plus *un plus petit élément.*

(ii) Si A admet un plus grand élément, alors cet élément est unique. En d'autres termes, A admet au plus *un plus grand élément.*

Preuve. Supposons que a et b représentent tous les deux un plus petit élément de A. Alors $a \leq b$ et $b \leq a$. Ainsi, par la Proposition 2.8, on obtient $a = b$. La preuve de la deuxième partie de la proposition est similaire. □

Exemple 2.30. Par les Propositions 2.4 et 2.21, 1 est un plus petit élément de $\mathbb{N}$. D'une autre part, par la Proposition 2.7, $\mathbb{N}$ n'admet pas de plus grand élément.

Exemple 2.31. L'ensemble des entiers pairs n'a ni de plus petit élément, ni de plus grand élément. Toutefois, l'ensemble des entiers pairs négatifs admet un plus grand élément -2, mais pas de plus petit élément.

Remarque 2.32. On emploiera toujours les termes *positifs* et *négatifs* au sens strict. Donc $a \in \mathbb{Z}$ est positif si $a > 0$ et négatif si $a < 0$. On dit que $a \in \mathbb{Z}$ est *non négatif* si $a \geq 0$ (et *non positif* si $a \leq 0$).

Théorème 2.33 (Principe du bon ordre)**.** *Tout sous-ensemble non vide de* $\mathbb{N}$ *admet un plus petit élément.*

Preuve. Définissons l'ensemble

$$A := \{k \in \mathbb{N} : \text{tout sous-ensemble de } \mathbb{N} \text{ contenant un entier} \leq k \text{ admet un plus petit élément}\}.$$

Si on démontre que $A = \mathbb{N}$, alors le théorème suivra. On démontre par induction que A contient tous les nombres naturels (en employant l'axiome d'induction).

Cas de base: Comme à l'exemple 2.30, 1 est le plus petit élément de $\mathbb{N}$. Donc, si un sous-ensemble de $\mathbb{N}$ contient un nombre ≤ 1, il s'agit donc de 1, et ce sera également le plus petit élément de ce sous-ensemble. Donc, $1 \in A$.

Étape inductive: Prenons un $n \in A$. (On veut montrer que $n + 1 \in A$.) Considérons arbitrairement un sous-ensemble $S \subseteq \mathbb{N}$ qui contient un entier $\leq n + 1$. On doit vérifier que S admet un plus petit élément. Si S contient un entier $\leq n$, alors S admet un plus petit élément selon notre hypothèse que $n \in A$. Autrement (i.e. quand S ne contient pas d'entier $\leq n$), S doit contenir $n + 1$, et cet entier est le plus petit élément de S. □

Proposition 2.34. *Supposons que* A *est sous-ensemble non vide de* $\mathbb{Z}$ *et que* $b \in \mathbb{Z}$ *satisfait* $b \leq a$ *pour tout* $a \in A$*. (On dit que* A *est* minoré *par* b*.) Alors,* A *admet un plus petit élément.*

Preuve. Soient A un sous-ensemble non vide de $\mathbb{Z}$ et $b \in \mathbb{Z}$ satisfaisant $b \leq a$ pour tout $a \in A$. On définit un nouvel ensemble

$$B := \{a + 1 - b : a \in A\}.$$

Pour tout entier $a \in A$, nous avons $b \leq a$, donc $b < a + 1$, et donc $a + 1 - b \in \mathbb{N}$. Cela veut dire que $B \subseteq \mathbb{N}$. Et puisque A est non vide, B est non vide aussi. De ce fait, par le principe du bon ordre (Théorème 2.33), B admet un plus petit élément c. Puis, $c = d + 1 - b$ pour un certain $d \in A$ (par la définition de B). Or, pour tout $a \in A$, on a

$$a + 1 - b \in B \implies a + 1 - b \geq c = d + 1 - b \implies a \geq d.$$

Ainsi, d est un plus petit élément de A. □

On veut maintenant employé le principe du bon ordre dans une définition, mais il faut tout d'abord une proposition.

Proposition 2.35. *Supposons que a et b sont deux entiers qui ne sont pas tous les deux nuls. Alors l'ensemble*

$$S = \{k \in \mathbb{N} : k = ax + by \text{ pour des } x, y \in \mathbb{Z}\}$$

est non vide.

Preuve. La preuve de cette proposition est laissée en exercice (Exercice 2.4.1). □

Définition 2.36 (pgcd)**.** Supposons que $a, b \in \mathbb{Z}$. Si a et b ne sont pas tous les deux nuls, on définit

$$\text{pgcd}(a, b) = \min\big(\{k \in \mathbb{N} : k = ax + by \text{ pour des } x, y \in \mathbb{Z}\}\big).$$

(Puisque cet ensemble est non vide par la Proposition 2.35, il admet un minimum par le Théorème 2.33.) Si $a = b = 0$, on définit $\text{pgcd}(0, 0) = 0$.

On verra plus tard que $\text{pgcd}(a, b)$ est en fait le plus grand commun diviseur de a et b, justifiant ainsi sa notation (voir Proposition 6.29).

Exercices.

2.4.1. Démontrez la Proposition 2.35.

Chapitre 3

Logique

On a déjà employé divers arguments logiques dans les Chapitres 1 et 2. L'un des objectifs de ces chapitres étaient de s'initier au concept de preuve avant d'aborder les technicalités de la logique. Dans le chapitre en cours, on examinera certains concepts de base de la logique plus en détail. Cela nous permettra d'être plus précis dans nos arguments mathématiques.

3.1 Quantificateurs

Le symbole $\exists$ est appelé *quantificateur existentiel* et il signifie *il existe*. Le symbole $\forall$ est appelé *quantificateur universel* et il signifie *pour tout* ou *pour chaque*.

Exemples 3.1. (i) "$\exists m \in \mathbb{Z}$ tel que $m > 5$" veut dire "il existe un élément $m \in \mathbb{Z}$ tel que $m > 5$". (Cet énoncé est vrai.)

(ii) "$\forall m \in \mathbb{Z}$, $m < 5$" veut dire "pour tout $m \in \mathbb{Z}$, on a $m < 5$". (Cet énoncé est faux.)

(iii) L'Axiome 1.2 pourrait s'écrire: $\exists 0 \in \mathbb{Z}$ tel que $\forall a \in \mathbb{Z}$, $a + 0 = a$.

(iv) L'Axiome 1.3 pourrait s'écrire: $\exists 1 \in \mathbb{Z}$ tel que ($1 \neq 0$ et $\forall a \in \mathbb{Z}$, $a \cdot 1 = a$).

Les énoncés avec des quantificateurs consistent en des *segments quantifiés* de la forme ($\exists \ldots$ tel que) et/ou ($\forall \ldots$) dans un certain ordre, et suivi de l'*énoncé final* ou assertion. Par exemple, avec l'énoncé (iii) ci-haut, on a

$$\underbrace{(\exists 0 \in \mathbb{Z} \text{ tel que})(\forall a \in Z)}_{\text{segments quantifiés}} \underbrace{a + 0 = a}_{\text{énoncé final}}.$$

L'ordre de ces quantificateurs est *très* important. Considérez les énoncés suivants:

(i) $(\forall a \in \mathbb{Z})(\exists b \in \mathbb{Z}$ tel que$)$ $a + b = 0$

(ii) $(\exists b \in \mathbb{Z}$ tel que$)(\forall a \in \mathbb{Z})$ $a + b = 0$

L'énoncé (i) affirme que, pour chaque entier a, il existe un entier $b \in \mathbb{Z}$, *lequel peut dépendre de* a, tel que $a + b = 0$. Cela est vrai, car on peut choisir $b = -a$. D'une autre part,

l'énoncé (ii) affirme qu'il existe un entier b tel que $a + b = 0$ pour *tout* entier a. Cela est faux, car il n'y a pas de b satisafisant cette condition pour tout a. Ainsi, dans l'énoncé (i), b peut dépendre de a, mais dans l'énoncé (ii) il ne peut pas. La variable employé dans un énoncé quantifié est sans importance. Par exemple, les énoncés

$$(\forall a \in \mathbb{Z})(\exists b \in \mathbb{Z} \text{ tel que})\ a + b = 0 \qquad \text{et} \qquad (\forall m \in \mathbb{Z})(\exists n \in \mathbb{Z} \text{ tel que})\ m + n = 0$$

sont équivalents.

On peut combiner syntaxiquement plusieurs segments quantifiés avec $\forall$ lorsqu'ils se suivent l'un après l'autre. Par exemple

$$(\forall a \in \mathbb{Z})(\forall b \in \mathbb{Z}) \qquad \text{signifie la même chose que} \qquad (\forall a, b \in \mathbb{Z}).$$

Similairement, on peut combiner des segments consécutifs avec $\exists$:

$$(\exists a \in \mathbb{N})(\exists b \in \mathbb{N}) \qquad \text{signifie la même chose que} \qquad (\exists a, b \in \mathbb{N}).$$

Exemples 3.2. On peut exprimer un grand nombre d'énoncé avec les quantificateurs.

(i) "Tout nombre naturel est plus grand que -1." s'exprime $(\forall n \in \mathbb{N})\ n > -1$.

(ii) "Tout entier est la somme de deux entiers." peut s'écrire $(\forall a \in \mathbb{Z})(\exists b, c \in \mathbb{Z} \text{ tel que})\ b + c = a$.

(iii) "Il y a un plus petit nombre naturel." peut s'écrire $(\exists n \in \mathbb{N} \text{ tel que})(\forall m \in \mathbb{N})\ n \leq m$.

Exemples 3.3. (i) L'énoncé "$(\forall x \in \mathbb{Z})(\exists y \in \mathbb{N} \text{ tel que })\ x < y$" est vrai.

(ii) L'énoncé "$(\exists y \in \mathbb{N} \text{ tel que })(\forall x \in \mathbb{Z})\ x < y$" est faux.

(iii) L'énoncé "$(\forall x \in \mathbb{Z})\ x^2 \geq 0$" est vrai.

Les énoncés avec *pour tout* sont souvent écrit de la forme *si ..., alors*. Par exemple

$$(\forall x \in \mathbb{Z})\ x^2 \geq 0 \qquad \text{est équivalent à} \qquad \text{si } x \in \mathbb{Z}, \text{ alors } x^2 \geq 0.$$

Le symbole $\nexists$ veut dire *il n'existe pas*. Par exemple, l'énoncé

$$(\nexists a \in \mathbb{N} \text{ tel que})(\forall b \in \mathbb{N})\ a > b$$

veut dire qu'il n'existe pas de nombre naturel plus grand que tous les autres nombres naturels.

Unicité. Le symbole $\exists!$ veut dire *il existe un unique*. Par exemple, l'Axiome 1.4 et la Proposition 1.10 implique que

$$(\forall a \in \mathbb{Z})(\exists! b \in \mathbb{Z} \text{ tel que})\ a + b = 0.$$

Un énoncé de cette forme $(\exists! n \in \mathbb{N} \text{ tel que}) P(n)$ consiste en fait en deux énoncés:

- *existence*: $(\exists n \in \mathbb{N} \text{ tel que}) P(n)$, et
- *unicité*: $(\forall m, n \in \mathbb{N}).[(P(m) \text{ et } P(n)) \implies n = m]$.

Exercices.

3.1.1. Exprimez chacun des énoncés suivants avec des quantificateurs. (Notez qu'on n'affirme rien à l'égard de la vérité de ces énoncés; on ne fait que les traduire.)

(i) Il existe un plus grand entier.

(ii) Il existe un plus petit nombre naturel.

(iii) Chaque entier est la somme de deux entiers.

(iv) Tout entier est le carré d'un entier.

(v) L'équation $x^2 + 5y^3 = 4$ admet une solution entière unique (i.e. elle a une et seulement une solution lorsque x et y sont des entiers).

3.1.2. Pour chacun des énoncés suivants, déterminez s'il est vrai ou faux.

(i) $(\forall x \in \mathbb{Z})(\exists y \in \mathbb{Z}$ tel que$)$ $x + y = 2$

(ii) $(\forall x \in \mathbb{Z})(\exists y \in \mathbb{N}$ tel que$)$ $x + y = 2$

(iii) $(\exists x \in \mathbb{Z}$ tel que$)(\forall y \in \mathbb{Z})$ $x + y = 2$

(iv) $(\exists a \in \mathbb{Z}$ tel que$)(\forall b \in \mathbb{Z})$ $a + b = b$

(v) $(\forall b \in \mathbb{Z})(\exists a \in \mathbb{Z}$ tel que$)$ $a + b = b$

3.2 Implication

Le symbole $\implies$ veut dire *implique*. Si P et Q sont des énoncés, alors les formulations suivantes sont équivalentes:

- $P \implies Q$.
- P implique Q.
- Si P, alors Q.
- (non P) ou Q.

Remarque 3.4. Il est important de notez que si P est un énoncé faux, alors l'implication $P \implies Q$ est vrai. Cela découle du fait que "$P \implies Q$" est équivalent à "(non P) ou Q". Par exemple, l'énoncé

si 5 est un nombre pair, alors il y a de la vie sur Mars

est vrai (peu importe s'il y a de la vie sur Mars ou non), puisque l'énoncé "5 est un nombre pair" est faux.

Pour voir si l'implication $P \implies Q$ est équivalente à "(non P) ou Q", on peut comparer leurs *tables de vérités*.

P	Q	$P \implies Q$	(non P) ou Q
vrai	vrai	vrai	vrai
vrai	faux	faux	faux
faux	vrai	vrai	vrai
faux	faux	vrai	vrai

L'*implication double* est symbolisée par $\iff$ et veut dire *si et seulement si*. Si P et Q sont des énoncés, alors les énoncés suivants sont équivalents:

- $P \iff Q$.
- P si et seulement si Q.
- $(P \implies Q)$ et $(Q \implies P)$.
- Soit P et Q sont tous les deux faux, soit P et Q sont tous les deux vrais.
- (P et Q) ou ((non P) et (non Q)).

Exemples 3.5. Supposons que n est un entier.

(i) L'énoncé (n est divisible par 2 $\implies$ n est pair) est vrai.

(ii) L'énoncé (n est divisible par 4 $\iff$ n est pair) est faux.

Réciproque. La *réciproque* de l'implication $P \implies Q$ est l'implication $Q \implies P$. **Important:** Une implication et sa réciproque ne sont *pas* équivalents en général. Il est possible que l'un soit vrai, mais que l'autre ne le soit pas. (Il est également possible que les deux soient vraies, ou que les deux soient fausses.)

Exemple 3.6. L'énoncé

$$n \text{ est divisible par } 4 \implies n \text{ est pair}$$

est vrai. Mais sa réciproque :

$$n \text{ est pair} \implies n \text{ est divisible par } 4,$$

est fausse.

Contraposée. La *contraposée* d'une implication $P \implies Q$ est l'implication (non Q) $\implies$ (non P). Une implication et sa contraposée sont équivalents. C'est-à-dire

$$P \implies Q \qquad \text{est équivalent à} \qquad (\text{non } Q) \implies (\text{non } P).$$

Exemple 3.7. L'énoncé

$$n \text{ est divisible par } 4 \implies n \text{ est pair}$$

est équivalent à sa contraposée

$$n \text{ n'est pas pair} \implies n \text{ n'est pas divisible 4.}$$

Parfois, l'approche la plus simple pour démontrer un énoncé est de démontrer sa contraposée. Dans ce cas, on parle d'une *preuve par contraposée* ou *preuve indirecte*.

Exercices.

3.2.1. Donnez deux exemples d'énoncés mathématiques vrais dont la réciproque est fausse. (Ne donnez pas des exemples qu'on a déjà vus.)

3.2.2. Tentez de prouver à nouveau quelques-unes des propositions de la forme si-alors dans les Chapitres 1 et 2, mais avec une preuve par contraposée.

3.3 Négation

Si P est un énoncé, alors sa *négation* est l'énoncé (non P). Par exemple, la négation de (n est pair) est (n n'est pas pair). On écrira parfois $\neg P$ pour symboliser "non P".

Négation de "et" et "ou". La négation échange les "et" et "ou" de la manière suivante (parfois appelé *la loi de De Morgan*):

- La négation de "P ou Q" est équivalente à "$\neg P$ et $\neg Q$".
- La négation de "P et Q" est "$\neg P$ ou $\neg Q$".

Exemple 3.8. Supposons que P est une propriété qu'un entier pourrait avoir. Alors, l'énoncé "$\exists! n \in \mathbb{Z}$ avec la propriété P" est équivalent à

($\exists n \in \mathbb{Z}$ avec la proprété P) et (il y a au plus un entier avec la propriété P).

Sa négation est alors

(il n'y a pas de $n \in \mathbb{Z}$ avec la proprété P) ou (il y a plus d'un entier avec la proprété P).

Négation de l'implication. Puisque l'implication $P \implies Q$ est équivalent à "$\neg P$ ou Q", la négation de l'implication $P \implies Q$ est "P et $\neg Q$".

Négations avec des quantificateurs. Maintenant, supposons que l'on veut trouver la négation d'un énoncé incluant des quantificateurs $\forall$ et $\exists$, et écrit sous la forme de segments quantifiés et d'un énoncé final. Alors, pour déterminer sa négation, on suit la procédure suivante:

(i) On préserve l'ordre des segments quantifiés, mais on change tous les segments $(\forall \ldots)$ en des segments $(\exists \ldots$ tel que) correspondants.

(ii) Inversement, chaque segment $(\exists \ldots$ tel que) est substitué par un segment $(\forall \ldots)$ correspondant.

(iii) On applique finalement la négation à l'énoncé final.

Exemple 3.9. L'Axiome 1.2 peut s'écrire

$$(\exists b \in \mathbb{Z} \text{ tel que})(\forall a \in \mathbb{Z})\ a + b = a.$$

(On a remplacé la variable quantifiée 0 par b, ce qui ne change pas le signification de l'implication.) Sa négation est

$$(\forall b \in \mathbb{Z})(\exists a \in \mathbb{Z} \text{ tel que})\ a + b \neq a.$$

Exemples 3.10. (i) La négation de "toute fonction différentiable est continue" est "il existe une fonction différentiable qui n'est pas continue".

(ii) La négation de "aucune des publications de Paul sur Facebook n'est intéressante" est "il existe une publication de Paul sur Facebook qui est intéressante".

(iii) La négation de

$$(\forall \epsilon > 0)\ (\exists \delta > 0 \text{ tel que})\ (\forall x \in \mathbb{R})\ (|x - a| < \delta \implies |f(x) - f(a)| < \epsilon)$$

est

$$(\exists \epsilon > 0 \text{ tel que})\ (\forall \delta > 0)\ (\exists x \in \mathbb{R} \text{ tel que})\ (|x - a| < \delta \text{ et } |f(x) - f(a)| \geq \epsilon).$$

(Le premier énoncé est la définition de la continuité d'une fonction en un point a.)

Exercices.

3.3.1. Déterminez la négation des énoncés suivants.

(i) Tout polynôme admet une racine réelle.

(ii) Steve est blond et Samantha est grande.

(iii) $\forall x \in \mathbb{Z},\ \exists! y \in \mathbb{Z}$ tel que $xy = 3$.

(iv) Cette vache n'est ni immense ni rose.

(v) Si $f(x, y) > 0$, alors $x > 0$ ou $y \leq 0$.

(vi) Le groupe quotient G/N est fini si et seulement si G est fini.

(vii) Pour chaque $L \in \mathbb{N}$, il existe $N \in \mathbb{N}$ tel que $x_N > L$.

Chapitre 4

Séries finies et induction forte

Dans ce chapitre, nous allons introduire certaines notions mathématiques courantes telles que la notation de sommation, la notation de produit et les factorielles. On démontrera par la suite l'important Théorème du Binome et introduira une deuxième forme d'induction mathématique.

4.1 Préliminaires

Une *suite (infinie)* est une liste d'entiers x_j indexée par des *indices* $j \in \mathbb{N}$. On dénote une telle suite par $(x_j)_{j=1}^{\infty}$. (Plus tard, on verra qu'une suite est une fonction dont le domaine est $\mathbb{N}$. Voir l'exemple 5.20.) Il est possible que les indices ne commence pas à 1, mais à un autre entier quelconque m. Dans ce cas, on écrit $(x_j)_{j=m}^{\infty}$. Une *suite finie* $(x_j)_{j=m}^{M}$ est une liste de nombres

$$x_m, x_{m+1}, x_{m+2}, \ldots, x_{M-1}, x_M.$$

(Ici, $m, M \in \mathbb{Z}$ avec $m \leq M$.)

Exemple 4.1. Si on définit $x_j = j^2 - 5$, alors $x_1 = -4$, $x_2 = -1$, $x_3 = 4$, etc. Le nombre x_n est appelé le n-ième *terme* de la suite.

Certaines suites sont définies *récursivement*:

Exemple 4.2. Considérez la suite $(x_j)_{j=1}^{\infty}$ définie comme suit:

(i) Posons $x_1 = 1$.

(ii) Supposons que x_n est déjà défini, posons $x_{n+1} = 2x_n - 3$.

Alors, dans cette suite, on obtient $x_1 = 1$, $x_2 = -1$, $x_3 = -5$, $x_4 = -13$, etc.

Notez que la suite de l'exemple 4.1 est définie directement. Étant donné n'importe quel k, on peut calculer immédiatement x_k. Or, la suite de l'exemple 4.2 est définie récursivement. Afin de calculer le k-ième terme, on doit calculer tous ceux qui le précède.

Notation pour sommation et produit. Si $(x_j)_{j=m}^n$ est une suite finie d'entiers, on définit

$$\sum_{j=m}^{n} x_j = x_m + x_{m+1} + \cdots + x_n,$$

$$\prod_{j=m}^{n} x_j = x_m x_{m+1} \cdots x_n.$$

(Si $m = n$, on interprète comme suit: $\sum_{j=m}^m x_j = x_m$ et $\prod_{j=m}^m x_j = x_m$.)

On laisse

$$\mathbb{Z}_{\geq 0} := \{n \in \mathbb{Z} : n \geq 0\}$$

dénoté l'ensemble des entiers non négatifs..

Factorielle. Pour $n \in \mathbb{Z}_{\geq 0}$ on définit $n!$ (se lit "n factorielle") comme suit:

(i) On définit $0! := 1$.

(ii) Pour $n > 0$, on définit $n! = \prod_{j=1}^n j = 1 \cdot 2 \cdot \cdots \cdot n$.

Puissance. Fixons un entier b. On définit b^k pour tout $k \in \mathbb{Z}_{\geq 0}$ par récurrence comme suit:

(i) On définit $b^0 := 1$.

(ii) Pour $n > 0$, on définit $b^n = \underbrace{bb \cdots b}_{n \text{ termes}}$.

Notez qu'il s'ensuit de la définition ci-haut que $0^0 = 1$. Aussi, pour tout $a \in \mathbb{Z}$ et $m, k \in \mathbb{Z}_{\geq 0}$,

- $a^m a^k = a^{m+k}$.
- $(a^m)^k = a^{mk}$.

Exemple 4.3. Démontrons que $8^n - 3^n$ est divisible par 5 pour tout $n \in \mathbb{N}$. On effectue une preuve par induction. Posons

$$P(n) \quad \text{comme étant l'énoncé} \quad \text{"}8^n - 3^n \text{ est divisible par 5"}.$$

Puisque $8^1 - 3^1 = 8 - 3 = 5 = 5 \cdot 1$, on voit que $P(1)$ est vrai.

Maintenant, supposons que $P(n)$ est vrai pour un certain $n \in \mathbb{N}$. Donc, il existe $m \in \mathbb{Z}$ tel que $8^n - 3^n = 5m$. Alors

$$\begin{aligned} 8^{n+1} - 3^{n+1} &= 8^{n+1} - 3 \cdot 8^n + 3 \cdot 8^n - 3^{n+1} \\ &= 8 \cdot 8^n - 3 \cdot 8^n + 3 \cdot 8^n - 3 \cdot 3^n \\ &= (8 - 3) \cdot 8^n + 3 \cdot (8^n - 3^n) \\ &= 5 \cdot 8^n + 15m \\ &= 5 \cdot (8^n + 3m). \end{aligned}$$

Puisque $8^n + 3m \in \mathbb{Z}$, on voit que 5 divise $8^{n+1} - 3^{n+1}$.

Exercices.

4.1.1 ([BG10, Proj. 4.3]). Soit m un nombre naturel. Définissons la suite suivante:

(i) Posons $x_1 = m$.

(ii) Supposons que x_n soit déjà défini, posons

$$x_{n+1} = \begin{cases} \frac{x_n}{2} & \text{si } x_n \text{ est pair,} \\ x_n + 1 & \text{sinon.} \end{cases}$$

Cette suite atteint-elle éventuellement la valeur de 1, peu importe la valeur de $m \in \mathbb{N}$ avec laquelle on commence? Essayez de démontrer cette assertion.

4.1.2 ([BG10, Prop. 4.7]). Démontrez que, pour tout $k \in \mathbb{N}$:

(i) $5^{2k} - 1$ est divisible par 24;

(ii) $2^{2k+1} + 1$ est divisible par 3;

(iii) $10^k + 3 \cdot 4^{k+2} + 5$ est divisible par 9.

4.1.3 ([BG10, Prop. 4.8]). Démontrez que, pour tout $k \in \mathbb{N}$, $4^k > k$.

4.1.4 ([BG10, Proj. 4.9]). Déterminez pour quel nombre naturel k l'inégalité $k^2 < 2^k$ est vraie. Donnez une preuve justifiant votre réponse.

4.1.5. Définissons une suite $(x_n)_{n=1}^{\infty}$ récursivement comme suit:

$$x_1 = -4,$$
$$x_{n+1} = 3x_n - 8 \text{ pour } n \geq 1.$$

Démontrez que x_n est pair pour tout $n \in \mathbb{N}$.

4.2 Séries finies

On s'attardera maintenant à l'étude de quelques exemples de sommes pouvant être calculées explicitement, et on énoncera certaines propriétés utiles sur les sommes.

Rappelons que, si $a, b \in \mathbb{Z}$ et a divise b, alors il existe $c \in \mathbb{Z}$ tel que $ac = b$. On dénote c par $\frac{b}{a}$. Notez que cela implique que $\frac{b}{a}$ est un entier et que (pour l'instant) celui-ci est *seulement* défini lorsque a divise b. On n'a pas encore introduit le concept de nombre rationnel.

Proposition 4.4. *Soit $n \in \mathbb{N}$.*

(i) $\displaystyle\sum_{j=1}^{n} j = \frac{n(n+1)}{2}$.

(ii) $\displaystyle\sum_{j=1}^{n} j^2 = \frac{n(n+1)(2n+1)}{6}$.

Preuve. On démontre la première égalité, et on laisse la deuxième en exercice. On procède par induction sur n. Si $n = 1$, on a

$$\sum_{j=1}^{1} j = 1 = \frac{1(1+1)}{2},$$

ce qui établit le cas de base.

Maintenant, supposons que le résultat est vrai pour un certain $n \in \mathbb{N}$. Alors on a

$$\begin{aligned}
\sum_{j=1}^{n+1} j &= \left(\sum_{j=1}^{n} j\right) + (n+1) \\
&= \frac{n(n+1)}{2} + (n+1) \\
&= \frac{n(n+1) + 2(n+1)}{2} \\
&= \frac{n^2 + 3n + 2}{2} \\
&= \frac{(n+1)(n+2)}{2} \\
&= \frac{(n+1)\big((n+1)+1\big)}{2}.
\end{aligned}$$

Cela complète l'étape inductive de la preuve. □

Proposition 4.5. *Pour $x \in \mathbb{Z}$ avec $x \neq 1$, et $n \in \mathbb{Z}_{\geq 0}$, on a*

$$\sum_{j=0}^{n} x^j = \frac{1 - x^{n+1}}{1 - x}.$$

Preuve. Fixons $x \in \mathbb{Z}$, $x \neq 1$. On va montrer que

$$(1-x)\sum_{j=0}^{k} x^j = 1 - x^{k+1}$$

par induction sur $k \geq 0$. Le cas de base $k = 0$ énonce que

$$(1-x)\sum_{j=0}^{0} x^j = 1 - x,$$

lequel est vrai car $\sum_{j=0}^{0} x^j = x^0 = 1$.

Pour l'étape inductive, on suppose que le résultat est vrai pour un $k \in \mathbb{N}$. Ainsi, on suppose que $(1-x)\sum_{j=0}^{k} x^j = 1 - x^{k+1}$. Alors

$$\begin{aligned}(1-x)\sum_{j=0}^{k+1} x^j &= (1-x)\left(\sum_{j=0}^{k} x^j + x^{k+1}\right) \\ &= (1-x)\sum_{j=0}^{k} x^j + (1-x)x^{k+1} = 1 - x^{k+1} + x^{k+1} - x^{k+2} = 1 - x^{k+2},\end{aligned}$$

où l'on a employé l'hypothèse d'induction à l'avant-dernière étape. □

Les prochaines propositions énoncent des propriétés d'arithmétique utiles à l'égard des sommes.

Proposition 4.6. *(i) Soient $a \in \mathbb{Z}$ et $(x_j)_{j=m}^{M}$ une suite finie dans $\mathbb{Z}$. Alors*

$$a \cdot \left(\sum_{j=m}^{M} x_j\right) = \sum_{j=m}^{M} (a x_j).$$

(ii) Si $a \in \mathbb{Z}$, alors pour tout $n \in \mathbb{N}$,

$$\sum_{j=1}^{n} a = na.$$

En particulier, $\sum_{j=1}^{n} 1 = n$.

Preuve. La preuve de cette proposition est laissée en exercice (Exercice 4.2.4). □

Proposition 4.7. *Supposons que $a, b, c \in \mathbb{Z}$ satisfont $a \leq b < c$. De plus, supposons que $(x_j)_{j=a}^{c}$ et $(y_j)_{j=a}^{c}$ sont des suites finies dans $\mathbb{Z}$.*

(i) $\displaystyle\sum_{j=a}^{c} x_j = \sum_{j=a}^{b} x_j + \sum_{j=b+1}^{c} x_j.$

(ii) $\displaystyle\sum_{j=a}^{b} (x_j + y_j) = \sum_{j=a}^{b} x_j + \sum_{j=a}^{b} y_j.$

Preuve. La preuve de cette proposition est laissée en exercice (Exercice 4.2.5). □

La proposition suivante démontre comment on peut déplacer un indice de sommation sans altérer une somme.

Proposition 4.8. *Supposons que $(x_j)_{j=m}^{M}$ est une suite finie dans $\mathbb{Z}$ et que $r \in \mathbb{Z}$. Alors*

$$\sum_{j=m}^{M} x_j = \sum_{j=m+r}^{M+r} x_{j-r}.$$

Preuve. La preuve de cette proposition est laissée en exercice (Exercice 4.2.6). □

Proposition 4.9. *Supposons que* $(x_j)_{j=m}^M$ *et* $(y_j)_{j=m}^M$ *sont des suites finies dans* $\mathbb{Z}$ *telles que* $x_j \leq y_j$ *pour tout* $m \leq j \leq M$. *Alors*

$$\sum_{j=m}^{M} x_j \leq \sum_{k=m}^{M} y_j.$$

Preuve. Supposons que $(x_j)_{j=m}^M$ et $(y_j)_{j=m}^M$ sont des suites finies dans $\mathbb{Z}$ telles que $x_j \leq y_j$ pour tout $m \leq j \leq M$. Pour $m \leq k \leq M$, on pose $P(k)$ comme étant l'énoncé

$$\sum_{j=m}^{k} x_j \leq \sum_{k=m}^{k} y_j.$$

On va démontrer par induction que $P(k)$ est vrai pour tout k avec $m \leq k \leq M$.

Premièrement, notons que $P(m)$ est l'énoncé $x_m \leq y_m$, lequel est vrai par hypothèse. Maintenant, supposons que $P(k)$ est vrai pour un certain $m \leq k < M$. Alors

$$\sum_{j=1}^{k+1} x_j = \sum_{j=1}^{k} x_j + x_{k+1} \leq \sum_{j=1}^{k} y_j + y_{k+1} = \sum_{j=1}^{j+1} y_{k+1}.$$

Cela complète la preuve de l'étape inductive. □

Exercices.

4.2.1 ([BG10, Proj. 4.12]). Trouvez une formule pour $\sum_{j=1}^{k} j^3$ et démontrez l'égalité en question.

4.2.2. Démontrez par induction que

$$\sum_{i=1}^{k}(3i-2) = \frac{k(3k-1)}{2} \quad \text{pour tout } k \in \mathbb{N}.$$

4.2.3. Démontrez par induction que

$$\sum_{k=3}^{n} \frac{2}{k^2-3k+2} = \frac{2n-4}{n-1} \quad \text{pour tout } n \in \mathbb{Z},\ n \geq 3.$$

(Strictement parlant, cette question emploie des nombres rationnels, que l'on a pas encore vus. Mais vous pouvez faire de l'arithmétique avec eux au sens habituel, comme dans vos cours précédents de mathématique.)

4.2.4. Démontrez la Proposition 4.6.

4.2.5. Démontrez la Proposition 4.7.

4.2.6. Démontrez la Proposition 4.8.

4.3 Le Théorème du Binôme

Théorème 4.10. *Supposons que $k, m \in \mathbb{Z}_{\geq 0}$, avec $m \leq k$. Alors $k!$ est divisible par $m!(k-m)!$.*

Preuve. On démontre ce résultat par induction. Toutefois, étant donné que l'énoncé comporte deux paramètres, il faut faire attention à la manière dont on entreprend l'induction. Pour chaque $k \in \mathbb{Z}_{\geq 0}$, on pose $P(k)$ comme étant l'énoncé

$$\text{pour tout } 0 \leq m \leq k,\ k! \text{ est divisible par } m!(k-m)!.$$

Ensuite, pour prouver le théorème, il suffit de montrer que $P(k)$ est vrai pour tout $k \in \mathbb{Z}_{\geq 0}$. On procède par induction sur k pour faire cela.

Le cas de base correspond à $k = 0$. Sous cette condition $0 \leq m \leq k$ force $m = 0$, et il suffit d'observer que $k! = 0! = 1$ est divisible par $m!(k-m)! = 0!0! = 1 \cdot 1 = 1$.

Maintenant, supposons que $P(n)$ est vrai pour un certain $n \in \mathbb{N}$. On doit montrer que $P(n+1)$ est vrai. Si $m = 0$, alors $m!(n+1-m)! = 0!(n+1)! = (n+1)!$, lequel divise clairement $(n+1)!$. De manière similaire, si $m = n+1$, alors $m!(n+1-m)! = (n+1)!0! = (n+1)!$, lequel divise $(n+1)!$. Donc, il reste à vérifier les autres cas avec $1 \leq m \leq n$.

Fixons m tel que $1 \leq m \leq n$. On a supposé que $P(n)$ est vrai, donc, pour les cas $m-1$ et m, $P(n)$ nous dit qu'il existe des entiers a et b tels que

$$n! = a(m-1)!(n-m+1)! \quad \text{et} \quad n! = b(m!)(n-m)!.$$

Alors

$$\begin{aligned}(n+1)! &= n!(n+1)\\ &= n!(m+n+1-m)\\ &= n!m + n!(n+1-m)\\ &= a(m-1)!(n-m+1)!m + b(m!)(n-m)!(n+1-m)\\ &= (a+b)(m!)(n-m+1)!,\end{aligned}$$

ce qui implique que $m!(n+1-m)!$ divise $(n+1)!$, complétant ainsi la preuve de l'étape inductive. □

Par le Théorème 4.10, $\frac{k!}{m!(k-m)!}$ est un entier pour tout choix d'entiers $0 \leq m \leq k$. On définit

$$\binom{k}{m} = \frac{k!}{m!(k-m)!},$$

que l'on lit "m parmi k" (étant donné que l'on peut démontrer qu'il correspond au nombre de façon dont on peut choisir m objets parmi une collection de k objets) et que l'on appelle le *coefficient binomial*.

Corollaire 4.11. *Pour $1 \leq m \leq n$, on a*

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

Preuve. Dans la preuve du Théorème 4.10, on a obtenu l'égalité

$$(n+1)! = n!m + n!(n+1-m).$$

En divisant chaque côté par $m!(n+1-m)!$, on obtient

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

ce qui correspond précisément au corollaire. (Notez que, même si l'on n'a pas encore abordé la division, les étapes ci-haut sont justifiées car le Théorème 4.10 nous garantit que les fractions données sont des entiers. Ainsi, on ne fait qu'employer les propriétés de divisibilité des entiers.) □

Le corollaire 4.11 énonce que les coefficients binomiaux peuvent être obtenus à partir du *triangle de Pascal*.

$$\begin{array}{ccccccccccccc} & & & & & & 1 & & & & & & \\ & & & & & 1 & & 1 & & & & & \\ & & & & 1 & & 2 & & 1 & & & & \\ & & & 1 & & 3 & & 3 & & 1 & & & \\ & & 1 & & 4 & & 6 & & 4 & & 1 & & \\ & 1 & & 5 & & 10 & & 10 & & 5 & & 1 & \\ 1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1 \\ & & & & & & \vdots & & & & & & \end{array}$$

Si on énumère les rangées en partant du haut, en commençant à zéro, alors la m-ième entrée dans la k-ième rangée est égale à $\binom{k}{m}$. Chaque entrée qui ne figure pas sur les bords du triangle est la somme de ces deux voisins dans la rangée juste au-dessus. Vous avez peut-être appris au secondaire que

$$\begin{aligned} (a+b)^2 &= a^2 + 2ab + b^2, \\ (a+b)^3 &= a^3 + 3a^2b + 3ab^2 + b^3. \end{aligned}$$

Voici la forme général, nous permettant d'écrire une formule similaire pour un exposant (non négatif) arbitraire.

Théorème 4.12 (Théorème du Binôme pour les entiers)**.** *Si $a, b \in \mathbb{Z}$ et $k \in \mathbb{Z}_{\geq 0}$, alors*

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

Preuve. On démontre ce résultat par induction sur k. Pour le cas de base, on a

$$(a+b)^0 = 1 = \binom{0}{0} a^0 b^0.$$

Maintenant, supposons que, pour un certain $n \in \mathbb{Z}_{\geq 0}$, on a que

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

Alors

$$\begin{aligned}
&\sum_{m=0}^{n+1} \binom{n+1}{m} a^m b^{n+1-m} \\
&\quad = \binom{n+1}{0} a^0 b^{n+1} + \sum_{m=1}^{n} \binom{n+1}{m} a^m b^{n+1-m} + \binom{n+1}{n+1} a^{n+1} b^0 && \text{(Prop. 4.7(i))} \\
&\quad = b^{n+1} + \sum_{m=1}^{n} \left(\binom{n}{m-1} + \binom{n}{m} \right) a^m b^{n+1-m} + a^{n+1} && \text{(Cor. 4.11)} \\
&\quad = b^{n+1} + \sum_{m=1}^{n} \binom{n}{m-1} a^m b^{n+1-m} + \sum_{m=1}^{n} \binom{n}{m} a^m b^{n+1-m} + a^{n+1} && \text{(Prop. 4.7(ii))} \\
&\quad = b^{n+1} + \sum_{m=0}^{n-1} \binom{n}{m} a^{m+1} b^{n+1-(m+1)} + \sum_{m=1}^{n} \binom{n}{m} a^m b^{n+1-m} + a^{n+1} && \text{(Prop. 4.8 avec } r=1) \\
&\quad = \sum_{m=0}^{n} \binom{n}{m} a^{m+1} b^{n+1-(m+1)} + \sum_{m=0}^{n} \binom{n}{m} a^m b^{n+1-m} && \text{(Prop. 4.7(i))} \\
&\quad = a \sum_{m=0}^{n} \binom{n}{m} a^m b^{n-m} + b \sum_{m=0}^{n} \binom{n}{m} a^m b^{n-m} && \text{(Prop. 4.6(i))} \\
&\quad = a(a+b)^n + b(a+b)^n && \text{(par l'hyp. d'induction)} \\
&\quad = (a+b)^{n+1},
\end{aligned}$$

complétant ainsi la preuve de l'étape inductive. □

Le Théorème 4.12 justifie l'emploi du terme *coefficient binomial*, puisque les entiers $\binom{k}{m}$ donnent les *coefficients* pour le développement de la puissance d'un *binôme*.

Corollaire 4.13. *Pour $k \in \mathbb{Z}_{\geq 0}$, on a*

$$\sum_{m=0}^{k} \binom{k}{m} = 2^k.$$

Preuve. Il suffit de prendre $a = b = 1$ et d'appliquer le Théorème 4.12. □

Exercices.

4.3.1 (Formule de Leibniz [BG10, Proj. 4.23]). Considérez une opération dénotée par $'$ appliqué à des fonctions (dénotées u, v, w). Supposons que l'opérateur satisfait les axiomes suivants:

$$\begin{aligned}(u+v)' &= u'+v',\\ (uv)' &= uv'+u'v,\\ (cu)' &= cu', \text{ où } c \text{ est une constante.}\end{aligned}$$

Définissons $w^{(k)}$ récursivement par

(i) $w^{(0)} = w$.

(ii) Supposons que $w^{(n)}$ est défini (où $n \in \mathbb{Z}_{\geq 0}$), posons $w^{(n+1)} = \left(w^{(n)}\right)'$.

Démontrez que

$$(uv)^{(k)} = \sum_{m=0}^{k} \binom{k}{m} u^{(m)} v^{(k-m)}.$$

(Bien sûr, vous connaissez déjà une opération avec ces propriétés, soit la dérivée. Toutefois, aucun calcul infinitésimal n'est requis pour démontrer l'énoncé ci-haut.

4.4 Induction forte

Il y a une deuxième forme d'induction, parfois appelée l'*induction forte*.

Théorème 4.14 (Principe de l'induction mathématique—deuxième forme)**.** *Pour chaque $k \in \mathbb{N}$, soit $P(k)$ un énoncé. Supposons que*

(i) $P(1)$ est vrai, et

(ii) pour tout $n \in \mathbb{N}$, si $P(j)$ est vrai pour tout entier j tel que $1 \leq j \leq n$, alors $P(n+1)$ est vrai.

Alors $P(k)$ est vrai pour tout $k \in \mathbb{N}$.

Preuve. Cela peut être démontré avec les énoncés $Q(k) :=$"$P(j)$ est vrai pour tout entier j tel que $1 \leq j \leq k$" en procédant par induction sur k (avec la première forme d'induction). On laisse les détails de la preuve en exercice (Exercice 4.4.1). □

Notez la différence entre le Théorème 4.14 et le Théorème 2.19. Dans le Théorème 2.19, on suppose seulement que $P(n)$ est vrai lors de l'étape inductive. Tandis que dans le Théorème 4.14, on suppose que tous les $P(j)$ pour $1 \leq j \leq n$ sont vrais. Bien entendu, on peut démarrer l'induction sur n'importe quel entier (pas seulement à 1).

Les *nombres de Fibonacci* $(f_j)_{j=1}^{\infty}$ se définissent par

$$f_1 = 1, \qquad f_2 = 1, \qquad \text{et}$$
$$f_n = f_{n-1} + f_{n-2} \qquad \text{pour } n \geq 3.$$

En employant l'induction forte, on peut obtenir une formule explicite pour les nombres de Fibonacci—en permettant de calculer le n-ième nombre de Fibonacci directement, sans le calculer récursivement. La formule inclue des nombres irrationnels, que nous allons discuter plus en détail plus tard. Toutefois, puisqu'il s'agit d'un exemple classique, on va supposer pour l'instant que l'on connait les nombres irrationnels.

Proposition 4.15. *Pour $k \in \mathbb{N}$, on a*

$$f_k = \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^k - \left(\frac{1-\sqrt{5}}{2} \right)^k \right). \tag{4.1}$$

Preuve. Posons

$$a = \frac{1+\sqrt{5}}{2} \qquad \text{et} \qquad b = \frac{1-\sqrt{5}}{2}.$$

Puisque la formule récursive pour les nombres de Fibonacci n'est que valide à partir de $n \geq 3$, on doit vérifier deux cas de base. On laisse en exercice la vérification que (4.1) donne bien $f_1 = 1$ et $f_2 = 1$, tel que souhaité.

Maintenant, fixons un $n \geq 2$ et supposons que la formule (4.1) est vraie pour tout $1 \leq k \leq n$. Il nous faudra les calculs suivants

$$a + 1 = \frac{3+\sqrt{5}}{2} = \frac{1+2\sqrt{5}+5}{4} = a^2,$$
$$b + 1 = \frac{3-\sqrt{5}}{2} = \frac{1-2\sqrt{5}+5}{4} = b^2.$$

Puis, on obtient

$$\begin{aligned} f_{n+1} &= f_n + f_{n-1} \\ &= \frac{1}{\sqrt{5}}(a^n - b^n) + \frac{1}{\sqrt{5}}(a^{n-1} - b^{n-1}) \\ &= \frac{1}{\sqrt{5}}(a^n + a^{n-1} - b^n - b^{n-1}) \\ &= \frac{1}{\sqrt{5}}(a^{n-1}(a+1) - b^{n-1}(b+1)) \\ &= \frac{1}{\sqrt{5}}(a^{n-1}a^2 - b^{n-1}b^2) \\ &= \frac{1}{\sqrt{5}}(a^{n+1} - b^{n+1}), \end{aligned}$$

complétant la preuve de l'étape inductive. □

Exercices.

4.4.1. Démontrez le Théorème 4.14.

4.4.2 ([BG10, Proj. 4.26]). Supposons qu'une suite $(x_j)_{j=0}^{\infty}$ satisfait

$$x_1 = 1, \quad \text{et pour tout } m \geq n \geq 0, \quad x_{m+n} + x_{m-n} = \frac{1}{2}(x_{2m} + x_{2n}).$$

Trouvez une formule pour x_j. Démontrez que la formule est correcte.

4.4.3 ([BG10, Prop. 4.30]). Démontrez que, pour tout $k, m \in \mathbb{N}$, où $m \geq 2$, on a

$$f_{m+k} = f_{m-1}f_k + f_m f_{k+1}.$$

4.4.4 ([BG10, Prop. 4.31]). Démontrez que, pour tout $k \in \mathbb{N}$, on a

$$f_{2k+1} = f_k^2 + f_{k+1}^2.$$

4.4.5 ([BG10, Prop. 4.32]). Démontrez que, pour tout $k, m \in \mathbb{N}$, f_{mk} est divisible par f_m.

4.4.6 ([BG10, Proj. 4.33]). De combien de façons peut-on ordonner les nombres $1, 2, \ldots, 20$ en une rangée de telle manière que le premier nombre soit 1, le dernier nombre 20, et que chaque paire de nombres consécutifs diffèrent par au plus 2?

Chapitre 5

Théorie naïve des ensembles

Dans cette section, on aborde certains concepts de base importants dans la théorie des ensembles. Puisque tout en mathématique est, d'une certaine façon, construit à partir d'ensembles, la notion d'ensemble est fondamentale.

5.1 Sous-ensemble et égalité

Comme nous l'avons déjà mentionné, un *ensemble* est une collection de choses, appelées ses *éléments* ou *membres*. On écrit $x \in A$ pour indiquer que x est un membre de l'ensemble A et on écrit $x \notin A$ (défini à travers $\neg(x \in A)$) pour indiquer que x n'est pas un membre de l'ensemble A.

Il est important de comprendre que pour chaque x, les seules options sont $x \in A$ et $x \notin A$. En particulier, un objet ne peut pas faire partie d'un ensemble plus d'une fois et l'ordre des éléments est sans importance. Par exemple, les ensembles

$$\{2, 2, 3\} \qquad \text{et} \qquad \{2, 3\} \qquad \text{et} \qquad \{3, 2\}$$

sont égaux. Ils contiennent tous les trois les nombres naturels 2 et 3, et rien d'autre.

Dans la Section 2.2, on a introduit les symboles $\subseteq$, $\subsetneq$, et $\not\subseteq$. En particulier,

$$(A \subseteq B) \qquad \text{si et seulement si} \qquad \forall x.(x \in A \implies x \in B).$$

On va parfois aussi écrire $B \supseteq A$ pour signifier que $A \subseteq B$.

Proposition 5.1. *Supposons que A, B et C sont des ensembles.*

(i) $A \subseteq A$. (L'inclusion d'ensemble est réflexive.)

(ii) Si $A \subseteq B$ et $B \subseteq C$, alors $A \subseteq C$. (L'inclusion d'ensemble est transitive.)

Preuve. (i) Étant donné que $x \in A \implies x \in A$ est clairement vrai, alors on a $A \subseteq A$.

(ii) Supposons que $A \subseteq B$ et $B \subseteq C$. On veut montrer que $\forall x.(x \in A \implies x \in C)$. Prenons un x arbitraire. On a

$$x \in A \implies x \in B \qquad \text{(puisque } A \subseteq B\text{)}$$

$$\implies x \in C. \qquad \text{(puisque } B \subseteq C\text{)}$$

Donc, $\forall x.(x \in A \implies x \in C)$ est vrai, i.e. $A \subseteq C$. □

On a également discuté de la notion d'égalité d'ensembles à la Section 2.2. En particulier, les énoncés suivants sont équivalents pour deux ensembles A et B:

- $A = B$.
- $\forall x.(x \in A \iff x \in B)$.
- $A \subseteq B$ et $B \subseteq A$.

Exemple 5.2. Définissons

$$A = \{3n + 1 : n \in \mathbb{Z}\} \qquad \text{et} \qquad B = \{3m + 10 : m \in \mathbb{Z}\}.$$

On va démontrer que $A = B$. Pour ce faire, on va démontrer $A \subseteq B$ et $B \subseteq A$ séparément.

Premièrement, démontrons que $A \subseteq B$. Soit $x \in A$. Alors, il existe $n \in \mathbb{Z}$ tel que $x = 3n + 1$. Ainsi

$$x = 3n + 1 = 3n - 9 + 10 = 3(n - 3) + 10.$$

Puis, si on prend $m = n - 3$, on a $m \in \mathbb{Z}$ et $x = 3m + 10$. Donc $x \in B$. Cela complète la preuve que $\forall x.(x \in A \implies x \in B)$, c'est-à-dire que $A \subseteq B$.

Maintenant, démontrons que $B \subseteq A$. Soit $x \in B$. Alors, il existe $m \in \mathbb{Z}$ tel que $x = 3m + 10$. Donc

$$x = 3m + 10 = 3m + 9 + 1 = 3(m + 3) + 1.$$

Puis, en prenant $n = m + 3$, on obtient $n \in \mathbb{Z}$ et $x = 3n + 1$. Donc $x \in A$. Cela complète la preuve que $\forall x.(x \in B \implies x \in A)$, c'est-à-dire que $B \subseteq A$.

Proposition 5.3. *Supposons que A, B et C sont des ensembles.*

(i) $A = A$. *(L'égalité d'ensemble est réflexive.)*

(ii) Si $A = B$, *alors* $B = A$. *(L'égalité d'ensemble est symétrique.)*

(iii) Si $A = B$ *et* $B = C$, *alors* $A = C$. *(L'égalité d'ensemble est transitive.)*

Preuve. La preuve de cette proposition est laissée en exercice (Exercice 5.1.2). □

L'*ensemble vide*, dénoté $\varnothing$, est l'ensemble qui ne contient aucun élément. C'est-à-dire que, c'est l'ensemble pour lequel $x \in \varnothing$ est toujours faux, peu importe le x (i.e. $\forall x.x \notin \varnothing$). La proposition suivante affirme qu'il existe un seul ensemble vide.

Proposition 5.4. *Supposons que $\varnothing_1$ et $\varnothing_2$ ont la propriété que $x \in \varnothing_1$ n'est jamais vrai et que $x \in \varnothing_2$ n'est jamais vrai. Dans ce cas, $\varnothing_1 = \varnothing_2$.*

Preuve. Supposons que $\varnothing_1$ et $\varnothing_2$ admettent la propriété en question. On va démontrer que $\varnothing_1 = \varnothing_2$ par contradiction. Puisque l'énoncé "$\varnothing_1 = \varnothing_2$" est équivalent à

$$\varnothing_1 \subseteq \varnothing_2 \qquad \text{et} \qquad \varnothing_2 \subseteq \varnothing_1,$$

la négation est

$$\varnothing_1 \not\subseteq \varnothing_2 \qquad \text{ou} \qquad \varnothing_1 \not\subseteq \varnothing_1.$$

Mais si $\varnothing_1 \not\subseteq \varnothing_2$, alors il existe un $x \in \varnothing_1$ tel que $x \notin \varnothing_2$. Mais cela contredit la supposition que $x \in \varnothing_1$ n'est jamais vrai. Dans l'autre cas, $\varnothing_2 \not\subseteq \varnothing_1$ mène à une contradiction similaire. □

Proposition 5.5. *L'ensemble vide est un sous-ensemble de tout ensemble. C'est-à-dire, pour tout ensemble S, on a $\varnothing \subseteq S$.*

Preuve. Soit S un ensemble. Alors, l'inclusion $\varnothing \subseteq S$ est équivalente à l'implication

$$\forall x.(x \in \varnothing \implies x \in S),$$

laquelle est vraie, car l'hypothèse est toujours fausse. (Voir la remarque 3.4.) □

Exercices.

5.1.1 ([BG10, Proj. 5.3]). Considérez les ensembles suivants:

$$\begin{aligned} A &= \{3x : x \in \mathbb{N}\}, \\ B &= \{3x + 21 : x \in \mathbb{N}\}, \\ C &= \{x + 7 : x \in \mathbb{N}\}, \\ D &= \{3x : x \in \mathbb{N} \text{ et } x > 7\}, \\ E &= \{x : x \in \mathbb{N}\}, \\ F &= \{3x - 21 : x \in \mathbb{N}\}, \\ G &= \{x : x \in \mathbb{N} \text{ et } x > 7\}. \end{aligned}$$

Déterminez, parmi les égalités suivantes, lesquelles sont vraies. Si un énoncé est vrai, démontrez-le. Sinon, expliquez pourquoi l'égalité ne tient pas. (L'exercice n'emploie pas tous les ensembles spécifiés ci-haut; ces derniers joueront un rôle dans l'exercice 5.2.1.)

(i) $D = E$.

(ii) $C = G$.

(iii) $D = B$.

5.1.2. Démontrez la Proposition 5.3.

5.1.3 ([BG10, Proj. 5.5]). Les égalités suivantes sont-elles vraies?

(i) $S = \{m : m \in \mathbb{N}\}$ et $T_m = \{m\}$ pour un $m \in \mathbb{N}$ spécifique.

(ii) $U = \{my : y \in \mathbb{Z},\ m \in \mathbb{N},\ my > 0\}$ et $V_m = \{my : y \in \mathbb{Z},\ my > 0\}$ pour un $m \in \mathbb{N}$ spécifique.

(iii) V_m et $W_m = \{my : y \in \mathbb{Z},\ y > 0\}$ pour un $m \in \mathbb{N}$ spécifique.

Déterminez la manière la plus simple de spécifier chacun de ces ensembles.

5.2 Intersections et unions

L'*intersection* de deux ensembles A et B est

$$A \cap B = \{x : x \in A \text{ et } x \in B\}.$$

En d'autres mots,

$$\forall x.[(x \in A \cap B) \iff (x \in A \text{ et } x \in B)].$$

Si $A \cap B = \varnothing$, on dit que A et B sont *disjoints*.

L'*union* de A et B est

$$A \cup B = \{x : x \in A \text{ ou } x \in B\}.$$

En d'autres mots,

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

Exemples 5.6. (i) $\{1, 2, 5\} \cup \{2, 8, 9\} = \{1, 2, 5, 8, 9\}$ et $\{1, 2, 5\} \cap \{2, 8, 9\} = \{2\}$.

(ii) $\{-n : n \in \mathbb{Z},\ n \geq 0\} \cup \mathbb{N} = \mathbb{Z}$.

(iii) $\{n \in \mathbb{N} : n \text{ est pair }\} \cap \{n \in \mathbb{N} : n \text{ est divisible par } 4\} = \{n \in \mathbb{N} : n \text{ est divisible par } 4\}$

(iv) Si $A = \{2n : n \in \mathbb{Z}\}$ et $B = \{2n + 1 : n \in \mathbb{Z}\}$, alors $A \cup B = \mathbb{Z}$ et $A \cap B = \varnothing$. En particulier, A et B sont disjoints.

(v) $\{n \in \mathbb{Z} \colon n \geq 3\} \cap \{n \in \mathbb{Z} \colon n \text{ est pair}\} = \{2n \colon n \in \mathbb{N},\ n \geq 2\}$.

Si A et B sont des ensembles, alors la *différence* de A par B est

$$A - B = \{x \colon x \in A \text{ et } x \notin B\}.$$

La différence d'ensemble s'écrit parfois $A \setminus B$. La *différence symétrique* de A et B est

$$A \Delta B = (A - B) \cup (B - A).$$

Il est clair que, selon cette définition, $A \Delta B = B \Delta A$, d'où son nom de différence *symétrique*. (Notez que $A - B$ n'est pas égal à $B - A$ en général.)

Si $A \subseteq X$, alors le *complément* de A dans X est $X - A$. Si l'ensemble plus grand X est clair dans le contexte, alors on écrit parfois $A^{\complement}$ pour désigner le complément de A dans X. Toutefois, il faut noter que la notation $A^{\complement}$ n'a pas de sens si on n'a pas de X à l'esprit.

Exemples 5.7. (i) Un entier est dit *impair* s'il n'est pas pair. Ainsi, l'ensemble des entiers impairs est le complément dans $\mathbb{Z}$ de l'ensemble des entiers pairs:

$$\mathbb{Z} - \{n \in \mathbb{Z} : n \text{ est pair}\} = \{n \in \mathbb{Z} : n \text{ est impair}\}.$$

(ii) $\mathbb{Z} - \mathbb{N} = \{n \in \mathbb{Z} : n \leq 0\}$ et $\mathbb{N} - \mathbb{Z} = \varnothing$.

(iii) $\{n \in \mathbb{Z} : n \leq 0\} \Delta \{n \in \mathbb{Z} : n \geq 0\} = \{n \in \mathbb{Z} : n \neq 0\}$.

Proposition 5.8. *Soient $A, B \subseteq X$. Alors*

$$A \subseteq B \iff B^{\complement} \subseteq A^{\complement}.$$

Preuve. Soient $A \subseteq B$ (dans X). Alors pour tout $x \in X$,

$$\begin{aligned} x \in B^{\complement} &\iff (x \in X) \text{ et } (x \notin B) \\ &\implies (x \in X) \text{ et } (x \notin A) \qquad \text{(puisque } x \in A \text{ impliquerait } x \in B) \\ &\iff x \in A^{\complement}. \end{aligned}$$

Donc $B^{\complement} \subseteq A^{\complement}$.

Pour prouver l'implication inverse, notons tout d'abord que, pour tout $Y \subseteq X$, on a $\left(Y^{\complement}\right)^{\complement} = Y$ (Exercice 5.2.3). Puis, on peut appliquer ce qu'on vient de démontrer pour obtenir

$$B^{\complement} \subseteq A^{\complement} \implies \left(A^{\complement}\right)^{\complement} \subseteq \left(B^{\complement}\right)^{\complement} \implies A \subseteq B. \qquad \square$$

Théorème 5.9 (Loi de De Morgan (pour ensembles))**.** *Soient $A, B \subseteq X$.*

(i) $(A \cap B)^{\complement} = A^{\complement} \cup B^{\complement}$.

(ii) $(A \cup B)^{\complement} = A^{\complement} \cap B^{\complement}$.

Preuve. On démontre (ii) et on laisse la preuve de (i) en exercice (Exercice 5.2.4). Pour $x \in X$, on a

$$\begin{aligned} & x \in (A \cup B)^{\complement} \\ \iff & \neg(x \in A \cup B) \\ \iff & \neg(x \in A \text{ ou } x \in B) \\ \iff & x \notin A \text{ et } x \notin B \\ \iff & x \in A^{\complement} \text{ et } x \in B^{\complement} \\ \iff & x \in A^{\complement} \cap B^{\complement}. \end{aligned}$$

Donc $x \in (A \cup B)^{\complement} \iff x \in A^{\complement} \cap B^{\complement}$. Ainsi, $(A \cup B)^{\complement} = A^{\complement} \cap B^{\complement}$. $\square$

Si A, B et C sont des ensembles, nous avons

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

(On laisse la vérification en exercice.) En d'autres mots, les opérations d'union et d'intersection sont associatives. Il s'ensuit que, comme pour l'addition (voir remarque 1.29), on peut écrire sans ambiguïté des expressions comme

$$A \cup B \cup C \cup D \quad \text{et} \quad A \cap B \cap C \cap D,$$

car le résultat est le même, peu importe comment on regroupe les termes.

En fait, on peut même former des unions et intersections arbitraires. Si I est un certain ensemble (que l'on emploie à titre d'*index*) et, pour tout $i \in I$, A_i est un ensemble. Alors on définit

$$\bigcup_{i \in I} A_i = \{x : x \in A_i \text{ pour un } i \in I\} \quad \text{et} \quad \bigcap_{i \in I} A_i = \{x : x \in A_i \text{ pour tout } i \in I\}.$$

Exemple 5.10. (i) Pour $i \in \mathbb{Z}$, posons $A_i = \{n : n \in \mathbb{Z},\ n \geq i\}$. Alors

$$\bigcap_{i \in \mathbb{Z}} A_i = \varnothing, \qquad \bigcup_{i \in \mathbb{Z}} A_i = \mathbb{Z}.$$

(ii) On a

$$\bigcap_{m \in \mathbb{N}} \{n : n \in \mathbb{N},\ n \leq m\} = \{1\}, \qquad \bigcup_{m \in \mathbb{N}} \{n : n \in \mathbb{N},\ n \leq m\} = \mathbb{N}$$

Un cas particulier des unions et intersections arbitraires définies ci-haut est lorsque nous avons un nombre fini d'ensembles $A_1, A_2, \ldots, A_k$ pour un certain $k \in \mathbb{N}$. Alors

$$\bigcup_{i=1}^{k} A_i = \{x : x \in A_i \text{ pour un } i \in \{1, 2, \ldots, k\}\} \quad \text{et}$$

$$\bigcap_{i=1}^{k} A_i = \{x : x \in A_i \text{ pour tout } i \in \{1, 2, \ldots, k\}\}.$$

L'union et l'intersection sont également commutatives:

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

On a même une forme de distributivité pour l'union et l'intersection. Notre preuve de ces propriétés fera appel aux équivalences logiques suivantes: Si P, Q et R sont des énoncés, alors

$$P \text{ et } (Q \text{ ou } R) \iff (P \text{ et } Q) \text{ ou } (P \text{ et } R)$$

et

$$P \text{ ou } (Q \text{ et } R) \iff (P \text{ ou } Q) \text{ et } (P \text{ ou } R).$$

En d'autres mots, le *et* se distribue sur le *ou*, et vice-versa, le *ou* se distribue sur le *et*.

Proposition 5.11. *Soient A, B et C des ensembles. Alors*

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

Preuve. On a

$$\begin{aligned} & x \in C \cap (A \cup B) \\ \iff & x \in C \text{ et } x \in A \cup B \\ \iff & x \in C \text{ et } (x \in A \text{ ou } x \in B) \\ \iff & (x \in C \text{ et } x \in A) \text{ ou } (x \in C \text{ et } x \in B) \\ \iff & x \in C \cap A \text{ ou } x \in C \cap B \\ \iff & x \in (C \cap A) \cup (C \cap B). \end{aligned}$$

□

Proposition 5.12. *Soient A, B et C des ensembles. Alors*

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

Preuve. On a

$$\begin{aligned} & x \in C \cup (A \cap B) \\ \iff & x \in C \text{ ou } x \in A \cap B \\ \iff & x \in C \text{ ou } (x \in A \text{ et } x \in B) \\ \iff & (x \in C \text{ ou } x \in A) \text{ et } (x \in C \text{ ou } x \in B) \\ \iff & (x \in C \cup A) \text{ et} (x \in C \cup B) \\ \iff & x \in (C \cup A) \cap (C \cup B). \end{aligned}$$

□

La Proposition 5.11 énonce que l'intersection se distribue sur l'union, tandis que la Proposition 5.12 énonce que l'union se distribue sur l'intersection.

Exemple 5.13. Posons

$$A = \{1, 2, 4, 5\}, \quad B = \{2, 3, 5, 6\}, \quad C = \{4, 5, 6, 7\}.$$

Alors

$$C \cup (A \cap B) = \{4, 5, 6, 7\} \cup \{2, 5\} = \{2, 4, 5, 6, 7\},$$

mais

$$(C \cup A) \cap (C \cup B) = \{1, 2, 4, 5, 6, 7\} \cap \{2, 3, 4, 5, 6, 7\} = \{2, 4, 5, 6, 7\}.$$

Donc on a bien $C \cup (A \cap B) = (C \cup A) \cap (C \cup B)$.

Exercices.

5.2.1 ([BG10, Proj. 5.11]). Considérez les ensembles de l'exercise 5.1.1. Déterminez quelles égalités parmi les suivantes sont vraies. Si un énoncé est vrai, prouvez-le. Sinon, expliquez pourquoi l'égalité ne tient pas.

(i) $A \cap E = B$.

(ii) $A \cap C = B$.

(iii) $E \cap F = A$.

5.2.2 ([BG10, Proj. 5.12]). Déterminez lesquels des énoncés suivants sont vrais pour tout choix d'ensembles A, B et C. Si une implication double ne tient pas, déterminez si l'une ou l'autre de ses implications est vraie. Si un énoncé est vrai, prouvez-le. Sinon, donnez un contre-exemple.

(i) $C \subseteq A$ et $C \subseteq B \iff C \subseteq (A \cup B)$.

(ii) $C \subseteq A$ ou $C \subseteq B \iff C \subseteq (A \cup B)$.

(iii) $C \subseteq A$ et $C \subseteq B \iff C \subseteq (C \cap B)$.

(iv) $C \subseteq A$ ou $C \subseteq B \iff C \subseteq (A \cap B)$.

5.2.3. Soient $Y \subseteq X$. Démontrez que $\left(Y^{\complement}\right)^{\complement} = Y$

5.2.4. Démontrez le Théorème 5.9(i).

5.2.5 ([BG10, Proj. 5.16]). Pour chaque énoncé suivant, démontrez qu'il est vrai pour tous ensembles A, B et C, ou bien donnez un contre-exemple.

(i) $A - (B \cup C) = (A - B) \cup (A - C)$.

(ii) $A \cap (B - C) = (A \cap B) - (A \cap C)$.

5.3 Produit cartésien

Soient A et B des ensembles. On définit un nouvel ensemble

$$A \times B := \{(a, b) \colon a \in A,\ b \in B\},$$

appelé le *produit cartésien* de A et B. On appelle (a, b) une *paire ordonnée*. Notez que (a, b) n'est *pas* le même chose que l'ensemble $\{a, b\}$. Dans un ensemble, l'ordre d'un élément est sans importance, donc $\{a, b\} = \{b, a\}$ pour tous a et b. Toutefois, l'égalité sur des paires ordonnées est définie par

$$(a, b) = (c, d) \iff a = c \text{ et } b = d.$$

Donc, $(a, b) = (b, a)$ si et seulement si $a = b$.

Exemple 5.14. Si $A = \{1, 2\}$ et $B = \{2, 3\}$, alors

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

Exemple 5.15. Le produit cartésien $\mathbb{N} \times \mathbb{N}$ est l'ensemble de toutes les paires ordonnées de nombres naturels. Par exemple, $(3, 5) \in \mathbb{N} \times \mathbb{N}$.

Proposition 5.16. *Si A et B sont des ensembles non vides tels que $A \neq B$, alors $A \times B \neq B \times A$.*

Preuve. Supposons que $A \neq B$. Alors soit $A \not\subseteq B$, soit $B \not\subseteq A$. Supposons que $A \not\subseteq B$. Alors, il existe un élément $a \in A$ tel que $a \notin B$. Puisque B n'est pas vide, on peut prendre un $b \in B$. Ainsi $(a, b) \in A \times B$, mais $(a, b) \notin B \times A$, puisque $a \notin B$. Le cas où $B \not\subseteq A$ est similaire. □

Remarque 5.17. Notez que $\varnothing \times A = \varnothing = A \times \varnothing$, pour tout ensemble A. C'est la raison pour laquelle il nous faut l'hypothèse que A et B soient non vides dans la Proposition 5.16.

Proposition 5.18. *Soient A, B et C des ensembles.*

(i) $A \times (B \cup C) = (A \times B) \cup (A \times C)$.

(ii) $A \times (B \cap C) = (A \times B) \cap (A \times C)$.

Preuve. On démontre la partie (i) et on laisse la preuve de la partie (ii) en exercice (Exercice 5.3.1). On a

$$\begin{aligned}
(x, y) \in A \times (B \cup C) &\iff x \in A \text{ et } y \in (B \cup C) \\
&\iff x \in A \text{ et } (y \in B \text{ ou } y \in C) \\
&\iff (x \in A \text{ et } y \in B) \text{ ou } (x \in A \text{ et } y \in C) \\
&\iff (x, y) \in A \times B \text{ ou } (x, y) \in A \times C \\
&\iff (x, y) \in (A \times B) \cup (A \times C).
\end{aligned}$$

□

Exercices.

5.3.1. Démontrez la Proposition 5.18(ii).

5.3.2 ([BG10, Proj. 5.21]). Pour chaque énoncé suivant, démontrez qu'il est vrai pour tout choix d'ensembles A, B, C et D, ou bien donnez un contre-exemple.

(i) $(A \times B) \cup (C \times D) = (A \cup C) \times (B \cup D)$.

(ii) $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$.

5.4 Fonctions

On dirige maintenant notre attention vers le concept important de fonction. Vous avez tous déjà vu des fonctions dans vos cours de mathématique auparavant. Vous pensiez sans doute à une fonction de la manière suivante. Une fonction consiste en

- un ensemble A appelé le *domaine* de la fonction;
- un ensemble B appelé le *codomaine* de la fonction;
- une "règle" f qui "assigne" à chaque $a \in A$ un élément $f(a) \in B$.

On dénote une telle fonction par $f\colon A \to B$.

Exemple 5.19. Considérons une fonction $f\colon \mathbb{Z} \to \mathbb{Z}$ définie par $f(n) = n^2 + 2$ pour tout $n \in \mathbb{Z}$. Le domaine de f est $\mathbb{Z}$ et le codomaine est également $\mathbb{Z}$. Notez que, même si f doit assigner un élément du codomaine à chaque élément du domaine, ce n'est *pas* le cas que tout élément du codomaine est égal à $f(n)$ pour un certain élément n du domaine. Par exemple, pour la fonction ci-haut, il n'y pas de $n \in \mathbb{Z}$ tel que $f(n) = -1$. Les fonctions

- $f\colon \mathbb{Z} \to \mathbb{Z}$, $f(n) = n^2 + 2$ pour tout $n \in \mathbb{Z}$, et
- $f\colon \mathbb{Z} \to \mathbb{N}$, $f(n) = n^2 + 2$ pour tout $n \in \mathbb{Z}$,

sont *différentes*, même si leurs domaines sont égaux et que la règle est la même. Le domaine et le codomaine font partie de la fonction. Donc, si deux fonctions ont des codomaines différents, alors ce sont des fonctions différentes.

Exemple 5.20. Toute suite $(x_j)_{j=1}^{\infty}$ est réellement une fonction dont le domaine est $\mathbb{N}$, où on emploie la notation x_j au lieu de $f(j)$.

La définition de fonction ci-haut est relativement vague. En particulier, que veulent dire les mots "règle" et "assigner"? Pour donner une définition précise d'une fonction, on doit se la représenter en termes de son graphe. Le *graphe* de $f\colon A \to B$ est

$$\Gamma(f) = \{(a, b) \in A \times B : b = f(a)\} = \{(a, f(a)) : a \in A\} \subseteq A \times B.$$

Si vous pensez à la façon dont vous avez dessinez des graphes (disons, en calcul infinitésimal), vous pouvez vous convaincre que cette définition correspond à ce que vous avez vu antécédemment.

Définition 5.21 (Fonction)**.** Une *fonction* avec *domaine* A et *codomaine* B est un sous-ensemble Γ de $A \times B$ tel que pour chaque $a \in A$, il y a un et un seul $b \in B$, tel que $(a, b) \in \Gamma$. Si $(a, b) \in \Gamma$, on écrit $b = f(a)$.

Remarque 5.22. Si vous pensez à notre définition précise d'une fonction (Définition 5.21), elle correspond avec ce que vous appeliez peut-être le "test de la droite verticale" pour les fonctions en calcul infinitésimal.

Exemple 5.23. Une opération binaire sur un ensemble A est une fonction $f\colon A \times A \to A$. Par exemple, l'addition est une opération binaire sur $\mathbb{Z}$. Donc, c'est une fonction $+\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$. Toutefois, on écrit habituellement $m + n$ au lieu de $+(m, n)$.

Exercices.

5.4.1. Parmi les constructions suivantes, lesquelles sont des fonctions?

(i) $\{(a, a^2) : a \in \mathbb{Z}\} \subseteq \mathbb{Z} \times \mathbb{Z}$

(ii) $\{(a, a^2) : a \in \mathbb{N}\} \subseteq \mathbb{N} \times \mathbb{N}$

(iii) $\{(a^2, a) : a \in \mathbb{Z}\} \subseteq \{n^2 : n \in \mathbb{Z}\} \times \mathbb{Z}$

(iv) $\{(a^2, a) : a \in \mathbb{N}\} \subseteq \{n^2 : n \in \mathbb{N}\} \times \mathbb{N}$.

5.5 Paradoxe de Russell et théorie axiomatique des ensembles

Vous vous demandez peut-être pour ce chapitre des notes s'intitule la théorie *naïve* des ensembles. C'est parce que nous avons pris pour acquis que, pour toute propriété P, on peut définir un ensemble

$$\{x : x \text{ a la propriété } P\}.$$

Toutefois, cela occasione des problèmes. Considérez l'ensemble

$$R = \{x : x \text{ est un ensemble et } x \notin x\}.$$

Alors on pose la question

$$\text{est-ce que } R \in R?$$

Si $R \in R$, alors, par définition de R, on obtient aussi $R \notin R$. D'une autre part, si $R \notin R$, alors, par définition de R, on obtient $R \in R$. Ainsi, on remarque que

$$R \in R \iff R \notin R.$$

Cela est une contradition connu sous le nom du *paradoxe de Russell*.

Il est possible de rectifier le paradoxe de Russell. La rectification nécessite que l'on retravaille notre concept d'ensemble, en commençant avec une liste spécifique d'axiome dictant ce qui est admissible et ce qui est non admissible de faire avec les ensembles. C'est ce qu'on appelle la *théorie axiomatique des ensembles*, ce qui va au-delà de l'étendue de ce cours. La théorie axiomatique des ensembles canonique s'appelle *ZFC*, nommé d'après Ernst Zermelo, Abraham Fraenkel et l'axiome du choix.

Dans ce cours, les problèmes liés au paradoxe de Russell n'occasioneront pas d'ennuis: on peut montrer que tous les ensembles utilisés dans le cours existent dans la théorie de ZFC. Ainsi, on demeurera "naïf" et on ignorera ces problèmes.

Chapitre 6

Relations d'équivalence et arithmétique modulaire

Dans ce chapitre, on aborde le concept de relation et, en particulier, de relation d'équivalence, un concept omniprésent en mathématiques. On dirige ensuite notre attention vers une famille particulière de relations d'équivalence, laquelle donne lieu à l'*arithmétique modulaire*.

6.1 Relations d'équivalence

Définition 6.1 (Relation)**.** Une *relation* sur un ensemble A est un sous-ensemble de $A \times A$. Si $R \subseteq A \times A$ est une relation sur A, on écrit habituellement xRy pour indiquer que $(x, y) \in R$ et on dit que x *est relié à* y par la relation R. Donc

$$xRy \iff (x, y) \in R.$$

On emploie souvent d'autres symboles que R, tel que $\sim, \approx, \equiv, <, \leq, >, \geq, \prec, \succ$, etc.

Exemple 6.2. Quelques exemples de relations sur $\mathbb{Z}$ sont:

- l'égalité $(=)$,
- plus petit que $(<)$,
- plus petit ou égal à $(\leq)$,
- divise (i.e. $a \mid b$).

Or, formellement parlant, ces relations sont des sous-ensembles de $\mathbb{Z} \times \mathbb{Z}$ et, par exemple, $\leq$ est donnée par

$$\{(a, b) : b - a \in \mathbb{N} \text{ ou } a = b\}.$$

Exemple 6.3. Le graphe $\Gamma(f)$ d'une fonction $f \colon A \to A$ est un cas spécial de relation, pour laquelle il y a exactement un $(x, y) \in \Gamma(f)$ pour chaque $x \in A$.

Définition 6.4 (Relation d'équivalence, classe d'équivalence)**.** Une relation $\sim$ sur un ensemble A est une *relation d'équivalence* si elle satisfait les trois propriétés suivantes:

Pour tous $a, b, c \in A$,

- $a \sim a$. (*Réflexivité*)
- Si $a \sim b$, alors $b \sim a$. (*Symétrie*)
- Si $a \sim b$ et $b \sim c$, alors $a \sim c$. (*Transitivité*)

Si $\sim$ est une relation d'équivalence sur A, alors la *classe d'équivalence* de $a \in A$ est

$$[a] := \{b \in A : b \sim a\}.$$

Parfois, on veut mettre l'accent sur une relation d'équivalence particulière (par exemple, lorsqu'on travaille avec plus d'une relation en même temps). Dans ce cas, on écrit $[a]_\sim$ au lieu de $[a]$.

Exemples 6.5. (i) La relation $=$ sur $\mathbb{Z}$ est une relation d'équivalence.

(ii) La relation $\leq$ sur $\mathbb{Z}$ n'est pas une relation d'équivalence, puisqu'elle n'est pas symétrique (e.g. $1 \leq 2$, mais $2 \not\leq 1$).

(iii) La relation $=$ sur les sous-ensembles de $\mathbb{Z}$ (i.e. l'égalité d'ensembles) est une relation d'équivalence.

(iv) La relation $\subseteq$ sur les sous-ensembles de $\mathbb{Z}$ n'est pas une relation d'équivalence car elle n'est pas symétrique.

Notez que, pour (iii) et (iv), la relation est définie sur l'ensemble

$$A = \{X : X \subseteq \mathbb{Z}\}$$

des sous-ensembles de $\mathbb{Z}$.

Proposition 6.6. *Soit $\sim$ une relation d'équivalence sur un ensemble A, et $a, b \in A$. Alors*

(i) $a \in [a]$, *et*

(ii) $a \sim b \iff [a] = [b]$.

Preuve. (i) Sachant que $\sim$ est une relation d'équivalence, elle est réflexive. Donc, pour tout $a \in A$, on a $a \sim a$, donc $a \in [a]$.

(ii) Supposons que $a \sim b$ pour $a, b \in A$. On démontre que $[a] = [b]$ en montrant les deux inclusions $[a] \subseteq [b]$ et $[b] \subseteq [a]$.

Soit $c \in [a]$. Alors $c \sim a$. Par la transitivité de $\sim$, on a $c \sim b$, et donc $c \in [b]$. Ainsi, $[a] \subseteq [b]$.

Maintenant, supposons que $c \in [b]$. Alors $c \sim b$. Par la symétrie de $\sim$, on a alors $b \sim a$ (puisque $a \sim b$). Puis, par la transitivité de $\sim$, on obtient $c \sim a$, et donc $c \in [a]$. Ainsi, $[b] \subseteq [a]$.

Réciproquement, supposons que $[a] = [b]$. Par la partie (i), on obtient $a \in [a] = [b]$, donc $a \in [b]$. Ainsi, $a \sim b$. □

On dit que a est un *représentant* de la classe d'équivalence $[a]$. Une classe peut admettre plus d'un représentant en général. Par la Proposition 6.6(ii), b est un représentant de la classe d'équivalence de $[a]$ si et seulement si $a \sim b$ (ce qui équivaut à dire $b \in [a]$).

La Proposition 6.6 implique que pour chaque $a \in A$, il existe une unique classe d'équivalence (i.e. $[a]$) contenant a. En fait, les classes d'équivalence d'une relation d'équivalence sur A subdivise l'ensemble A d'une certaine façon, ce que nous allons maintenant expliquer.

Proposition 6.7. *Supposons qu'on a une relation d'équivalence sur un ensemble A. Alors, pour tous $a, b \in A$, on a*

$$[a] = [b] \quad \textit{ou} \quad [a] \cap [b] = \varnothing.$$

Preuve. Soient $a, b \in A$. Si $[a] \cap [b] = \varnothing$, alors on a fini. Donc, supposons que $[a] \cap [b] \neq \varnothing$. Dans ce cas, il existe un élément $c \in [a] \cap [b]$. Ainsi, $a \sim c \sim b$, ce qui implique $a \sim b$. Puis, par la Proposition 6.6(ii), on obtient $[a] = [b]$. □

Définition 6.8 (Partition)**.** Une *partition* d'un ensemble A est un ensemble Π, dont les éléments sont des sous-ensembles de A, et il satisfait

- $P \in \Pi \implies P \neq \varnothing$
- $P_1, P_2 \in \Pi,\ P_1 \neq P_2 \implies P_1 \cap P_2 = \varnothing$, et
- tout $a \in A$ appartient à un $P \in \Pi$.

De manière équivalente, un ensemble Π de sous-ensembles non vides de A est une partition de A si chaque élément de A appartient à un unique élément de Π.

Intuitivement, une partition d'un ensemble A est une subdivision de A en sous-ensembles disjoints.

Exemple 6.9. Soit P_1 l'ensemble des entiers pairs et soit P_2 l'ensemble des entiers impairs. Alors $\Pi = \{P_1, P_2\}$ est une partition de $\mathbb{Z}$.

La prochaine proposition nous dit que, dans un certain sens, les relations d'équivalences et les partitions sont deux façons de représenter la même idée.

Proposition 6.10. *(i) Supposons que $\sim$ est une relation d'équivalence sur A. Alors, l'ensemble Π des classes d'équivalences de $\sim$ est une partition de A.*

(ii) Supposons que Π est une partition de A. Alors la relation $\sim$ définie pour tout $a, b \in A$ par

$$a \sim b \iff a \text{ et } b \text{ appartiennent au même élément de } \Pi$$

est une relation d'équivalence sur A.

Preuve. La partie (i) est la Proposition 6.7 combinée avec la Proposition (i) ($a \in A \implies [a] \neq \varnothing$). Pour démontrer la partie (ii), soit Π une partition de A. On définit la relation $\sim$ sur A par

$$a \sim b \iff a \text{ et } b \text{ appartiennent au même élément de } \Pi.$$

Réflexivité: Supposons que $a \in A$. Alors $a \in P$ pour un $P \in \Pi$. Donc, $a \sim a$.

Symétrie: Supposons que $a, b \in A$ avec $a \sim b$. Alors a et b (et donc b et a) appartiennent au même élément de Π. Donc, $b \sim a$.

Transitivité: Supposons que $a, b, c \in A$ avec $a \sim b$ et $b \sim c$. Alors a et b appartiennent à un $P \in \Pi$. Aussi, b et c appartiennent à un $P' \in \Pi$. Puisque b ne peut appartenir à un seul élément de Π, on a $P = P'$. Ainsi a et c appartiennent tous les deux à P, ce qui donne $a \sim c$. □

La *valeur absolue* d'un entier x est définie par

$$|x| = \begin{cases} x & \text{si } x \geq 0, \\ -x & \text{si } x < 0. \end{cases}$$

Exemple 6.11. Considérez la relation sur $\mathbb{Z}$ définie par

$$x \sim y \iff |x| = |y|.$$

- *Réflexivité*: Pour tout $x \in \mathbb{Z}$, $|x| = |x|$, donc $x \sim x$.
- *Symétrie*: Pour tous $x, y \in \mathbb{Z}$,

$$x \sim y \implies |x| = |y| \implies |y| = |x| \implies y \sim x.$$

- *Transitivité*: Pour tous $x, y, z \in \mathbb{Z}$,

$$x \sim y \text{ et } y \sim z \implies |x| = |y| = |z| \implies x \sim z.$$

Donc, $\sim$ est une relation d'équivalence. La classe d'équivalence de $x \in \mathbb{Z}$ est l'ensemble $\{x, -x\}$. L'ensemble

$$\Pi = \{\{x, -x\} : x \in \mathbb{Z}\}$$

est une partition de $\mathbb{Z}$.

Exemple 6.12. Considérez la relation sur $\mathbb{Z} \times \mathbb{Z}$ définie par

$$(x, y) \sim (v, w) \iff 2x - 3y = 2v - 3w.$$

- *Réflexivité*: Pour tout $(x, y) \in \mathbb{Z} \times \mathbb{Z}$, on a $2x - 3y = 2x - 3y$, donc $(x, y) \sim (x, y)$.
- *Symétrie*: Pour tous $(x, y), (v, w) \in \mathbb{Z} \times \mathbb{Z}$, $(x, y) \sim (v, w) \implies 2x - 3y = 2v - 3w \implies 2v - 3w = 2x - 3y \implies (v, w) \sim (x, y)$.
- *Transitivité*: Supposons que $(x, y) \sim (v, w)$ et que $(v, w) \sim (u, z)$. Alors, $2x - 3y = 2v - 3w$ et $2v - 3w = 2u - 3z$. Ainsi $2x - 3y = 2u - 3z$, et donc $(x, y) \sim (u, z)$.

Il s'ensuit que $\sim$ est une relation d'équivalence sur $\mathbb{Z} \times \mathbb{Z}$. Les classes d'équivalence sont les ensembles

$$\{(x, y) \in \mathbb{Z} \times \mathbb{Z} : 2x - 3y = n\}, \quad n \in \mathbb{Z}.$$

Il s'agit donc des points à coordonnées entiers le long de la droite fixée $2x - 3y = n$ dans le plan.

Exercices.

6.1.1 ([BG10, Proj. 6.7]). Pour chacune des relations suivantes définies sur $\mathbb{Z}$, déterminez lesquelles sont des relations d'équivalences. Si c'est le cas, déterminez les classes d'équivalences.

(i) $x \sim y$ si $x < y$.

(ii) $x \sim y$ si $x \leq y$.

(iii) $x \sim y$ si $|x| = |y|$.

(iv) $x \sim y$ si $x \neq y$.

(v) $x \sim y$ si $xy > 0$.

(vi) $x \sim y$ si ($x \mid y$ ou $y \mid x$).

6.1.2 ([BG10, Proj. 6.8]). Démontrez que chacune des relations suivantes définies sur $\mathbb{Z} \times \mathbb{Z}$ est une relation d'équivalences. Déterminez les classes d'équivalences pour chaque relation.

(i) $(x, y) \sim (v, w)$ si $x^2 + y^2 = v^2 + w^2$.

(ii) $(x, y) \sim (v, w)$ si $y - x^2 = w - v^2$.

(iii) $(x, y) \sim (v, w)$ si $xy = vw$.

(iv) $(x, y) \sim (v, w)$ si $x + 2y = v + 2w$.

6.1.3 ([BG10, Proj. 6.9]). Sur $\mathbb{Z} \times (\mathbb{Z} - \{0\})$ on définit la relation $(m_1, n_1) \sim (m_2, n_2)$ si $m_1 n_2 = n_1 m_2$.

(i) Montrez qu'il s'agit d'une relation d'équivalence.

(ii) Étant donné deux classes d'équivalence $[(m_1, n_1)]$ et $[(m_2, n_2)]$, on définit deux opérations binaires $\oplus$ et $\odot$ via

$$[(m_1, n_1)] \oplus [(m_2, n_2)] = [(m_1 n_2 + m_2 n_1, n_1 n_2)]$$

et

$$[(m_1, n_1)] \odot [(m_2, n_2)] = [(m_1 m_2, n_1 n_2)].$$

Quelles propriétés ces opérations binaires satisfont-elles? Par exemple, quels axiomes des entiers sont satisfaits?

6.2 L'algorithme de division

Dans la Section 6.3, on discutera une relation d'équivalence importante. Il nous faut tout d'abord un théorème sur la division des entiers.

Théorème 6.13 (L'algorithme de division)**.** *Soit $n \in \mathbb{N}$. Pour tout $m \in \mathbb{Z}$, il existe des $q, r \in \mathbb{Z}$ uniques tels que*

$$m = qn + r \quad \textit{et} \quad 0 \leq r \leq n-1.$$

L'entier q s'appelle le quotient *et r s'appelle le* reste *de la division de m par n.*

Preuve. Fixons un $n \in \mathbb{N}$. On démontre tout d'abord la partie existence du théorème. Puis, on commence par démontrer ce résultat pour tout entier $m \geq 0$, par induction sur m. Pour le cas de base $m = 0$, on peut choisir $q = r = 0$.

Pour l'étape inductive, supposons qu'il existe des $q, r \in \mathbb{Z}$ tels que

$$m = qn + r \qquad \text{et} \qquad 0 \leq r \leq n-1.$$

Cas 1: $r < n-1$. Donc, en posant $q' = q$ et $r' = r+1$, on obtient

$$m + 1 = q'n + r' \qquad \text{et} \qquad 0 \leq r' \leq n-1.$$

Case 2: $r = n-1$. Alors, en posant $q' = q+1$ et $r' = 0$, on obtient

$$m + 1 = qn + r + 1 = (q+1)n = q'n + r' \qquad \text{et} \qquad 0 \leq r' \leq n-1.$$

Dans les deux cas, on a trouvé des entiers q' et r' avec la propriété requise, complétant ainsi la preuve de l'étape inductive.

Maintenant, considérons le cas avec $m < 0$. Puisque $-m > 0$, on peut trouver, par la première partie de la preuve, des entiers q et r tels que

$$-m = qn + r \qquad \text{et} \qquad 0 \leq r \leq n-1.$$

Cas 1: $r = 0$. Alors $m = (-q)n + 0$ donne l'expression requise pour m.
Cas 2: $r > 0$. Alors

$$m = -qn - r = (-q-1)n + (n-r)$$

est l'expression requise, car $0 < n - r < n$.

Il reste à démontrer la partie unicité du théorème. Supposons que $m \in \mathbb{Z}$ et que

$$q_1 n + r_1 = m = q_2 n + r_2 \quad \text{pour des } q_1, q_2, r_1, r_2 \in \mathbb{Z},\ 0 \leq r_1, r_2 \leq n-1.$$

Alors nous avons

$$(q_1 - q_2)n = r_2 - r_1. \tag{6.1}$$

Ainsi, $r_2 - r_1$ est divisible par n. Mais puisque $0 \leq r_1, r_2 \leq n-1$, nous avons

$$1 - n \leq r_2 - r_1 \leq n - 1.$$

Puisque le seul multiple de n entre $1-n$ et $n-1$ est 0, on obtient $r_2 - r_1 = 0$, et donc $r_1 = r_2$. Cela (6.1) implique que $q_1 = q_2$ également. □

Exemples 6.14. (i) Pour $n = 3$ et $m = 11$, on obtient $q = 3$ et $r = 2$ car $11 = 3 \cdot 3 + 2$.

(ii) Pour $n = 5$ et $m = -26$, on obtient $q = -6$ et $r = 4$ car $-26 = (-6) \cdot 5 + 4$.

Exercices.

6.2.1. Démontrez les énoncés suivants.

(i) Un entier $m \in \mathbb{Z}$ est impair si et seulement s'il existe $q \in \mathbb{Z}$ tel que $m = 2q + 1$.

(ii) Pour tout $n \in \mathbb{Z}$, n est pair ou $n + 1$ est pair.

(iii) Un entier $m \in \mathbb{Z}$ est pair si et seulement si m^2 est pair.

6.3 Les entiers modulo n

Dans cette secion, on aborde un concept important et fréquemment rencontré en mathématiques: les entiers modulo n.

Pour un $n \in \mathbb{N}$ fixé, on définit une relation $\equiv$ sur $\mathbb{Z}$ par

$$x \equiv y \iff x - y \text{ est divisible par } n.$$

Le nombre naturel n est appelé le *module*. Lorsqu'on veut se référer explicitement au module, on écrit

$$x \equiv y \mod n.$$

Si $x \equiv y \mod n$, alors on dit que x et y sont *équivalents modulo n* ou *congruents modulo n* (ou parfois, simplement *équivalents/congruents mod n*). Notez que $x \equiv y \mod 1$ pour tout $x, y \in \mathbb{Z}$, et donc l'équivalence modulo 1 n'est pas très intéressante. Pour cette raison, on suppose habituellement que $n \geq 2$.

Exemple 6.15. Soit $n = 2$. Alors $x \equiv y \mod 2$ si et seulement si $x - y$ est pair, i.e. x et y sont soit tous les deux pairs, soit tous les deux impairs. Dans ce cas, on dit que x et y ont la même *parité*.

Exemple 6.16. Fixons le module 7. Alors $2 \equiv 16$, car $2 - 16 = -14$ est divisible par 7. De manière similaire, on a aussi

$$0 \equiv -7 \equiv 7 \equiv 14, \quad 1 \equiv -6 \equiv 8 \equiv 701, \quad 5 \equiv 7005.$$

Exemple 6.17. Soient $n \in \mathbb{N}$ et $m \in \mathbb{Z}$. Par l'algorithme de division (Théoreme 6.13), on a

$$m = qn + r \quad \text{pour des } q, r \in \mathbb{Z},\ 0 \leq r \leq n - 1.$$

Ainsi, $m - r = qn$ est divisible par n, et donc $m \equiv r \mod n$.

Proposition 6.18. *Fixons un module $n \in \mathbb{N}$.*

(i) L'équivalence modulo n (i.e. $\equiv$) est une relation d'équivalence.

(ii) La relation d'équivalence $\equiv$ admet exactement n classes d'équivalences distinctes, soient

$$[0], [1], \ldots, [n-1].$$

Preuve. Pour démontrer (i), on doit vérifier que $\equiv$ est réflexive, symétrique et transitive.
Réflexivité: Pour tout $a \in \mathbb{Z}$, $a - a = 0$ et 0 est divisible par n, donc $a \equiv a$.
Symétrie: Supposons que $a \equiv b$. Alors, n divise $a - b$. Par définition, il existe un $j \in \mathbb{Z}$ tel que $a - b = jn$. Mais alors, $b - a = -jn = (-j)n$ est également divisible par n, donc $b \equiv a$.
Transitivité: Supposons que $a \equiv b$ et $b \equiv c$. Alors n divise $a - b$ et $b - c$. Donc, il existe $j, k \in \mathbb{Z}$ tels que

$$a - b = jn \quad \text{et} \quad b - c = kn.$$

Alors,

$$a - c = (a - b) + (b - c) = jn + kn = (j + k)n$$

est divisible par n, donc $a \equiv c$.

Pour démontrer (ii), on doit démontrer que les classes d'équivalences $[0], [1], \ldots, [n-1]$ sont distinctes, et que tout entier est contenu dans l'une de ces classes.

Soit $m \in \mathbb{Z}$. L'exemple 6.17 démontre que $m \in [r]$ pour un certain $0 \leq r \leq n - 1$. Donc, tout entier est contenu dans une des classes $[0], [1], \ldots, [n-1]$.

Il reste à vérifier que ces classes sont distinctes. Donc, supposons qu'il existe $0 \leq m, k \leq n - 1$ avec $[m] = [k]$ (i.e. n divise $m - k$). On veut montrer que cela implique $m = k$. Or,

$$0 \leq m, k \leq n - 1 \implies -n + 1 \leq m - k \leq n - 1,$$

et le seul nombre entre $-n + 1$ et $n - 1$ qui est divisible par n est 0. Donc, $m - k = 0$, i.e. $m = k$. □

L'ensemble des classes d'équivalence pour la relation d'équivalence modulo n est appelé l'*ensemble des entiers modulo n*, et il est dénoté par $\mathbb{Z}_n$ ou $\mathbb{Z}/n\mathbb{Z}$.

Exemple 6.19. On a

$$\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}.$$

Exemple 6.20. Par la Proposition 6.18, pour tout entier a, sa classe d'équivalence modulo n est égale à une des classes

$$[0], [1], \ldots, [n-1].$$

L'exemple 6.17 nous dit comment déterminer de quelle classe il s'agit: on a $[a] = [r]$, où r est le reste de la division de a par n. Par exemple, si $n = 5$, alors on a

$$31 = 6 \cdot 5 + 1,$$

et donc $[31] = [1]$. Similairement,

$$[26] = [1], \quad [-1] = [4], \quad [12] = [2], \quad [35] = [0].$$

(L'idée de base est que l'on peut ajouter ou soustraire des multiples de n, jusqu'à ce que le représentant tombe dans l'intervalle $0, 1, \ldots, n-1$.) Si $n = 3$, on a

$$[-2] = [1], \quad [33] = [0], \quad [20] = [2].$$

Proposition 6.21. *Fixons un module $n \in \mathbb{N}$. Si $a \equiv a'$ et $b \equiv b'$, alors*

$$a + b \equiv a' + b' \quad \textit{et} \quad ab \equiv a'b'.$$

Preuve. Fixons un module n. Supposons que $a \equiv a'$ et $b \equiv b'$. Alors, il existe $k, \ell \in \mathbb{Z}$ tels que

$$a - a' = kn \quad \text{et} \quad b - b' = \ell n.$$

Puis,

$$(a + b) - (a' + b') = (a - a') + (b - b') = kn + \ell n = (k + \ell)n,$$

et donc $a + b \equiv a' + b'$. Aussi,

$$ab - a'b' = ab - ab' + ab' - a'b' = a(b - b') + (a - a')b' = a\ell n + knb' = (a\ell + kb')n,$$

et donc $ab \equiv a'b'$. □

La proposition ci-haut nous permet de définir deux opérations sur $\mathbb{Z}_n$: l'*addition* $\oplus$ et la *multiplication* $\odot$ sur $\mathbb{Z}_n$ à travers

$$[a] \oplus [b] = [a + b] \quad \text{et} \quad [a] \odot [b] = [ab].$$

Remarque 6.22. Il est important de comprendre *pourquoi* nous avons besoin de la Proposition 6.21 pour définir les opérations ci-haut. Rappelez-vous que $[a] = [a'] \iff a \equiv a'$ et $[b] = [b'] \iff b \equiv b'$ (par la Proposition 6.6(ii)). Notre définition de $\oplus$ requiert que la somme des classes $[a] = [a']$ et $[b] = [b']$ soit

$$[a + b] = [a] \oplus [b] = [a'] \oplus [b'] = [a' + b'].$$

Donc, si ce n'était pas vrai que $[a + b] = [a' + b']$, alors l'opération $\oplus$ ne serait pas bien définie (i.e. il y aurait un conflit dans notre définition). Heureusement, la Proposition 6.21 nous assure que l'opération ne dépend du choix de représentants pour les classes: on a bien $[a + b] = [a' + b']$.

Pour illustrer davantage ce point, supposons qu'on cherche à définir la fonction

$$f \colon \mathbb{Z}_5 \to \mathbb{Z}, \quad f([n]) = n.$$

Alors, puisque $[1] = [6]$, on aurait $f([1]) = f([6])$. Mais $f([1]) = 1 \neq 6 = f([6])$. Donc, en fait, cette fonction n'est *pas* bien définie.

Remarque 6.23. Plusieurs textes ne font que réutiliser la notation $+$ et $\cdot$ pour l'addition et la multiplication sur $\mathbb{Z}_n$. (En fait, c'est l'approche la plus courante.) On utilise la notation $\oplus$ et $\odot$ pour mettre en évidence le fait que ce sont des opérations sur des ensembles distincts ($\mathbb{Z}_n$ par opposition à $\mathbb{Z}$).

Exemple 6.24. Fixons un module $n \in \mathbb{N}$. Par la Proposition 6.18(ii), pour tout $a \in \mathbb{Z}$, la classe d'équivalence $[a]$ doit être égal à l'une des classes $[0], [1], \ldots, [n-1]$. Lorsqu'on effectue des calculs en arithmétique modulaire, on tend à écrire notre réponse finale sous cette forme. (Voir l'exemple 6.20.) Par exemple,

(i) Si $n = 4$, on a $[3] \oplus [2] = [3 + 2] = [5] = [1]$.

(ii) Si $n = 5$, on a $[4] \odot [3] = [4 \cdot 3] = [12] = [2]$.

(iii) Si $n = 2$, alors

$$[235] \odot [35423] \odot [24] = [1] \odot [1] \odot [0] = [1 \cdot 1 \cdot 0] = [0].$$

Proposition 6.25. *Fixons un entier $n \geq 2$. L'addition et la multiplication sur $\mathbb{Z}_n$ est commutative, associative et distributive. Aussi, l'ensemble $\mathbb{Z}_n$ admet un élément neutre additif $[0]$, un élément neutre multiplicatif $[1]$, et des inverses additifs (l'inverse additif de $[a]$ étant $[-a]$). En d'autres mots, en remplaçant $\mathbb{Z}$ par $\mathbb{Z}_n$ dans les Axiomes 1.1–1.4, ces derniers s'appliquent à $\mathbb{Z}_n$.*

Preuve. On va démontrer trois de ces énoncés, et on laisse les autres en exercices.

L'addition dans $\mathbb{Z}_n$ est commutative: Prenons deux éléments arbitraires $[a], [b] \in \mathbb{Z}_n$. Nous avons alors

$$\begin{aligned} [a] \oplus [b] &= [a + b] && \text{définition de } \oplus \\ &= [b + a] && \text{commutativité de l'addition dans } \mathbb{Z} \\ &= [b] \oplus [a]. && \text{définition de } \oplus \end{aligned}$$

Donc, l'addition dans $\mathbb{Z}_n$ est commutative.

La multiplication est distributive sur l'addition dans $\mathbb{Z}_n$: Prenons trois éléments arbitraires $[a], [b], [c] \in \mathbb{Z}_n$. Alors, on a

$$\begin{aligned} [a] \odot ([b] \oplus [c]) &= [a] \odot [b + c] && \text{par la définition de } \oplus \\ &= [a(b + c)] && \text{définition de } \odot \\ &= [ab + ac] && \text{distributivité dans } \mathbb{Z} \\ &= [ab] \oplus [ac] && \text{définition de } \oplus \\ &= [a] \odot [b] \oplus [a] \odot [c]. && \text{définition de } \odot \end{aligned}$$

Donc, la distributivité s'applique à $\mathbb{Z}_n$.

$[0] \in \mathbb{Z}_n$ *est l'élément neutre additif*: Prenons un élement arbitraire $[a] \in \mathbb{Z}_n$. Alors,

$$\begin{aligned} [a] \oplus [0] &= [a + 0] && \text{définition de } \oplus \\ &= [a]. && \text{car 0 est l'élém. neutre additif dans } \mathbb{Z} \end{aligned}$$

Ainsi, pour tout $[a] \in \mathbb{Z}_n$, on a $[a] \oplus [0]$. Donc, $[0]$ est un élément neutre additif dans $\mathbb{Z}_n$.

Les autres énoncés sont laissés en exercise (Exercice 6.3.3). □

Exercices.

6.3.1. Effectuez les calculs suivants dans $\mathbb{Z}_n$ avec la valeur donnée pour n. Dans chaque cas, écrivez votre réponse finale sous la forme standard: $[0], [1], [2], \ldots, [n-1]$. Vous ne devriez pas avoir recours à une calculatrice.

(i) $[3] \oplus [4]$, $n = 5$.

(ii) $[0] \oplus [4]$, $n = 8$.

(iii) $[3667] \oplus [6991]$, $n = 3$.

(iv) $[2] \odot [3]$, $n = 6$.

(v) $[2] \odot [3]$, $n = 5$.

(vi) $[5] \odot [6]$, $n = 7$.

(vii) $[503259] \odot [32485]$, $n = 2$.

6.3.2. Pour chacune des questions suivantes, écrivez votre réponse sous la forme standard: $[0], [1], [2], \ldots, [n-1]$, où n est le module.

(i) Quel est l'inverse additif de $[3]$ dans $\mathbb{Z}_7$?

(ii) Quel est l'inverse additif de $[3]$ dans $\mathbb{Z}_6$?

(iii) Quel est l'inverse additif de $[5]$ dans $\mathbb{Z}_{21}$?

(iv) Existe-t-il un élément $[a]$ de $\mathbb{Z}_7$ tel que $[a] \odot [3] = [1]$? Si oui, trouvez-le. Si non, démontrez qu'il n'existe pas de tel élément.

(v) Existe-t-il un élément $[a]$ de $\mathbb{Z}_{12}$ tel que $[a] \odot [3] = [1]$? Si oui, trouvez-le. Si non, démontrez qu'il n'existe pas de tel élément.

6.3.3. Complétez la preuve de la Proposition 6.25.

6.3.4. Fixons un module n. Supposons que $a, b \in \mathbb{Z}$ satisfont $0 < b < n$ et $[a] \odot [b] = [0]$. Démontrez que $[a]$ ne peut pas avoir d'inverse multiplicatif. En d'autres mots, démontrez qu'il n'existe pas de $[c] \in \mathbb{Z}_n$ tel que $[c] \odot [a] = [1]$.

6.3.5. Démontrez qu'il n'y pas d'entiers x, y, z tel que

$$9x^6 + 13y^5 + 4y^2 + 3z^6 = 0 \quad \text{et} \quad -6x^4 - 2y^5 + y^2 - 3z^8 = 1.$$

Indice: Faites une preuve par contradiction. Supposez que votre équations admet une solution et puis effectuez des calculs en représentation modulo 3 pour parvenir à une contradiction.

6.3.6. (i) Sans employer l'induction, démontrez que les énoncés suivants sont vrais:

$$\forall\, a \in \mathbb{Z} \ \left(a^2 \text{ est divisible par } 4 \text{ ou } a^2+3 \text{ est divisible par } 4\right).$$

Indice: Utilisez l'arithmétique modulaire.

(ii) Est-ce que l'énoncé

$$\left(\forall\, a \in \mathbb{Z},\ a^2 \text{ est divisible par } 4\right) \text{ ou } \left(\forall\, a \in \mathbb{Z},\ a^2+3 \text{ est divisible par } 4\right)$$

est vrai? Justifiez votre réponse.

6.4 Nombres premiers

Définition 6.26 (Nombre premier, nombre composé, facteur)**.** Un entier $n \geq 2$ est *premier* s'il est divisible uniquement par ± 1 et $\pm n$. Si un entier $n \geq 2$ n'est pas premier, on dit qu'il est *composé*. Si $n = q_1 q_2 \cdots q_k$ pour des $q_1, q_2, \ldots, q_k \in \mathbb{Z}$, alors les $q_1, q_2, \ldots, q_k$ sont appelés des *facteurs* de n, et l'expression $n = q_1 q_2 \cdots q_k$ est appelée une *factorisation* de n.

Proposition 6.27. *Tout entier $n \geq 2$ peut être factorisé en nombres premiers.*

Preuve. On démontre le résultat par induction sur n. Le cas de base s'associe à $n = 2$, lequel est déjà premier.

Pour l'étape inductive, prenons un $n \geq 3$ et supposons que tout entier plus petit que n (et ≥ 2) peut être factorisé en nombres premiers (induction forte). Si n est premier, on a terminé. Sinon, il existe $a, b \in \mathbb{N}$, $a, b \geq 2$, tels que $n = ab$. Alors $a, b < n$ et donc, par l'hypothèse d'induction, a et b peuvent s'écrire sous forme de produits de nombres premiers. Cela donne une factorisation première de n. □

Proposition 6.28. *Il y a une infinité de nombres premiers.*

Preuve. On démontre ce résultat par contradiction. Supposons qu'il existe seulement un nombre fini de nombres premiers: $p_1, p_2, \ldots, p_n$. Alors, considérons le nombre

$$q = p_1 p_2 \cdots p_n + 1.$$

Le reste de la division de q par p_i est 1, pour tout $1 \leq i \leq n$. Donc, q n'est divisible par aucun nombre premier. Ainsi, q n'admet pas de factorisation en nombres premiers, une contradiction avec la Proposition 6.27. □

Rappelons la Définition 2.36 où, pour $m, n \in \mathbb{Z}$, pas tous les deux nuls, on a défini $\text{pgcd}(m, n)$ comme étant le plus petit élément de l'ensemble

$$S = \{k \in \mathbb{N} : k = mx + ny \text{ pour des } x, y \in \mathbb{Z}\}.$$

Quand $m = n = 0$, l'ensemble S est vide et, dans ce cas, on a défini $\text{pgcd}(0, 0) = 0$.

Proposition 6.29. *Soient $m, n \in \mathbb{Z}$.*

(i) $\operatorname{pgcd}(m,n)$ *divise* m *et* n.

(ii) Si $m \neq 0$ *ou* $n \neq 0$, *alors* $\operatorname{pgcd}(m,n) > 0$.

(iii) Tout entier qui divise à la fois m *et* n, *divise également* $\operatorname{pgcd}(m,n)$.

Preuve. La preuve de cette proposition se trouve dans [BG10, Prop. 6.29]. □

Les Propositions 6.29 et 2.24 impliquent que $\operatorname{pgcd}(m,n)$ est le plus grand entier qui divise à la fois m et n. Ainsi, $\operatorname{pgcd}(m,n)$ est le *plus grand commun diviseur* de m et n, justifiant ainsi la notation.

Proposition 6.30. *Pour tous* $k,m,n \in \mathbb{Z}$, *on a*

$$\operatorname{pgcd}(km,kn) = |k| \operatorname{pgcd}(m,n).$$

Preuve. Si $k=0$, alors $\operatorname{pgcd}(km,kn) = \operatorname{pgcd}(0,0) = 0 = 0 \cdot \operatorname{pgcd}(m,n) = |k| \operatorname{pgcd}(m,n)$. Si $m=n=0$, alors $\operatorname{pgcd}(km,kn) = 0 = 0 = |k| \operatorname{pgcd}(m,n)$ également. Donc, supposons que $k \neq 0$, et que $m \neq 0$ ou $n \neq 0$.

Posons

$$S = \{j \in \mathbb{N} : j = mx + ny \text{ pour des } x,y \in \mathbb{Z}\}$$

et

$$T = \{j \in \mathbb{N} : j = kmx + kny \text{ pour des } x,y \in \mathbb{Z}\}.$$

Soient $g = \operatorname{pgcd}(m,n)$ et $h = \operatorname{pgcd}(km,kn)$. Donc, g est le plus petit élément de S et h est le plus petit élément de T. Notre objectif est de démontrer que $|k|g = h$.

Puisque $g \in S$, alors il existe des entiers x_1 et y_1 tels que $g = mx_1 + ny_1$. Ainsi,

$$|k|g = m(|k|x_1) + n(|k|y_1) = mk(\pm x_1) + nk(\pm y_1)$$

est un élément de T. (Ici, on se sert du fait que $|k|$ est égal à k ou à $-k$.) Puisque h est le *plus petit* élément de T, cela implique que $|k|g \geq h$.

D'une autre part, $h \in T$, et donc il existe des entiers x_2 et y_2 tels que

$$h = kmx_2 + kny_2 = \pm|k|(mx_2 + ny_2).$$

Donc, $|k|$ divise h, et il s'ensuit que l'entier $\frac{h}{|k|} = \pm(mx_2 + ny_2) = m(\pm x_2) + n(\pm y_2)$ est un élément de S. Or, g est le *plus petit* élément de S, donc on a $g \leq \frac{h}{|k|}$, et donc $|k|g \leq h$.

Les deux inégalités impliquent que $|k|g = h$. □

Proposition 6.31 (Lemme d'Euclide)**.** *Supposons que* p *est un nombre premier et que* $m,n \in \mathbb{N}$. *Si* $p|mn$, *alors* $p|m$ *ou* $p|n$.

Preuve. Supposons que p divise mn. Si p divise m, alors on a terminé. Sinon, considérons le cas où p ne divise pas m. On doit montrer que p divise n. Puisque p est premier et qu'il ne divise pas m, alors nous avons $\operatorname{pgcd}(m,p) = 1$. Par la Proposition 6.30, on a

$$\operatorname{pgcd}(mn,pn) = n \operatorname{pgcd}(m,p) = n.$$

Puis, par la Proposition 6.29(iii), combiné avec le fait que p divise à la fois mn et pn, on peut conclure que p divise n. □

Corollaire 6.32. *Soient $k \in \mathbb{N}$, p un nombre premier et $m_1, \ldots, m_k \in \mathbb{N}$. Si $p \mid m_1 m_2 \cdots m_k$, alors $p \mid m_i$ pour un certain i avec $1 \leq i \leq k$.*

Preuve. Soit $P(k)$, l'énoncé

$$\forall m_1, m_2, \ldots, m_k \in \mathbb{N},\ (p|m_1 m_2 \cdots m_k) \implies (p|m_i \text{ pour un certain } i \text{ avec } 1 \leq i \leq k).$$

On démontre que $P(k)$ est vrai pour tout $k \geq 1$, par induction sur k.

Cas de base: Considérons le cas où $k = 1$. L'énoncé $P(1)$ est

$$\forall m_1 \in \mathbb{N},\ (p|m_1) \implies (p|m_1),$$

lequel est clairement vrai.

Étape inductive: Supposons que $P(n)$ est vrai pour un certain $n \in \mathbb{N}$. On va démontrer que $P(n+1)$ est vrai. Considérons n'importe quels $m_1, \ldots, m_{n+1} \in \mathbb{N}$ et supposons que p divise

$$m_1 m_2 \cdots m_{n+1} = (m_1 m_2 \cdots m_n) m_{n+1}.$$

Alors, par la Proposition 6.31, $p|m_1 \cdots m_n$ ou $p|m_{n+1}$. Dans le premier cas, l'hypothèse d'induction implique que $p|m_i$ pour un certain i avec $1 \leq i \leq n$. Donc, d'une façon ou d'une autre, $p|m_i$ pour un certain i avec $1 \leq i \leq n+1$. Cela complète la preuve de l'étape inductive. □

Par la Proposition 6.27, tout entier $n \geq 2$ admet une factorisation en nombres premiers. Notre prochain objectif est de démontrer que, en fait, une telle factorisation première est *unique*. Bien sûr, on peut toujours réarranger l'ordre des facteurs de la factorisation. Par exemple,

$$30 = 2 \cdot 3 \cdot 5 = 3 \cdot 2 \cdot 5.$$

Donc, le mieux qu'on peut espérer est que la factorisation première soit unique à l'ordre près des facteurs (i.e. que deux factorisations premières d'un même entier $n \geq 2$ ne diffèrent que par un réarrangement de leurs facteurs premiers).

Théorème 6.33. *Tout entier $n \geq 2$ admet une factorisation unique en nombres premiers, à l'ordre près des facteurs.*

Preuve. Une factorisation première *existe* par la Proposition 6.27. Il reste à démontrer la partie unicité du théorème. On procède par induction sur n.

Cas de base: Quand $n = 2$, la seule factorisation possible est l'expression 2 elle-même, puisqu'il n'y a pas d'autre façon d'écrire 2 comme un produit de nombres premiers (il n'y a pas de nombre premier plus petit que 2).

Étape inductive: Maintenant, considérons un $n \geq 3$ et supposons que tout entier plus petit que n (et ≥ 2) admet une factorisation unique en nombres premiers. Supposons que n admet deux factorisations en nombres premiers

$$n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_j.$$

Alors, par le corollaire 6.32, p_1 divise q_i pour un certain $1 \leq i \leq j$. Mais puisque q_i est premier, cela implique $p_1 = q_i$ (car p_1 ne peut être égal à ± 1 ou $-q_i$, et ce sont les seuls autres facteurs de q_i). Donc, on a

$$\frac{n}{p_1} = p_2 p_3 \cdots p_k = q_1 q_2 \cdots q_{i-1} q_{i+1} \cdots q_j.$$

Par l'hypothèse d'induction, ces deux factorisations en nombre premiers de $\frac{n}{p_1}$ sont identiques, à l'ordre près des facteurs. Ainsi, les deux factorisations premières données pour n sont identiques, à l'ordre près des facteurs. □

Proposition 6.34. *Si p est premier et $0 < r < p$, alors $\binom{p}{r}$ est divisible par p.*

Preuve. La preuve de cette proposition se trouve dans [BG10, Prop. 6.34]. □

Théorème 6.35 (Petit théorème de Fermat)**.** *Si $m \in \mathbb{Z}$ et p est un nombre premier, alors*

$$m^p \equiv m \mod p.$$

Preuve. Fixons un nombre premier p. Si $p = 2$, alors le petit théorème de Fermat énonce que m^2 est pair si et seulement si m est pair, et il s'agit simplement de la Proposition 6.2.1(iii). Donc, supposons que $p > 2$.

Soit $P(k)$ l'énoncé

$$k^p \equiv k \mod p.$$

On commence par démontrer que $P(m)$ est vrai pour tout $m \geq 0$. (On s'occupera du cas de $m < 0$ après.)

Cas de base: Puisque $0^p - 0 = 0 - 0 = 0$ est divisible par p, on a $0^p \equiv 0$.

Étape inductive: On suppose que $P(m)$ est vrai pour un certain $m \geq 0$ et on montre que $P(m+1)$ est vrai. Par le théorème du binôme (Théorème 4.12), on a

$$(m+1)^p = \sum_{\ell=0}^{p} \binom{p}{\ell} m^\ell 1^{p-\ell} = \sum_{\ell=0}^{p} \binom{p}{\ell} m^\ell.$$

Par la Proposition 6.34, $\binom{p}{\ell} \equiv 0 \mod p$ pour $0 < \ell < p$. Donc,

$$(m+1)^p = \sum_{\ell=0}^{p} \binom{p}{\ell} m^\ell \equiv \binom{p}{0} m^0 + \binom{p}{p} m^p = 1 + m^p \equiv 1 + m \mod p,$$

où l'on a employé l'hypothèse d'induction à la dernière étape. Cela complète la preuve de l'étape inductive. (Notez que la séquences d'équations ci-haut comporte à la fois $=$ et $\equiv$. Mais, étant donné que l'égalité implique l'équivalence mod p, on peut remplacer tous les symboles $=$ par $\equiv$ dans la séquence, et les énoncés restent vrais. On peut ensuite appliquer la transitivité de $\equiv$ pour conclure que $(m+1)^p \equiv 1 + m$.)

Il reste à démontrer $P(m)$ pour les $m < 0$. Soit $m < 0$. Posons $n = -m$. Alors $n > 0$ et donc, par la preuve ci-haut, on obtient $n^p \equiv n \mod p$. Puisque p est impair, on a

$$m^p = (-n)^p = (-1)^p n^p = -n^p \equiv -n = m.$$

Donc le résultat suit pour $m < 0$. □

Corollaire 6.36. *Soient $m \in \mathbb{Z}$ et p un nombre premier qui ne divise pas m. Alors*

$$m^{p-1} \equiv 1 \mod p.$$

Preuve. Par le Théorème 6.35, on a $m^p \equiv m$. En d'autres mots, p divise $m^p - m = m(m^{p-1} - 1)$. Mais p ne divise pas m, donc on peut conclure que p divise $m^{p-1} - 1$ par la Proposition 6.31. Ainsi, $m^{p-1} \equiv 1$. □

Remarque 6.37. Le petit théorème de Fermat constitue le résultat mathématique au fondement de la théorie du Chiffrement RSA. Donc, votre information de compte bancaire est sécurisé lorsque vous vérifier votre balance en ligne grâce au petit théorème de Fermat.

Exercices.

6.4.1 ([BG10, Proj. 6.27]). Pour quel $n \geq 2$, $\mathbb{Z}_n$ satisfait-il la propriété d'annulation (l'Axiome 1.5)? Démontrez votre assertion.

6.4.2. Soient $m, n \in \mathbb{N}$. Supposons que m divise n, et que p est un facteur premier de n qui n'est pas un facteur premier de m. Démontrez que m divise $\frac{n}{p}$. *Indice*: Utilisez la factorisation en nombres premiers.

6.4.3. Étant donné $a, b \in \mathbb{N}$, on peut les écrire comme des produits de nombres premiers

$$a = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k} \quad \text{et} \quad b = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k},$$

où les $p_1, \ldots, p_k$ sont des nombres premiers distincts, et les exposants sont des éléments de $\mathbb{Z}_{\geq 0}$. (On permet les exposants nuls pour permettre des factorisations premières de a et b qui emploient la même liste de nombres premiers—en utilisant un exposant de zéro quand l'un de ces nombres premiers n'apparait pas dans l'une des factorisations. Cela permet aussi de considérer le cas avec $a = 1$ ou $b = 1$, où tous les exposants sont nuls.) Démontrez que a divise b si et seulement si $n_i \leq m_i$ pour tout $1 \leq i \leq k$.

6.4.4. Supposons que p est un nombre premier. Démontrez que, pour tout $x \in \mathbb{Z}$,

$$3x^{p^2} - 5x^{p^3} + 2x$$

est divisible par p.

6.4.5. Supposons que $a, b \in \mathbb{N}$ admettent les factorisation premières suivantes

$$a = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k} \quad \text{et} \quad b = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k},$$

où les $p_1, \ldots, p_k$ sont des nombres premiers distincts, et où les exposants sont des éléments de $\mathbb{Z}_{\geq 0}$. Définissons

$$\text{PGCD}(a, b) = p_1^{\ell_1} p_2^{\ell_2} \cdots p_k^{\ell_k}$$

où, pour $1 \leq i \leq k$, ℓ_i est défini comme étant le minimum entre n_i et m_i. (Notez la différence entre cette définition et celle de $\text{pgcd}(a, b)$.)

(i) Démontrez que PGCD(a, b) divise pgcd(a, b). *Indice*: Utilisez la Proposition 6.29(iii).

(ii) Démontrez que pgcd(a, b) divise PGCD(a, b). *Indice*: Utilisez la Proposition 6.29(i).

(iii) Démontrez que PGCD$(a, b) =$ pgcd(a, b).

Chapitre 7

Nombres réels

Dans ce chapitre, on introduit les nombre réels. Comme pour le cas des entiers, vous avez sans doute rencontrez les nombres réels auparavant. Toutefois, nous allons prendre une approche beaucoup plus rigoureuse. Plus précisément, on va commencer avec une liste précise d'axiomes, et on va supposer qu'il existe un ensemble $\mathbb{R}$ satisfaisant les axiomes. Plusieurs des axiomes sont les mêmes que ceux des entiers. Toutefois, il y a des différences notables.

7.1 Axiomes

On suppose qu'il existe un ensemble, dénoté $\mathbb{R}$, avec des opérations binaires $+$ (*addition*) et $\cdot$ (*multiplication*) satisfaisant les Axiomes 7.1–7.5, 7.13 et 7.35. Les élément de $\mathbb{R}$ sont appelés les *nombres réels*.

Axiome 7.1 (Commutativité, associativité et distributivité)**.** Pour tout $x, y, z \in \mathbb{R}$, on a

(i) $x + y = y + x$, (*commutativité de l'addition*)

(ii) $(x + y) + z = x + (y + z)$, (*associativité de l'addition*)

(iii) $x \cdot (y + z) = x \cdot y + x \cdot z$, (*distributivité*)

(iv) $x \cdot y = y \cdot x$, (*commutativité de la multiplication*)

(v) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$. (*associativité de la multiplication*)

Comme on l'a fait pour les entiers, on dénotera souvent la multiplication à travers la *juxtaposition* (en écrivant xy au lieu de $x \cdot y$).

Axiome 7.2 (Élément neutre additif)**.** Il existe un nombre réel 0 satisfaisant $\forall x \in \mathbb{R},\ x+0 = x$. Cet élément 0 est appelé l'*élément neutre additif* (ou *élément identité de l'addition*).

Axiome 7.3 (Élément neutre multiplicatif)**.** Il existe un nombre réel 1 tel que $1 \neq 0$ et $\forall x \in \mathbb{R},\ x \cdot 1 = x$. L'élément 1 est appelé l'*élément neutre multiplicatif* (ou *élément identité de la multiplication*).

Axiome 7.4 (Inverse additif)**.** Pour chaque $x \in \mathbb{R}$, il existe un nombre réel, dénoté $-x$, tel que $x + (-x) = 0$. Cet élément $-x$ est appelé un *inverse additif* de x.

Axiome 7.5 (Inverse multiplicatif)**.** Pour chaque each $x \in \mathbb{R} - \{0\}$, il existe un nombre réel, dénoté x^{-1}, tel que $x \cdot x^{-1} = 1$. L'élément x^{-1} est appelé un *inverse multiplicatif* de x.

Remarque 7.6. Quoique nous employons la même notation 0 et 1 pour les éléments neutres additif et multiplicatif des nombres réels $\mathbb{R}$ que pour les éléments correspondants dans les entiers $\mathbb{Z}$, ils sont, *à priori*, des élements différents car nous n'avons pas encore établit de relation entre $\mathbb{Z}$ et $\mathbb{R}$. Plus tard, à la Section 8.2, on étudiera comment on peut voir $\mathbb{Z}$ comme un sous-ensemble de $\mathbb{R}$ et, ainsi, on aura que le 0 de $\mathbb{Z}$ correspond avec le 0 de $\mathbb{R}$, et de même pour le 1. Cela justifie l'emploi de la même notation.

Proposition 7.7. *Pour chaque $x \in \mathbb{R} - \{0\}$, il existe un* unique *nombre réel y tel que $xy = 1$.*

Preuve. Soit $x \in \mathbb{R} - \{0\}$. Par l'Axiome 7.5, il existe un nombre réel y tel que $xy = 1$. Il reste à vérifier que l'élément est unique. Supposons qu'il existe un autre nombre réel z tel que $xz = 1$. Alors on obtient

$$y = y \cdot 1 = y(xz) = (yx)z = (xy)z = 1 \cdot z = z.$$

Donc, l'élément avec la propriété en question est unique. □

La Proposition 7.7 nous permet ainsi de dire que x^{-1} est *l'*inverse multiplicatif de x (par opposition à *un* inverse multiplicatif de x).

Corollaire 7.8. *Pour $x \in \mathbb{R}$ avec $x \neq 0$, on a $(x^{-1})^{-1} = x$.*

Preuve. Soit $x \in \mathbb{R}$ tel que $x \neq 0$. Alors

$$x^{-1}x = xx^{-1} = 1.$$

Donc, x est l'inverse multiplicatif de x^{-1}. Puisque l'inverse multiplicatif est unique (par la Proposition 7.7), on doit avoir $(x^{-1})^{-1} = x$. □

Remarque 7.9. Étant donné que l'addition et la multiplication des nombres réels est associative, on peut omettre les parenthèses quand on écrit l'addition ou la multiplication de plus de deux éléments. Par exemple, si $w, x, y, z \in \mathbb{R}$, on peut écrire sans ambiguïté les expressions

$$w + x + y + z \quad \text{et} \quad wxyz,$$

étant donné que le résultat des additions et des multiplications ne dépend pas de la façon dont on regroupe les termes. (Voir la remarque 1.29.)

Proposition 7.10. *Pour tous $x, y \in \mathbb{R} - \{0\}$, on a $(xy)^{-1} = x^{-1}y^{-1}$.*

Preuve. Soient $x, y \in \mathbb{R} - \{0\}$. Par l'Axiome 7.5, x et y admettent des inverses multiplicatifs x^{-1} et y^{-1}, respectivement. On obtient alors

$$\begin{aligned} & (xy)^{-1}xy = 1 \\ \implies & (xy)^{-1}xyy^{-1} = y^{-1} \\ \implies & (xy)^{-1}x \cdot 1 = y^{-1} \\ \implies & (xy)^{-1}x = y^{-1} \\ \implies & (xy)^{-1}xx^{-1} = y^{-1}x^{-1} \\ \implies & (xy)^{-1} \cdot 1 = x^{-1}y^{-1} \\ \implies & (xy)^{-1} = x^{-1}y^{-1}. \end{aligned}$$

□

Proposition 7.11. *Soient $x, y, z \in \mathbb{R}$ avec $x \neq 0$. Si $xy = xz$, alors $y = z$.*

Preuve. Soient $x, y, z \in \mathbb{R}$ avec $x \neq 0$. Supposons que $xy = xz$. Par l'Axiome 7.5, x est l'inverse multiplicatif x^{-1}. Alors

$$\begin{aligned} & xy = xz \\ \implies & x^{-1}xy = x^{-1}xz \\ \implies & xx^{-1}y = xx^{-1}z \\ \implies & 1 \cdot y = 1 \cdot z \\ \implies & y = z. \end{aligned}$$

□

Remarque 7.12. Vous devez comparer les Axiomes 7.1–7.5 et les Axiomes 1.1–1.5. En remplaçant $\mathbb{Z}$ par $\mathbb{R}$,

- L'Axiome 1.1 devient l'Axiome 7.1,
- L'Axiome 1.2 devient l'Axiome 7.2,
- L'Axiome 1.3 devient l'Axiome 7.3, et
- L'Axiome 1.4 devient l'Axiome 7.4.

On remarque que les Axiomes 1.5 et 7.5 ne correspondent pas. Toutefois, la Proposition 7.11 affirme que l'Axiome 1.5 est vrai pour $\mathbb{R}$ également (i.e. l'Axiome 7.5 est plus fort que l'Axiome 1.5). Ainsi, toutes les propositions qu'on a démontrées pour $\mathbb{Z}$ en employant seulement les Axiomes 1.1–1.5 sont également vrai pour $\mathbb{R}$; elles admettent des preuves identiques. En particulier, toutes les propositions du Chapitre 1, où l'on remplace $\mathbb{Z}$ par $\mathbb{R}$, sont vraies pour $\mathbb{R}$. Pour se référer aux propositions correspondantes pour $\mathbb{R}$, on ajoutera le suffixe "pour $\mathbb{R}$". Par exemple, on pourra écrire "par la Proposition 1.9 pour $\mathbb{R}$".

Soustraction. Ainsi, comme pour les entiers, on peut définir la *soustraction* dans $\mathbb{R}$ par

$$x - y := x + (-y), \quad x, y \in \mathbb{R}.$$

Donc, la Proposition 1.28 tient également quand on remplace $\mathbb{Z}$ par $\mathbb{R}$.

Division. On n'a pas encore abordé la notion de division dans le cours, car elle ne se comportait pas bien pour les entiers. (Étant donné deux entiers arbitraires, il est improbable que l'on puisse diviser l'un par l'autre et obtenir un entier.) Toutefois, on peut définir la *division* dans $\mathbb{R}$. Pour tout $x, y \in \mathbb{R}$ avec $x \neq 0$, on définit

$$\frac{y}{x} := yx^{-1}.$$

Pour être plus précis, la division est une fonction

$$\text{division}\colon \mathbb{R} \times (\mathbb{R} - \{0\}) \to \mathbb{R}, \quad \text{division}(y, x) = yx^{-1}.$$

Notez que

$$\frac{1}{x} = 1 \cdot x^{-1} = x^{-1}.$$

Exercices.

7.1.1. En utilisant seulement les Axiomes 7.1–7.5 et la définition de la division, démontrez que vous pouvez additionner les "fractions" ayant un dénominateur commun, comme vous l'avez appris à l'école primaire. Plus précisément, démontrez que, pour tous $a, b, c \in \mathbb{R}$ avec $c \neq 0$,

$$\frac{a}{c} + \frac{b}{c} = \frac{a+b}{c}.$$

7.1.2. Soient $a, b, c, d \in \mathbb{R}$ et $b, d \neq 0$. Démontrez que

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}.$$

Démontrez toutes vos étapes.

7.1.3. Soit $x \in \mathbb{R}$ avec $x \neq 0$. Démontrez que $(-x)^{-1} = -x^{-1}$. (Par la priorité des opérations, $-x^{-1} = -(x^{-1})$.)

7.1.4. Soient $a, b \in \mathbb{R}$ avec $b \neq 0$. Démontrez que

$$\frac{-a}{b} = -\frac{a}{b} = \frac{a}{-b}.$$

7.1.5. Démontrez que zéro n'admet pas d'inverse multiplicatif.

7.2 Nombres réels positifs et ordre

Lors de notre discussion sur les nombres naturels, après avoir introduit les Axiomes 1.1–1.5 et démontré des propositions découlant de ces axiomes, on a ajouté un axiome (l'Axiome 2.1) garantissant l'existence de l'ensemble $\mathbb{N}$ des nombres naturels. Il s'ensuivit un ordre sur les entiers. On introduit maintenant un axiome correspondant à l'Axiome 2.1, mais pour $\mathbb{R}$. En effet, $\mathbb{N}$ était devenu le représentant de l'ensemble des entiers positifs, et on peut caractérisé un ensemble similaire pour $\mathbb{R}$: l'ensemble des entiers positifs.

Axiome 7.13. Il existe un sous-ensemble $\mathbb{R}_{>0} \subseteq \mathbb{R}$ avec les propriétés suivantes:

(i) Si $x, y \in \mathbb{R}_{>0}$, alors $x + y \in \mathbb{R}_{>0}$. (L'ensemble $\mathbb{R}_{>0}$ est fermé sous l'addition.)

(ii) Si $x, y \in \mathbb{R}_{>0}$, alors $xy \in \mathbb{R}_{>0}$. (L'ensemble $\mathbb{R}_{>0}$ est fermé sous la multipliaction .)

(iii) $0 \notin \mathbb{R}_{>0}$.

(iv) Pour tout $x \in \mathbb{R}$, on a $x \in \mathbb{R}_{>0}$ ou $x = 0$ ou $-x \in \mathbb{R}_{>0}$.

Les éléments de $\mathbb{R}_{>0}$ sont appelés les *nombres réels positifs*. Un nombre réel qui n'est ni positif ni zéro est appelé un *nombre réel négatif*.

Notez que l'Axiome 7.13 est le même que l'Axiome 2.1, mais avec $\mathbb{Z}$ et $\mathbb{N}$ remplacés par $\mathbb{R}$ et $\mathbb{R}_{>0}$, respectivement.

Proposition 7.14. *(i) Étant donné un $x \in \mathbb{R}$, un et un seul des énoncés suivants est vrai:*

- $x \in \mathbb{R}_{>0}$,
- $-x \in \mathbb{R}_{>0}$,
- $x = 0$.

(ii) On a $1 \in \mathbb{R}_{>0}$.

Preuve. La preuve de la partie (i) est la même que celle de la Proposition 2.3, mais avec $\mathbb{Z}$ et $\mathbb{N}$ remplacés par $\mathbb{R}$ et $\mathbb{R}_{>0}$, respectivement. Puis, la preuve de la partie (ii) est la même que celle de la Proposition 2.4. □

On peut maintenant définir un ordre sur l'ensemble des nombres réels, comme nous l'avons fait pour les entiers.

Définition 7.15 (Ordre sur les nombres réels)**.** Pour $x, y \in \mathbb{R}$, on écrit $x < y$ (et on dit que x est *plus petit que* y) ou $y > x$ (et on dit que y est *plus grand que* x) si et seulement si

$$y - x \in \mathbb{R}_{>0}.$$

On écrit $x \leq y$ (et on dit que x est *plus petit ou égal à* y) or $y \geq x$ (et on dit que y est *plus grand ou égal à* x) si et seulement si

$$x < y \quad \text{ou} \quad x = y.$$

Remarque 7.16. Notez que la Définition 7.15 est la même que la Définition 2.5, mais avec $\mathbb{Z}$ et $\mathbb{N}$ remplacés par $\mathbb{R}$ et $\mathbb{R}_{>0}$, respectivement. Ainsi, plusieurs des propositions concernant l'ordre sur $\mathbb{Z}$ que l'on a démontrées à la Section 2.2 sont également vraies lorsqu'on remplace $\mathbb{Z}$ et $\mathbb{N}$ par $\mathbb{R}$ et $\mathbb{R}_{>0}$, avec des preuves identiques. En particulier, les Propositions 2.6–2.15 sont vraies pour $\mathbb{R}$ également. Encore une fois (voir remarque 7.12) on se réferera aux propositions correspondantes pour $\mathbb{R}$ en ajoutant le suffixe "pour $\mathbb{R}$".

Proposition 7.17. *(i) Soit $x \in \mathbb{R}$ tel que $x \neq 0$. Alors $x \in \mathbb{R}_{>0}$ si et seulement si $\frac{1}{x} \in \mathbb{R}_{>0}$.*

(ii) Soient $x, y \in \mathbb{R}_{>0}$. Si $x < y$, alors $0 < \frac{1}{y} < \frac{1}{x}$.

Preuve. (i) Supposons que $x \in \mathbb{R}_{>0}$. Par l'Axiome 7.13(iv), on a $\frac{1}{x} \in \mathbb{R}_{>0}$ or $\frac{1}{x} = 0$ ou $-\frac{1}{x} \in \mathbb{R}_{>0}$. On démontre que les deux derniers cas mènent à une contradiction. Tout d'abord, supposons que $\frac{1}{x} = 0$. Alors

$$1 = x \cdot \frac{1}{x} = x \cdot 0 = 0,$$

où la Proposition 1.14 pour $\mathbb{R}$ a été employée à la dernière égalité. Mais l'égalité $1 = 0$ contredit l'Axiome 7.3. Maintenant, supposons que $-\frac{1}{x} \in \mathbb{R}_{>0}$. Alors

$$-1 = -\left(x \cdot \frac{1}{x}\right) = x \cdot \left(-\frac{1}{x}\right) \in \mathbb{R}_{>0},$$

par la fermeture de $\mathbb{R}_{>0}$ sous la multiplication (l'Axiome 7.13(ii)). Mais cela contredit la Proposition 7.14. Donc, on doit avoir $\frac{1}{x} \in \mathbb{R}_{>0}$.

Pour l'autre implication, supposons que $x^{-1} = \frac{1}{x} \in \mathbb{R}_{>0}$. Alors, par ce qu'on vient de démontrer, $x = (x^{-1})^{-1} \in \mathbb{R}_{>0}$.

(ii) Soient $x, y \in \mathbb{R}_{>0}$ satisfaisant $x < y$. Alors $x^{-1}, y^{-1} \in \mathbb{R}_{>0}$ par la partie (i), et donc $x^{-1}y^{-1} \in \mathbb{R}_{>0}$ par la fermeture de $\mathbb{R}_{>0}$ sous la multiplication (Axiom 7.13(ii)). Ainsi, on obtient

$$x < y \implies x^{-1}y^{-1}x < x^{-1}y^{-1}y \implies y^{-1} < x^{-1},$$

où, dans la première implication, on a utilisé la Proposition 2.9(iii) pour $\mathbb{R}$.

□

Exemple 7.18. On va prouver que, pour tout $x \in \mathbb{R}$,

$$x^4 < 2x^5 \iff x > \frac{1}{2}. \tag{7.1}$$

On sépare la preuve en deux cas: $x = 0$ et $x \neq 0$.

Cas 1: Supposons que $x = 0$. Alors $x^4 = 0^4 = 0$ et $2x^5 = 2 \cdot 0^5 = 0$. Ainsi, l'énoncé $x^4 < 2x^5$ est faux car $0 \not< 0$. Étant donné que l'énoncé $0 > \frac{1}{2}$ est également faux, la double implication (7.1) est vraie.

Cas 2: Supposons que $x \neq 0$. Étant donné que $x^4 = (x^2)^2$, la Proposition 2.11 pour $\mathbb{R}$ implique que $x^4 \in \mathbb{R}_{>0}$. Ainsi, $(x^4)^{-1} \in \mathbb{R}_{>0}$ par la Proposition 7.17. Similairement, $\frac{1}{2} \in \mathbb{R}_{>0}$. Donc,

$$\begin{aligned} x^4 < 2x^5 &\implies (x^4)^{-1}x^4 < (x^4)^{-1}2x^5 && \text{(Proposition 2.9(iii) pour } \mathbb{R}) \\ &\implies 1 < 2x && \text{(Proposition 2.9(iii) pour } \mathbb{R}) \\ &\implies \frac{1}{2} \cdot 1 < \frac{1}{2} \cdot 2x && \text{(Proposition 2.9(iii) pour } \mathbb{R}) \\ &\implies \frac{1}{2} < x. \end{aligned}$$

Il reste à vérifier l'autre implication. Supposons que $x > \frac{1}{2}$. Ainsi, $x \in \mathbb{R}_{>0}$, et donc $x^4 \in \mathbb{R}_{>0}$ par la fermeture de $\mathbb{R}_{>0}$ sous la multiplication. On obtient

$$\begin{aligned} x > \frac{1}{2} &\implies 2x > 2 \cdot \frac{1}{2} && \text{(Proposition 2.9(iii) pour } \mathbb{R}) \\ &\implies 2x > 1 \\ &\implies x^4 \cdot 2x > x^4 \cdot 1 && \text{(Proposition 2.9(iii) pour } \mathbb{R}) \\ &\implies 2x^5 > x^4. \end{aligned}$$

Pour un usage ultérieur, on définit

$$\mathbb{R}_{\geq 0} := \mathbb{R}_{>0} \cup \{0\} = \{x \in \mathbb{R} : x \geq 0\}.$$

Exercices.

7.2.1 ([BG10, Prop. 8.41]). Soit $x \in \mathbb{R}$. Alors $x^2 < x^3$ si et seulement si $x > 1$.

7.2.2. Rappelez-vous que nous avons défini $2 := 1 + 1 \in \mathbb{Z}$. Démontrez qu'il n'existe pas d'entier $n \in \mathbb{Z}$ tel que $2n = 1$. Ainsi, contrairement à $\mathbb{R}$, l'ensemble $\mathbb{Z}$ des entiers admet des éléments non nuls qui n'ont pas d'inverse multiplicatif. *Indice*: Essayez une preuve par contradiction, en employant la Proposition 2.21.

7.2.3. Soient $x, y \in \mathbb{R}$. Démontrez que

$$xy \in \mathbb{R}_{>0} \iff (x, y \in \mathbb{R}_{>0}) \text{ ou } (-x, -y \in \mathbb{R}_{>0}).$$

7.2.4. Démontrez que, pour tout $x \in \mathbb{R}$,

$$x^2 - 4 > 0 \iff x < -2 \text{ ou } x > 2.$$

7.2.5. Soient $x, y \in \mathbb{R}$ avec $x \neq 0$. Démontrez que

$$\frac{y}{x} \in \mathbb{R}_{>0} \iff (x, y \in \mathbb{R}_{>0}) \text{ ou } (-x, -y \in \mathbb{R}_{>0}).$$

7.3 Les nombres réels par rapport aux entiers

Comme nous l'avons discuté antécédemment, les Axiomes 1.1–1.4 pour $\mathbb{Z}$ sont identiques aux Axiomes 7.1–7.4. Aussi, l'Axiome 2.1 et l'Axiome 7.13 sont identiques.

Toutefois, l'Axiome 1.5 (l'annulation) et l'Axiome 7.5 diffèrent. On a montré à la Proposition 7.11 que l'Axiome 7.5 implique l'Axiome 1.5 (en remplaçant $\mathbb{Z}$ par $\mathbb{R}$). Toutefois, l'implication inverse est fausse. Par exemple, l'entier 2 n'a pas d'inverse multiplicatif dans $\mathbb{Z}$. Ainsi, l'Axiome 7.5 n'est *pas* vrai si on remplace $\mathbb{R}$ par $\mathbb{Z}$. Cela établit une distinction entre $\mathbb{Z}$ et $\mathbb{R}$.

Une autre différence importante entre $\mathbb{Z}$ et $\mathbb{R}$ se rapporte à l'ordre. Par la Proposition 2.21, l'ensemble $\mathbb{N}$ des nombres naturels admet un plus petit élément, soit 1. L'énoncé correspondant pour $\mathbb{R}$ est faux. Avant de démontrer cela (le Théorème 7.20), on démontre un lemme.

Lemme 7.19. *On a* $0 < \frac{1}{2} < 1$.

Preuve. Puisque $2 = 1+1 \in \mathbb{R}_{>0}$ par la fermeture de $\mathbb{R}_{>0}$ sous l'addition (l'Axiome 7.13(i)), il s'ensuit de la Proposition 7.17(i) que $0 < \frac{1}{2}$. Puisque $2 - 1 = (1+1) - 1 = 1 \in \mathbb{R}_{>0}$, on a $1 < 2$. Donc, par la Proposition 7.17(ii), on a $\frac{1}{2} < \frac{1}{1} = 1$.

Preuve alternative: On peut également démontrer $\frac{1}{2} < 1$ par contradiction. Supposons que $1 \leq \frac{1}{2}$. Mais alors,

$$0 < 1 < 2 \quad \text{et} \quad 0 < 1 \leq \frac{1}{2}.$$

Par la Proposition 2.9(iii) pour $\mathbb{R}$, on a ensuite

$$1 \cdot 1 < 2 \cdot \frac{1}{2} \implies 1 < 1 \implies 0 = 1 - 1 \in \mathbb{R}_{>0},$$

ce qui contredit l'Axiome 7.13(iii). □

Théorème 7.20. *L'ensemble* $\mathbb{R}_{>0}$ *des nombres réels positifs n'admet pas de plus petit élément.*

Preuve. On démontre que pour tout $x \in \mathbb{R}_{>0}$, on peut toujours trouver un élément dans $\mathbb{R}_{>0}$ qui est plus petit. En effet, pour un $x > 0$, et par le Lemme 7.19, on a

$$0 < \frac{1}{2} < 1 \quad \text{et} \quad 0 < x \leq x.$$

Par la Proposition 2.9(iii) pour $\mathbb{R}$, on obtient

$$\frac{1}{2} \cdot x < x.$$

Toutefois, par la fermeture de $\mathbb{R}_{>0}$ sous la multiplication (l'Axiome 7.13(ii)), on a que $\frac{1}{2} \cdot x \in \mathbb{R}_{>0}$. Donc, $\mathbb{R}_{>0}$ n'admet pas de plus petit élément. □

Un autre différence importante entre $\mathbb{Z}$ et $\mathbb{R}$ se rapporte à "l'espace vide" entre les nombres. Les entiers admettent de tels espaces entre eux. Par exemple, par la Proposition 2.22, il n'y a pas d'entiers entre 0 et 1. Par contre, les nombres réels n'admettent pas de tels espaces, comme le théorème suivant l'indique.

Théorème 7.21. *Pour tous $x, y \in \mathbb{R}$ tels que $x < y$, il existe un $z \in \mathbb{R}$ tel que $x < z < y$.*

Preuve. Supposons que $x, y \in \mathbb{R}$ satisfont $x < y$. On va démontrer que $z = \frac{x+y}{2}$ satisfait $x < z < y$. Tout d'abord,

$$z - x = \frac{x+y}{2} - 1 \cdot x = \frac{x+y}{2} - \frac{1}{2} \cdot 2 \cdot x = \frac{1}{2}(x + y - 2x) = \frac{1}{2}(y - x) \in \mathbb{R}_{>0},$$

par la fermeture de $\mathbb{R}_{>0}$ sous la multiplication (l'Axiome 7.13(ii)), et sachant que $\frac{1}{2} \in \mathbb{R}_{>0}$ (par le Lemme 7.19) et $y - x \in \mathbb{R}_{>0}$ par hypothèse. Donc, $x < z$. Deuxièmement,

$$y - z = 1 \cdot y - \frac{x+y}{2} = \frac{1}{2} \cdot 2 \cdot y - \frac{x+y}{2} = \frac{1}{2}(2y - (x+y)) = \frac{1}{2}(y - x) \in \mathbb{R}_{>0},$$

et donc $z < y$. □

Le dernier axiome pour $\mathbb{Z}$, l'Axiome 2.17, n'admet pas d'énoncé correspondant pour $\mathbb{R}$. Toutefois, on va introduire un dernier axiome pour $\mathbb{R}$ qui n'a pas d'énoncé correspondant dans $\mathbb{Z}$.

Exercices.

7.3.1 ([BG10, Proj. 8.44]). Construisez un sous-ensemble $A \subseteq \mathbb{R}$ satisfaisant

(i) $1 \in A$ et

(ii) si $n \in A$, alors $n + 1 \in A$,

mais pour lequel $\mathbb{R}_{>0}$ n'est pas un sous-ensemble de A.

7.4 Bornes supérieures et inférieures

Avant d'introduire le dernier axiome pour $\mathbb{R}$, on commence avec des définitions.

Définition 7.22 (Ensemble borné, supremum, infimum)**.** Soit $A \subseteq \mathbb{R}$ tel que $A \neq \varnothing$.

(i) L'ensemble A est *majoré* s'il existe un $b \in \mathbb{R}$ tel que $\forall a \in A,\ a \leq b$. Un nombre réel b avec cette propriété est appelé un *majorant* de A.

(ii) L'ensemble A est *minoré* s'il existe un $b \in \mathbb{R}$ tel que $\forall a \in A,\ a \geq b$. Un nombre réel b avec cette propriété est appelé un *minorant* de A

(iii) L'ensemble A est *borné* s'il est minoré et majoré.

(iv) Une *borne supérieure*, ou *supremum*, de A est un majorant qui est plus petite ou égale à tout majorant de A.

(v) Une *borne inférieure*, ou *infimum*, de A est un minorant de A qui est plus grande ou égale à tout minorant de A.

On note que la terminologie en français et en anglais sont différentes pour ces notions. En anglais, on dit "upper bound" et "lower bound" pour ce qu'on a appelé ici majorant et minorant, ce qui se traduirait littéralement en français par "borne supérieure" et "borne inférieure". Il ne faut donc pas confondre avec les notions qu'on appellés borne supérieure et inférieure! Ces notions ce nomment "least upper bound" et "greatest lower bound" en anglais, c'est à dire "plus petites bornes supérieure" et "plus grande borne inférieure".

La prochaine proposition démontre que les supremums et infimums sont uniques, s'ils existent.

Proposition 7.23. *Soit A un sous-ensemble nonvide de $\mathbb{R}$.*

(i) Si x_1 et x_2 sont des bornes supérieures de A, alors $x_1 = x_2$.

(ii) Si x_1 et x_2 sont des bornes inférieures de A, alors $x_1 = x_2$.

Preuve. On démontre seulement la première partie de l'énoncé, étant donné que la preuve de la deuxième est similaire. Soient x_1 et x_2 des bornes supérieures de A. Alors, puisque x_1 est un majorant de A et x_2 est une borne supérieure, on a $x_2 \leq x_1$. Similairement, on as $x_1 \leq x_2$. Donc, $x_1 = x_2$. □

Pour un sous-ensemble non vide A de $\mathbb{R}$, la borne supérieure (le supremum) de A est dénoté par $\sup(A)$ (ou $\sup A$) et la borne inférieure (l'infimum) de A est dénoté par $\inf(A)$ (ou $\inf A$). Gardez à l'esprit que, pour un ensemble arbritraire non vide $A \subseteq \mathbb{R}$, $\inf A$ et/ou $\sup A$ peut ne pas exister, comme nous allons le voir.

Exemple 7.24. On va démontrer que $\inf \mathbb{R}_{>0} = 0$. Étant donné que $0 < x$ pour tout $x \in \mathbb{R}_{>0}$, alors 0 est minorant de R. Il reste à vérifier que 0 est la borne inférieure. On effectue cela par contradiction. Supposons que $y \in \mathbb{R}$ est un minorant de $\mathbb{R}_{>0}$ et que $0 < y$. Alors, par le Théorème 7.21, il existe un $z \in \mathbb{R}$ tel que $0 < z < y$. Mais alors, on a un $z \in \mathbb{R}_{>0}$ qui ne satisfait *pas* $y \leq z$. Cela contredit l'hypothèse que y est un minorant de $\mathbb{R}_{>0}$.

Exemple 7.25. On a $\inf \mathbb{R}_{\geq 0} = 0$. La preuve est pratiquement identique à celle de l'exemple 7.24.

Les exemples 7.24 et 7.25 illustre un point important: le supremum ou l'infimum d'un ensemble A (s'il existe) peut ou peut ne pas être un élément de A. De plus, les infimums et supremums n'existent pas toujours, comme l'exemple suivant l'illustre.

Proposition 7.26. *L'ensemble $\mathbb{R}_{>0}$ n'a pas de majorant.*

Preuve. On démontre cela par contradiction. Supposons que x est un majorant de $\mathbb{R}_{>0}$. Alors, puisque $1 \in \mathbb{R}_{>0}$ par la Proposition 7.14(ii), on obtient

$$x \geq 1 > 0 \implies x > 0 \implies x \in \mathbb{R}_{>0}.$$

Donc, $x + 1 \in \mathbb{R}_{>0}$ par la fermeture de $\mathbb{R}_{>0}$ sous l'addition (l'Axiome 7.13(i)). Étant donné que

$$(x + 1) - x = 1 \in \mathbb{R}_{>0},$$

alors on a $x + 1 > x$. Cela contredit notre hypothèse que x est un majorant de $\mathbb{R}_{>0}$. □

Exemple 7.27. Considérons l'ensemble

$$A = \{x^{-1} : x \in \mathbb{R}_{>0}\}.$$

Alors $\inf(A) = 0$. Pour démontrer cela, il suffit de constater que $A = \mathbb{R}_{>0}$. En effet, pour tout $y \in A$, on a un $x \in \mathbb{R}_{>0}$ tel que $y = x^{-1}$, et par la Proposition 7.17, on obtient $y \in \mathbb{R}_{>0}$. Vice-versa, pour tout $y \in \mathbb{R}_{>0}$, la Proposition 7.17 donne $y^{-1} \in \mathbb{R}_{>0}$, puis par le corollaire 7.8 et la définition de A, $y = (y^{-1})^{-1} \in A$. Finalement, par l'exemple 7.24, on a $\inf(A) = \inf(\mathbb{R}_{>0}) = 0$.

Exemple 7.28. Déterminons quel est le supremum de l'ensemble suivant

$$A = \left\{2 - \frac{3}{x} : x \in \mathbb{R}_{>0}\right\}.$$

En fait, il semble que 2 est un majorant de A est que c'est le plus petit, donc on va essayer de démontrer que c'est le cas, i.e. que

$$\sup A = 2.$$

Pour effectuer cela, on démontre tout d'abord que 2 est un majorant de A. En effet,

$$\begin{aligned}
x \in \mathbb{R}_{>0} &\implies x > 0 \\
&\implies \frac{1}{x} > 0 && \text{(Prop. 7.17(i))} \\
&\implies \frac{-3}{x} < 0 && \text{(Prop. 2.9(iv) pour } \mathbb{R}) \\
&\implies 2 - \frac{3}{x} < 2. && \text{(Prop. 2.9(i) pour } \mathbb{R})
\end{aligned}$$

Puisque tout élément de A est de la forme $2 - \frac{3}{x}$ pour un certain $x \in \mathbb{R}_{>0}$, l'argument ci-haut démontre que 2 est un majorant de A.

Maintenant, on doit montrer que 2 est la borne supérieure de A. Pour effectuer cela, on procède par contradiction. Supposons que A admet un majorant b avec $b < 2$. Donc, $2 - b \in \mathbb{R}_{>0}$. Pour obtenir une contradiction, on doit trouver un $x \in \mathbb{R}_{>0}$ tel que $2 - \frac{3}{x} > b$.

Notons que, pour tout $x \in \mathbb{R}_{>0}$,

$$\begin{aligned}
2 - \frac{3}{x} > b &\iff 2 - b > \frac{3}{x} \\
&\iff \frac{x}{3} > \frac{1}{2-b} && \text{(Prop. 7.17(ii) et } 2 - b \in \mathbb{R}_{>0}) \\
&\iff x > \frac{3}{2-b}. && \text{(Prop. 2.9(iii))}
\end{aligned}$$

Or, on a que $(2-b)^{-1} \in \mathbb{R}_{>0}$ et $3 \in \mathbb{R}_{>0}$, donc $\frac{3}{2-b} \in \mathbb{R}_{>0}$. Par la Proposition 7.26, $\mathbb{R}_{>0}$ n'admet pas de majorant, donc il existe un $x \in \mathbb{R}$ tel que $x > \frac{3}{2-b}$ (et donc $x \in \mathbb{R}_{>0}$). Alors, en remontant la chaîne des doubles implications ci-haut pour ce x, on a que $2 - \frac{3}{x} > b$. Donc, b n'est pas un majorant de A, ce qui contredit notre hypothèse sur b.

Exemple 7.29. On démontre que l'ensemble

$$A = \left\{ 2 - \frac{3}{x} : x \in \mathbb{R}_{>0} \right\}.$$

de l'exemple 7.28 n'admet pas de minorant, et donc pas d'infimum. On démontre cela pas contradiction. Supposons que b est un minorant de A. Alors, en particulier, on a que $b \leq 2 - \frac{3}{4} < 2$. Donc

$$\begin{aligned} & b \leq 2 - \frac{3}{x} \quad \text{pour tout } x \in \mathbb{R}_{>0} \\ \implies & \frac{3}{x} \leq 2 - b \quad \text{pour tout } x \in \mathbb{R}_{>0} \\ \implies & \frac{3}{2-b} \leq x \quad \text{pour tout } x \in \mathbb{R}_{>0}. \qquad (\text{car } x \in \mathbb{R}_{>0},\ 2-b \in \mathbb{R}_{>0}) \end{aligned}$$

Toutefois, puisque $\frac{3}{2-b} > 0$, on peut trouver un $x \in \mathbb{R}_{>0}$ tel que $x < \frac{3}{2-b}$ par le Théorème 7.20. Cela nous donne une contradiction, tel que souhaité.

Exemples 7.30. (i) L'ensemble $\{x \in \mathbb{R} : x < 0\}$ a un supremum 0, mais pas d'infimum.

(ii) L'ensemble $\{x \in \mathbb{R} : x \leq 0\}$ a un supremum 0, mais pas d'infimum.

(iii) L'ensemble $\mathbb{R}$ n'a ni de supremum, ni d'infimum.

(iv) L'ensemble $\{x \in \mathbb{R} : 0 \leq x \leq 1\}$ a un infimum 0 et un supremum 1.

(v) L'ensemble $\{x \in \mathbb{R} : 0 < x \leq 1\}$ a un infimum 0 et un supremum 1.

(vi) L'ensemble $\{x \in \mathbb{Z} : 0 < x\}$ a un infimum 1, mais pas de supremum. (Techniquement parlant, on n'a pas définit les infimums et supremums pour des sous-ensembles de $\mathbb{Z}$, mais la définition est la même. De plus, on va discuter à la Section 8.2 comment on peut voir $\mathbb{Z}$ comme un sous-ensemble de $\mathbb{R}$.)

Définition 7.31 (Maximum, minimum)**.** Supposons que $A \subseteq \mathbb{R}$.

(i) Un élément $b \in A$ est le *maximum* ou *plus grand élément* de A si $\forall a \in A,\ a \leq b$. Dans ce cas, on écrit $b = \max(A)$.

(ii) Un élément $b \in A$ est le *minimum* ou *plus petit élément* de A si $\forall a \in A,\ b \leq a$. Dans ce cas, on écrit $b = \min(A)$.

Notez la différence importante entre la Définition 7.31 et les parties (i) et (ii) de la Définition 7.22. Dans la définition des minorant et majorant, ce sont des éléments quelconques de $\mathbb{R}$, mais dans la Définition 7.31, le maximum/minimum est un élément de l'ensemble A lui-même.

Proposition 7.32. *Supposons que $A \subseteq \mathbb{R}$ est non vide.*

(i) Si A admet un supremum et que $\sup(A) \in A$*, alors A admet un plus grand élément et* $\sup(A) = \max(A)$*. Réciproquement, si A admet un plus grand élément, alors A admet un supremum,* $\max(A) = \sup(A)$*, et* $\sup(A) \in A$*.*

(ii) Si A admet un infimum et que $\inf(A) \in A$*, alors A admet un plus petit élément et* $\inf(A) = \min(A)$*. Réciproquement, si A admet un plus petit élément, alors A admet un infimum,* $\min(A) = \inf(A)$*, et* $\inf(A) \in A$*.*

Preuve. On va démontrer le premier énoncé, la preuve du deuxième étant similaire. Supposons que A admet un supremum b et que $b \in A$. Alors, par la définition du supremum, on a $\forall a \in A,\ a \leq b$. Donc, $b = \max(A)$.

Réciproquement, supposons que A admet un plus grand élément b. Alors $b \in A$ et $\forall a \in A,\ a \leq b$. Donc, b est un majorant de A. Il reste à vérifier que b est la borne supérieure de A. Or, si M est un majorant de A, alors on a automatiquement $b \leq M$ car $b \in A$. Ainsi, b est la borne supérieure de A, i.e. $b = \sup(A)$. Donc, $\sup(A) = b = \max(A) \in A$. □

La Proposition 7.32 nous dit essentiellement qu'un plus grand élément de A est simplement un supremum de A qui est contenu dans A. Similairement, un plus petit élément de A est simplement un infimum de A qui est contenu dans A. Il s'ensuit de cela et la Proposition 7.23 qu'un plus grand ou plus petit élément, s'il existe, est unique.

Exemple 7.33. Considérons l'ensemble the set

$$A = \left\{ 2 - \frac{3}{x} : x \in \mathbb{R}_{>0} \right\}.$$

des exemples 7.28 et 7.29.

On a démontré à l'exemple 7.28 que $\sup A = 2$. Par la Proposition 7.32(i), si A avait un plus grand élément, ce serait 2. Mais $2 \notin A$ puisque, à l'exemple 7.28, on a vu que tout élément de A est strictement plus petit que 2. Donc, A n'a pas de plus grand élément.

De plus, à l'exemple 7.29 on a vu que A n'a pas d'infimum. Donc, par la Proposition 7.32(ii), il s'ensuit que A n'a pas de plus petit élément.

Exemples 7.34. Analysons les ensembles des exemples 7.30 à nouveau.

(i) L'ensemble $\{x \in \mathbb{R} : x < 0\}$ n'a ni de maximum, ni de minimum.

(ii) L'ensemble $\{x \in \mathbb{R} : x \leq 0\}$ a un maximum 0 et aucun minimum.

(iii) L'ensemble $\mathbb{R}$ n'a ni de maximum, ni de minimum..

(iv) L'ensemble $\{x \in \mathbb{R} : 0 \leq x \leq 1\}$ a un minimum 0 et un maximum 1.

(v) L'ensemble $\{x \in \mathbb{R} : 0 < x \leq 1\}$ a un maximum 1 et aucun minimum.

Voici notre dernier axiome pour les nombres réels.

Axiome 7.35 (Axiome de complétude)**.** Tout sous-ensemble non vide de $\mathbb{R}$ qui est majoré admet une borne supérieure.

Proposition 7.36. *Supposons que $A \subseteq B \subseteq \mathbb{R}$, que A et B sont non vides, et que B est majoré. Alors* $\sup(A) \leq \sup(B)$.

Preuve. Puisque B est majoré et que $A \subseteq B$, on sait que A est également majoré. Ainsi, par l'Axiome 7.35, $\sup(A)$ et $\sup(B)$ existent. Par définition, on a $b \leq \sup(B)$ pour tout $b \in B$. Puisque $A \subseteq B$, cela implique que $a \leq \sup(B)$ pour tout $a \in A$. Ainsi, $\sup(B)$ est un majorant de A. Mais $\sup(A)$ est la borne supérieure de A, donc $\sup(A) \leq \sup(B)$. □

On définit maintenant les *intervalles*. Pour $x, y \in \mathbb{R}$, on définit

$$\begin{aligned}
[x, y] &:= \{z \in \mathbb{R} : x \leq z \leq y\}, \\
(x, y] &:= \{z \in \mathbb{R} : x < z \leq y\}, \\
[x, y) &:= \{z \in \mathbb{R} : x \leq z < y\}, \\
(x, y) &:= \{z \in \mathbb{R} : x < z < y\}, \\
(-\infty, y] &:= \{z \in \mathbb{R} : z \leq y\}, \\
(-\infty, y) &:= \{z \in \mathbb{R} : z < y\}, \\
[x, \infty) &:= \{z \in \mathbb{R} : x \leq z\}, \\
(x, \infty) &:= \{z \in \mathbb{R} : x < z\}, \\
(-\infty, \infty) &:= \mathbb{R}.
\end{aligned}$$

Remarque 7.37. (i) Notez que ∞ et $-\infty$ ne sont *pas* des nombres réels. On ne fait qu'employer ces symboles dans la notation.

(ii) Le texte [BG10] requiert que $x < y$ pour les intervalles ci-haut. Toutefois, cela n'est pas nécessaire. Par exemple, quand $x = y$, on a

$$[x, x] = \{x\}, \quad [x, x) = (x, x] = (x, x) = \varnothing,$$

et quand $x > y$, on a

$$[x, y] = [x, y) = (x, y] = (x, y) = \varnothing,$$

(iii) On emploie la même notation pour l'intervalle (x, y) et pour le point $(x, y) \in \mathbb{R}^2$, donc il y a un risque de confusion. Or, il devrait être clair selon le contexte si l'on se réfère à un intervalle ou à un point dans $\mathbb{R}^2$.

Proposition 7.38. *Tout sous-ensemble non vide de $\mathbb{R}$ qui est minoré admet une borne inférieure.*

Preuve. Supposons que A est un sous-ensemble non vide de $\mathbb{R}$ qui est minoré. Alors, il existe un $m \in \mathbb{R}$ tel que $\forall x \in A,\ m \leq x$. Définissons

$$B = \{-x : x \in A\}.$$

On démontre que B est majoré par $-m$. En effet,

$$x \in B \implies -x \in A \implies m \leq -x \implies x \leq -m.$$

Ainsi, $\forall x \in B, x \leq -m$, comme souhaité. Donc, par l'Axiome 7.35, B a une borne supérieure y.

On démontre que $-y$ est la borne inférieure de A. Puisque

$$x \in A \implies -x \in B \implies -x \leq y \implies x \geq -y,$$

on peut voir que $-y$ est un minorant de A. Il reste à vérifier que $-y$ est la borne inférieure de A. Supposons que z est un minorant de A. Alors, comme ci-haut, $-z$ est un majorant de B. Puisque y est la borne supérieure de B, on a $y \leq -z$. Donc $-y \geq z$. Ainsi, $-y$ est la borne inférieure de A. □

Exercices.

7.4.1. Supposons que $A \subseteq \mathbb{R}$ admet un supremum M. Démontrez que l'ensemble

$$B = \{5 - 2x : x \in A\}$$

admet l'infimum $5 - 2M$.

7.4.2. Soient A et B des sous-ensembles non vides de $\mathbb{R}$ qui sont majorés. De plus, supposons que $A \cap B \neq \varnothing$. Démontrez que $A \cap B$ est majoré et que

$$\sup(A \cap B) \leq \min\{\sup A, \sup B\}.$$

7.4.3. Supposons que A est un sous-ensemble de $\mathbb{R}$ admettant un maximum et un minimum, tel que $\max A = \min A$. Démontrez que A contient exactement un élément.

7.4.4. Soient $a, b \in \mathbb{R}$ avec $a < b$. Prouvez que

$$\inf(a, b) = a \quad \text{et} \quad \sup(a, b) = b.$$

(Rappel: $(a, b) = \{x \in \mathbb{R} : a < x < b\}$.)

7.4.5. Déterminez le supremum et l'infimum de l'ensemble

$$\{x \in \mathbb{R} : x^2 < 4\}$$

ou démontrez qu'ils n'existent pas.

Chapitre 8

Injections, surjections et bijections

Dans ce chapitre, nous allons examiner certains types importants de fonctions. Plus spécifiquement, on va étudier les fonctions qui sont injectives, surjectives, ou les deux. On abordera ensuite comment l'ensemble des entiers peut être vu comme un sous-ensemble des nombres réels, de telle manière à préserver les opérations et relations importantes définies antécédemment.

8.1 Injections, surjections et bijections

Définition 8.1 (Injective, injection)**.** Une fonction $f\colon A \to B$ est dite *injective* (ou une *injection*, ou *une-à-une*) si

$$\forall x, y \in A.\ (x \neq y \implies f(x) \neq f(y)).$$

De manière équivalente (avec sa contraposée) f est injective si

$$\forall x, y \in A.\ (f(x) = f(y) \implies x = y).$$

Exemple 8.2. Pour $c \in \mathbb{R}$, $c \neq 0$, la fonction

$$f\colon \mathbb{R} \to \mathbb{R}, \quad f(x) = cx,$$

est injective. Pour démontrer cela, prenons des $x, y \in \mathbb{R}$. Alors

$$f(x) = f(y) \implies cx = cy \implies x = y,$$

où la dernière implication suit de la Proposition 7.11 (ou bien, il suffit de multiplier les deux côtés par c^{-1}). Ainsi, f est injective.

Exemple 8.3. La fonction

$$f\colon \mathbb{R} \to \mathbb{R}, \quad f(x) = x^2,$$

n'est *pas* injective. Pour prouver cela, il suffit de trouver deux éléments x et y du domaine tels que $x \neq y$ et $f(x) = f(y)$. En fait, en prenant $x = 1$ et $y = -1$, on obtient $1 \neq -1$, mais $f(1) = 1 = f(-1)$. Donc, f n'est pas injective.

Définition 8.4 (Surjective, surjection, image)**.** Une fonction $f\colon A \to B$ est dite *surjective* (ou une *surjection*) si

$$\forall b \in B.\ \exists a \in A \text{ tel que } f(a) = b.$$

Pour tout sous-ensemble $S \subseteq A$, l'*image de S par f* est l'ensemble

$$f(S) := \{f(a) : a \in S\} \subseteq B.$$

L'*image* de f est $f(A)$. En d'autres mots, l'image de f est l'image du domaine de f par f. Ainsi, f est surjective si et seulement si $f(A) = B$ (i.e. l'image de f est égale au codomaine de f).

Exemple 8.5. La fonction

$$f\colon \mathbb{Z} - \{0\} \to \mathbb{N}, \quad f(x) = |x|,$$

est surjective; il suffit de constater que pour tout $x \in \mathbb{N}$, on a $x \in \mathbb{Z} - \{0\}$ et $f(x) = |x| = x$.

Définition 8.6 (Bijective, bijection)**.** Une fonction *bijective* (ou une *bijection*) si elle est à la fois injective et surjective.

Exemple 8.7. Pour tout ensemble non vide A, on a la *fonction identité*

$$\mathrm{id}_A\colon A \to A, \quad \mathrm{id}_A(a) = a \text{ pour tout } a \in A.$$

Cette fonction est bijective.

Exemple 8.8. Considérons la fonction

$$f\colon \mathbb{R} \to \mathbb{R}, \quad f(x) = \frac{x}{3} + 1.$$

On va démontrer que cette fonction bijective. Soient $x, y \in \mathbb{R}$. Alors

$$f(x) = f(y) \implies \frac{x}{3} + 1 = \frac{y}{3} + 1 \implies \frac{x}{3} + 1 - 1 = \frac{y}{3} + 1 - 1$$
$$\implies \frac{x}{3} = \frac{y}{3} \implies 3 \cdot \frac{x}{3} = 3 \cdot \frac{y}{3} \implies x = y.$$

Donc, f est injective.

Il suffit de vérifier que f est surjective. Prenons un $y \in \mathbb{R}$ (le codomaine). On veut trouver un $x \in \mathbb{R}$ (le domaine) tel que $f(x) = y$. Notons que, pour tout $x \in \mathbb{R}$,

$$f(x) = y \implies \frac{x}{3} + 1 = y \implies x = 3(y - 1).$$

Mais puisque $3(y-1) \in \mathbb{R}$ (par la fermeture de $\mathbb{R}$ sous l'add. et la mult.), on peut essayer $x = 3(y-1)$, qui est dans le domaine de f. En effet, pour ce x, on obtient

$$f\big(3(y-1)\big) = \frac{3(y-1)}{3} + 1 = y - 1 + 1 = y.$$

Ainsi, f est surjective.

Exemples 8.9. (i) La fonction $f\colon \{0\} \to \{2, 5, -4\}$ donnée par $f(0) = -4$, est injective, mais pas surjective.

(ii) La fonction $f\colon \{1, 2\} \to \{1\}$ donnée par $f(1) = f(2) = 1$ est surjective, mais pas injective.

(iii) La fonction $f\colon \{1, 2\} \to \{1, 8\}$ donnée par $f(1) = f(2) = 8$ n'est ni surjective, ni injective.

(iv) La fonction $f\colon \{-1, 1\} \to \{-2, 13\}$ donnée par $f(-1) = -2$, $f(1) = 13$ est bijective.

(v) La fonction $f\colon \mathbb{Z} \to \mathbb{Z}_{\geq 0}$, $f(n) = n^2$, n'est pas injective car, par exemple $f(1) = 1 = f(-1)$. Elle n'est pas surjective non plus puisque, par exemple, il n'y a pas de $n \in \mathbb{Z}$ tel que $f(n) = 3$.

(vi) La fonction $f\colon \mathbb{Z}_{\geq 0} \to \mathbb{Z}_{\geq 0}$, $f(n) = n^2$, est injective, mais pas surjective.

(vii) La fonction $f\colon \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$, $f(x) = 3x$, est bijective.

(viii) La fonction $f\colon \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$, $f(x) = 3x + 1$ est injective, mais pas surjective. (Par exemple, son image ne contient pas 0.)

Si $f\colon A \to B$ et $g\colon B \to C$, alors leur *composition* est une fonction

$$g \circ f\colon A \to C, \quad (g \circ f)(a) = g(f(a)) \text{ pour tout } a \in A.$$

Exemple 8.10. Définissons

$$f\colon \{1, 2, 3\} \to \{2, 4\}, \quad f(1) = f(2) = 4,\ f(3) = 2,$$
$$g\colon \{2, 4\} \to \{1, 8, 10\}, \quad g(2) = 8,\ g(4) = 10.$$

Alors

$$g \circ f\colon \{1, 2, 3\} \to \{1, 8, 10\}$$

est donnée pas

$$(g \circ f)(1) = g(f(1)) = g(4) = 10,$$
$$(g \circ f)(2) = g(f(2)) = g(4) = 10,$$
$$(g \circ f)(3) = g(f(3)) = g(2) = 8.$$

Exemple 8.11. Soit $f\colon A \to B$. Alors

$$\mathrm{id}_B \circ f = f \quad \text{et} \quad f \circ \mathrm{id}_A = f.$$

Proposition 8.12. *Soient $f\colon A \to B$ et $g\colon B \to C$ (et donc $g \circ f\colon A \to C$).*

(i) Si f et g sont toutes les deux injectives, alors $g \circ f$ est injective.

(ii) Si f et g sont toutes les deux surjectives, alors $g \circ f$ est surjective.

(iii) Si f et g sont toutes les deux bijectives, alors $g \circ f$ est bijective.

Preuve. (i) Supposons que f et g sont toutes les deux injectives. Alors, pour tous $a_1, a_2 \in A$, on a

$$\begin{aligned} & (g \circ f)(a_1) = (g \circ f)(a_2) \\ \implies\ & g(f(a_1)) = g(f(a_2)) \\ \implies\ & f(a_1) = f(a_2) && \text{car } g \text{ est injective} \\ \implies\ & a_1 = a_2. && \text{car } f \text{ est injective} \end{aligned}$$

(ii) Supposons que f et g sont toutes les deux surjectives. Prenons un $c \in C$. Puisque g est surjective, alors il existe un $b \in B$ tel que $g(b) = c$. Puis f est surjective, donc il existe un $a \in A$ such that $f(a) = b$. On obtient

$$(g \circ f)(a) = g(f(a)) = g(b) = c.$$

Ainsi, pour tout $c \in C$, il existe un $a \in A$ tel que $(g \circ f)(a) = c$. Donc, $g \circ f$ est surjective.

(iii) Cela suit des deux parties précédentes, et de la définition de la bijectivité. □

Définition 8.13 (Fonctions inverses)**.** Soit $f \colon A \to B$.

(i) Un *inverse à gauche* de f est une fonction $g \colon B \to A$ telle que

$$g \circ f = \mathrm{id}_A.$$

(ii) Un *inverse à droite* de f est une function $g \colon B \to A$ telle que

$$f \circ g = \mathrm{id}_B.$$

(iii) Un *inverse* de f est une fonction qui est à la fois un inverse à gauche et un inverse à droite de f.

Exemple 8.14. Considérez les fonctions

$$\begin{aligned} f \colon \mathbb{Z}_{\geq 0} \to \mathbb{Z}, \quad f(x) = x, \\ g \colon \mathbb{Z} \to \mathbb{Z}_{\geq 0}, \quad g(x) = |x|. \end{aligned}$$

Alors, pour tout $x \in \mathbb{Z}_{\geq 0}$, on a

$$(g \circ f)(x) = g(f(x)) = g(x) = |x| = x.$$

Donc

$$g \circ f = \mathrm{id}_{\mathbb{Z}_{\geq 0}},$$

et donc g est un inverse à gauche de f et f est un inverse à droite de g. Toutefois, $f \circ g \neq \mathrm{id}_{\mathbb{Z}}$ puisque, par exemple

$$(f \circ g)(-1) = f(g(-1)) = f(1) = 1 \neq -1 = \mathrm{id}_{\mathbb{Z}}(-1).$$

Ainsi, g n'est *pas* un inverse à droite de f et f n'est *pas* un inverse à gauche de g.

Exemple 8.15. Considérez les fonctions

$$f\colon \mathbb{R} \to \mathbb{R}, \quad f(x) = 3x + 1,$$
$$g\colon \mathbb{R} \to \mathbb{R}, \quad g(x) = \frac{x-1}{3}.$$

Alors

$$f \circ g = \mathrm{id}_{\mathbb{R}} \quad \text{et} \quad g \circ f = \mathrm{id}_{\mathbb{R}}.$$

Ainsi, f est un inverse de g et g est un inverse de f.

Proposition 8.16. *Soit f une fonction.*

(i) La fonction f est injective si et seulement si f admet un inverse à gauche.

(ii) La fonction f est surjective si et seulement si f admet un inverse à droite.

(iii) La fonction f est bijective si et seulement si f admet un inverse.

Preuve. (i) Supposons que $f\colon A \to B$ est injective. Fixons un $a_0 \in A$ et définissons $g\colon B \to A$ par

$$g(b) = \begin{cases} a & \text{si } b \text{ est dans l'image de } f \text{ et } f(a) = b, \\ a_0 & \text{autrement.} \end{cases}$$

La fonction g est bien définie car f est injective, i.e. si b est dans l'image de f, il y a *exactement un* $a \in A$ tel que $f(a) = b$. Il s'ensuit de notre construction que $g \circ f = \mathrm{id}_A$, et donc g est un inverse à gauche de f.

Réciproquement, supposons que $f\colon A \to B$ admet un inverse à gauche $g\colon B \to A$. Alors, pour tous $a_1, a_2 \in A$, on a

$$f(a_1) = f(a_2) \implies g(f(a_1)) = g(f(a_2)) \implies (g \circ f)(a_1) = (g \circ f)(a_2)$$
$$\implies \mathrm{id}_A(a_1) = \mathrm{id}_A(a_2) \implies a_1 = a_2.$$

Ainsi, f est injective.

(ii) Supposons que $f\colon A \to B$ est surjective. On définit une fonction $g\colon B \to A$ comme suit: pour tout $b \in B$, on choisit un $a \in A$ tel que $f(a) = b$ (et on peut faire cela car f est surjective) et on définit $g(b) = a$. Puis, pour tout $b \in B$, on obtient

$$(f \circ g)(b) = f(g(b)) = f(a) = b,$$

et donc g est un inverse à droite de f.

Réciproquement, supposons que $f\colon A \to B$ admet un inverse à droite $g\colon B \to A$. Alors, pour tout $b \in B$, on a

$$f(g(b)) = (f \circ g)(b) = \mathrm{id}_B(b) = b,$$

et donc b est dans l'image de f. Puisque b était arbitraire, cela prouve que f est surjective.

(iii) Supposons que $f\colon A \to B$ est bijective. On peut définir une fonction $g\colon B \to A$ comme suit: pour chaque b, il existe exactement un $a \in A$ tel que $f(a) = b$ (puisque f est bijective). On définit $g(b) = a$. Ainsi, par construction, $(f \circ g)(b) = b$ pour tout $b \in B$, et $(g \circ f)(a) = a$ pour tout $a \in A$. Donc, g est un inverse de f.

Réciproquement, supposons que f admet un inverse. Alors f est injective par (i) et surjective par (ii). Donc, f est bijective. □

Proposition 8.17. *Si une fonction est bijective, alors son inverse est unique.*

Preuve. Supposons que $f\colon A \to B$ est bijective et que $g\colon B \to A$ et $h\colon B \to A$ sont des inverses de f. Alors

$$g = g \circ \mathrm{id}_B = g \circ f \circ h = \mathrm{id}_A \circ h = h. \qquad \square$$

Proposition 8.18. *Soient A et B des ensembles. Il existe une injection de A vers B si et seulement si il existe une surjection de B vers A.*

Preuve. Supposons que $f\colon A \to B$ est une injection. Alors, par la Proposition 8.16(i), f admet un inverse à gauche $g\colon B \to A$. Donc

$$g \circ f = \mathrm{id}_A. \tag{8.1}$$

Cela implique que g admet un inverse à droite, et donc g est surjective par la Proposition 8.16(ii). De manière similaire, si $g\colon B \to A$ est surjective, alors g admet un inverse à droite $f\colon A \to B$ satisfaisant (8.1). Donc, f admet un inverse à gauche, et donc f est injective. □

Exercices.

8.1.1. Définissons la fonction suivante

$$g\colon \mathbb{R}_{\geq 0} \to \mathbb{R}, \quad g(x) = -3x + 4.$$

(i) Démontrez que g est injective.

(ii) Quel est l'image de g? Écrivez votre réponse sous forme d'intervalle et justifiez votre réponse.

(iii) Est-ce que g est surjective?

8.1.2. Considérez la fonction

$$f\colon \mathbb{R} \to \mathbb{R}_{\geq 0}, \quad f(x) = |2x + 3|.$$

(i) Est-ce que f est injective? Justifiez votre réponse.

(ii) Est-ce que f est surjective? Justifiez votre réponse.

(iii) Est-ce que f admet un inverse à gauche? Si oui, donnez un tel inverse et démontrez qu'il s'agit bien d'un inverse à gauche. Si non, justifiez pourquoi f n'a pas d'inverse à gauche.

(iv) Est-ce que f admet un inverse à droite? Si oui, donnez un tel inverse et démontrez qu'il s'agit bien d'un inverse à droite. Si non, justifiez pourquoi f n'a pas d'inverse à droite.

8.1.3. Considérez la fonction

$$f\colon \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}, \quad f(x) = \frac{x}{3} + 1.$$

(i) Est-ce que f est injective? Justifiez votre réponse..

(ii) Est-ce que f est surjective? Justifiez votre réponse.

(iii) Est-ce que f admet un inverse à gauche? Si oui, donnez un tel inverse et démontrez qu'il s'agit bien d'un inverse à gauche. Si non, justifiez pourquoi f n'a pas d'inverse à gauche.

(iv) Est-ce que f admet un inverse à droite? Si oui, donnez un tel inverse et démontrez qu'il s'agit bien d'un inverse à droite. Si non, justifiez pourquoi f n'a pas d'inverse à droite.

8.1.4. (i) Supposons que $f\colon A \to B$ et $g\colon B \to C$ sont des fonctions, et que g est surjective. Est-il vrai que $g \circ f$ est surjective? Si oui, donnez une preuve. Si non, donnez un contre-exemple.

(ii) Supposons que $f\colon A \to B$ et $g\colon B \to C$ sont des fonctions, et que f est injective. Est-il vrai que $g \circ f$ est injective? Si oui, donnez une preuve. Si non, donnez un contre-exemple.

(iii) Supposons que $f\colon A \to B$ et $g\colon B \to C$ sont des fonctions telles que $g \circ f$ est injective. Est-il vrai que f est injective? Si oui, donnez une preuve. Si non, donnez un contre-exemple.

(iv) Supposons que $f\colon A \to B$ et $g\colon B \to C$ sont des fonctions telles que $g \circ f$ est surjective. Est-il vrai que g est surjective? Si oui, donnez une preuve. Si non, donnez un contre-exemple.

8.1.5. Soient A et B des sous-ensembles non vides de $\mathbb{R}$, et une fonction $f\colon A \to B$ satisfaisant

$$\forall a_1, a_2 \in A.\ \big(a_1 < a_2 \implies f(a_1) < f(a_2)\big).$$

(Une telle fonction est dite *strictement croissante.*) Démontrez que f est injective.

8.1.6. (i) Donnez un exemple de fonctions avec deux inverses à gauche différents.

(ii) Donnez un exemple de fonctions avec deux inverses à droite différents.

8.1.7. (i) Supposons que $f\colon A \to B$ et $g\colon B \to C$ ont des inverses à gauche. Démontrez que $g \circ f$ à un inverse à gauche.

(ii) Supposons que $f\colon A \to B$ et $g\colon B \to C$ ont des inverses à droite. Démontrez que $g \circ f$ à un inverse à droite.

(iii) Supposons que $f\colon A \to B$ et $g\colon B \to C$ ont des inverses. Démontrez que $g \circ f$ a un inverse.

8.2 Plongement de $\mathbb{Z}$ dans $\mathbb{R}$

On a introduit l'ensemble $\mathbb{Z}$ des entiers et l'ensemble $\mathbb{R}$ des nombres réels axiomatiquement. Ainsi, on a supposé qu'il existe des ensembles avec des opérations binaires d'addition et de multiplication satisfaisant certains axiomes. En raison de cette approche, il n'y a pas *à priori* de connexion entre $\mathbb{Z}$ et $\mathbb{R}$. Par exemple, l'élément neutre additif de $\mathbb{Z}$ n'est pas lié à l'élément neutre additif de $\mathbb{R}$ (et de même pour les éléments neutres multiplicatifs). Pour cette raison, dans cette section, on dénotera les éléments neutres de l'addition et la multiplication pour $\mathbb{Z}$ par $0_{\mathbb{Z}}$ et $1_{\mathbb{Z}}$, et ceux de $\mathbb{R}$ par $0_{\mathbb{R}}$ et $1_{\mathbb{R}}$.

On va maintenant aborder brièvement comment on comment on peut voir $\mathbb{Z}$ comme un sous-ensemble de $\mathbb{R}$, de telle manière à respecter les opérations d'addition et de multiplication. Pour plus de details, vous pouvez consulter [BG10, §9.2].

Définition 8.19 (Plongement de $\mathbb{Z}$ dans $\mathbb{R}$)**.** On définit une fonction $e\colon \mathbb{Z} \to \mathbb{R}$ comme suit:

(i) Premièrement, on définit e sur $\mathbb{Z}_{\geq 0}$ récursivement. On définit $e(0_{\mathbb{Z}}) = 0_{\mathbb{R}}$ et, supposant que $e(n)$ soit défini pour un certain $n \in \mathbb{Z}_{\geq 0}$, on pose

$$e(n + 1_{\mathbb{Z}}) := e(n) + 1_{\mathbb{R}}.$$

(ii) Puis, on définit e sur les entiers négatifs. Pour $k \in \mathbb{Z}$ avec $k < 0$, on pose

$$e(k) := -e(-k).$$

Proposition 8.20. *La fonction $e\colon \mathbb{Z} \to \mathbb{R}$ de la Définition 8.19 a les propriétés suivantes.*

(i) $e(1_{\mathbb{Z}}) = 1_{\mathbb{R}}$.

(ii) Pour tout $k \in \mathbb{Z}$, $e(-k) = -e(k)$. (La fonction e préserve les inverses additifs.)

(iii) Pour tous $m, k \in \mathbb{Z}$, on a $e(m+k) = e(m) + e(k)$. (La fonction e préserve l'addition.)

(iv) Pour tous $m, k \in \mathbb{Z}$, on a $e(mk) = e(m)e(k)$. (La fonction e préserve la multiplication.)

(v) Pour tous $m, k \in \mathbb{Z}$, on a $m < k \iff e(m) < e(k)$. (La fonction e préserve l'ordre.)

(vi) e est injective.

Preuve. Voir [BG10, §9.2]. □

Par la Proposition 8.20, l'image $e(\mathbb{Z})$ de e est un sous-ensemble de $\mathbb{R}$ qui se comporte exactement comme $\mathbb{Z}$. En d'autres mots, e est une bijection entre $\mathbb{Z}$ et un sous-ensemble de $\mathbb{R}$, et cette bijection préserve l'addition, la multiplication, les inverses additifs et l'ordre. Ainsi, à partir de maintenant, on va identifier $\mathbb{Z}$ avec son image, i.e. le sous-ensemble de $\mathbb{R}$ identifiant $n \in \mathbb{Z}$ avec $e(n) \in \mathbb{R}$. De cette façon, on verra $\mathbb{Z}$ directement comme un sous-ensemble de $\mathbb{R}$.

Chapitre 9

Limites

Dans ce chapitre, on introduit et on développe le concept d'une *limite*. C'est un concept crucial en mathématique, particulièrement dans le domaine de l'*analyse*, lequel intègre le calcul différentiel et intégral. Quoique les limites sont souvent traitées de manière intuitive dans les cours de calcul, on travaillera ici avec la définition précise.

9.1 $\mathbb{Z}$ non borné dans $\mathbb{R}$

À la Proposition 2.7, on a vu que $\mathbb{N}$ n'admet pas de plus grand élément. Toutefois, cela n'implique pas immédiatement que $\mathbb{N}$ n'est pas majpré comme sous-ensemble de $\mathbb{R}$, puisqu'on n'a pas encore éliminé la possibilité d'avoir un nombre réel plus grand que tous les nombres naturels.

Proposition 9.1. *L'ensemble $\mathbb{N}$ des nombres naturels, considéré comme un sous-ensemble de $\mathbb{R}$, n'est pas majoré.*

Preuve. On prouve cela par contradiction. Supposons que $\mathbb{N}$ est majoré. Alors, par l'Axiome 7.35, $\mathbb{N}$ admet une borne supérieure u. Considérons l'intervalle

$$\left(u - \frac{1}{2}, u\right] = \left\{x \in \mathbb{R} : u - \frac{1}{2} < x \leq u\right\}.$$

Si cet intervalle ne contenait pas de nombres naturels, alors $u - \frac{1}{2}$ serait un majorant de $\mathbb{N}$, contredisant notre hypothèse que u est la borne supérieure. Donc, il existe un $n \in \mathbb{N}$ tel que $n \in (u - \frac{1}{2}, u]$. Ainsi

$$u - \frac{1}{2} < n \implies u < n + \frac{1}{2} < n + 1.$$

Toutefois, $n + 1 \in \mathbb{N}$, car $1 \in \mathbb{N}$ (par la Proposition 2.4) et $\mathbb{N}$ est fermé sous l'addition (l'Axiome 2.1(i)), ce qui contredit notre hypothèse que u est un majorant. □

Corollaire 9.2. *L'ensemble $\mathbb{Z}$ des entiers n'est ni majoré, ni nimoré.*

Preuve. Puisque $\mathbb{N} \subseteq \mathbb{Z}$, tous majorant de $\mathbb{Z}$ serait également un majorant de de $\mathbb{N}$, contredisant la Proposition 9.1. Donc $\mathbb{Z}$ n'a pas de majorant.

Maintenant, si $\mathbb{Z}$ était minoré par b. Alors, pour tout $n \in \mathbb{N}$, on aurait

$$-n \in \mathbb{Z} \implies b \leq -n \implies n \leq -b,$$

et donc $\mathbb{N}$ serait majoré par $-b$, contredisant à nouveau la Proposition 9.1. □

Proposition 9.3. *Pour tout $\varepsilon \in \mathbb{R}_{>0}$, il existe $n \in \mathbb{N}$ tel que $\frac{1}{n} < \varepsilon$.*

Preuve. Soit $\varepsilon \in \mathbb{R}_{>0}$. Alors $\frac{1}{\varepsilon} \in \mathbb{R}_{>0}$ par la Proposition 7.17(i). Puis, par la Proposition 9.1, il existe un $n \in \mathbb{N}$ tel que $n > \frac{1}{\varepsilon}$. Et finalement, par la Proposition 7.17(ii), on a $\frac{1}{n} < \varepsilon$. □

Exercices.

9.1.1. Considérez l'ensemble

$$A = \left\{ 5 + \frac{3}{2n} : n \in \mathbb{N} \right\}$$

(i) Déterminez l'infimum de A (et justifiez) ou prouvez qu'il n'existe pas.

(ii) Déterminez le minimum de A ou prouvez qu'il n'existe pas.

(iii) Déterminez le maximum de A ou prouvez qu'il n'existe pas.

(iv) Déterminez le supremum de A ou prouvez qu'il n'existe pas.

9.2 Valeur absolue

On définit la *valeur aboslue* d'un nombre réel comme nous l'avons fait pour les entiers à la Section 6.1. Plus précisément, pour $x \in \mathbb{R}$, on définit

$$|x| = \begin{cases} x, & \text{si } x \geq 0, \\ -x, & \text{si } x < 0. \end{cases}$$

Donc $|x| \in \mathbb{R}_{\geq 0}$ pour tout $x \in \mathbb{R}$.

Proposition 9.4. *Pour tous $x, y \in \mathbb{R}_{\geq 0}$, on a*

$$x < y \iff x^2 < y^2.$$

Preuve. Soient $x, y \in \mathbb{R}_{\geq 0}$.

Supposons tout d'abord que $x < y$. Donc, $y - x \in \mathbb{R}_{>0}$. Si $x = 0$, alors $y \in \mathbb{R}_{>0}$, et donc

$$y^2 > 0 = x^2$$

par l'Axiome 7.13(ii). D'une autre part, si $x > 0$, alors on a $y > x > 0$, et donc $x + y \in \mathbb{R}_{>0}$ par l'Axiome 7.13(i). Ainsi

$$y^2 - x^2 = (y - x)(y + x) \in \mathbb{R}_{>0}$$

par l'Axiome 7.13(ii). Donc, $x^2 < y^2$.

Réciproquement, supposons que $x^2 < y^2$, et donc

$$(y - x)(y + x) = y^2 - x^2 \in \mathbb{R}_{>0}.$$

Mais $x = y = 0$ n'est pas possible, car on aurait $x^2 = 0 = y^2$. Ainsi, au moins un de x et y est positif, et donc $x + y \in \mathbb{R}_{>0}$. Puis

$$y - x = \frac{y^2 - x^2}{y + x} \in \mathbb{R}_{>0},$$

et donc $x < y$. □

Proposition 9.5. *Pour tout $x \in \mathbb{R}$, on a $|x|^2 = x^2$.*

Preuve. Cette preuve est laissée en exercice (Exercice 9.2.1). □

Proposition 9.6. *Pour tous $x, y \in \mathbb{R}$, on a:*

(i) $|x| = 0$ *si et seulement si* $x = 0$,

(ii) $|xy| = |x|\,|y|$,

(iii) $-|x| \leq x \leq |x|$,

(iv) $|x + y| \leq |x| + |y|$ *(l'*inégalité triangulaire*)*,

(v) si $-y < x < y$, *alors* $|x| < |y|$.

Preuve. (i) Voir [BG10, Prop. 10.8(i)].

(ii) Si $x, y \geq 0$, alors $xy \geq 0$, et donc

$$|xy| = xy = |x|\,|y|.$$

Si $x \geq 0$ et $y < 0$, alors $xy \leq 0$ et donc

$$|xy| = -xy = x(-y) = |x|\,|y|.$$

Les deux cas restants, où $x < 0$, $y \geq 0$, et où $x, y < 0$ sont similaires et sont laissés en exercice.

(iii) Si $x \geq 0$, alors $|x| = x$ et donc

$$-|x| = -x \leq 0 \leq x = |x| \implies -|x| \leq x \leq |x|.$$

D'une autre part, si $x < 0$, alors $|x| = -x$ et donc

$$-|x| = -(-x) = x < 0 \leq |x| \implies -|x| \leq x \leq |x|.$$

(iv) On a

$$\begin{aligned}
|x+y|^2 &= (x+y)^2 && \text{(Prop. 9.5)}\\
&= x^2 + 2xy + y^2 &&\\
&= |x|^2 + 2xy + |y|^2 && \text{(Prop. 9.5)}\\
&\leq |x|^2 + |2xy| + |y|^2 && \text{(partie (iii))}\\
&= |x|^2 + 2|x|\,|y| + |y|^2 && \text{(partie (ii))}\\
&= (|x| + |y|)^2. &&
\end{aligned}$$

Ainsi, par la Proposition 9.4, on a $|x+y| \leq |x| + |y|$.

(v) Supposons que $-y < x < y$. Alors, en particulier, on a $-y < y$, et donc $y > 0$, puis $|y| = y$. Si $x \geq 0$, alors

$$|x| = x < y = |y|.$$

D'une autre part, si $x < 0$, alors

$$|x| = -x < y = |y|,$$

où l'inégalité $-x < y$ suit de l'hypothèse que $-y < x$. □

Proposition 9.7. *Supposons que $x \in \mathbb{R}$ satisfait $0 \leq x \leq 1$. De plus, supposons que $m, n \in \mathbb{N}$ tels que $m \geq n$. alors $x^m \leq x^n$.*

Preuve. Soit $0 \leq x \leq 1$ et fixons un $n \in \mathbb{N}$. Posons $P(m)$ comme l'énoncé

$$x^m \leq x^n.$$

On démontre par induction sur m que $P(m)$ est vrai pour tout $m \geq n$.

Le cas de base, où $m = n$ est clairement vrai puisque $x^n \leq x^n$. Maintenant, prenons un $k \geq n$ avec supposons que $P(k)$ est vrai. Puisque $0 \leq x \leq 1$, on a $x^n \cdot x \leq x^n \cdot 1 = x^n$. Donc

$$x^{k+1} = x^k \cdot x \leq x^n \cdot x \leq x^n,$$

où la première inégalité suit de l'hypothèse induction. □

Exercices.

9.2.1. Démontrez la Proposition 9.5. *Indice*: Considérez les deux cas $x < 0$ et $x \geq 0$.

9.2.2 ([BG10, Prop. 10.7]). Soit $x, y \in \mathbb{R}$. Démontrez que $|x| < |y|$ si et seulement si $x^2 < y^2$.

9.2.3. Démontrez que pour tout $n \in \mathbb{N}$ et $x_1, x_2, \ldots, x_n \in \mathbb{R}$,

$$\left| \sum_{i=1}^{n} x_i \right| \leq \sum_{i=1}^{n} |x_i|.$$

9.3 Distance

Dans cette section, on discute brièvement l'idée de distance entre deux nombres réels. Pour $x, y \in \mathbb{R}$, on définit la *distance* entre x et y comme étant $|x - y|$. Cela correspond à notre intuition lorsqu'on s'imagine les nombres réels comme des points sur la droite réelle.

Proposition 9.8 (Propriétés de distance)**.** *Soient $x, y, z \in \mathbb{R}$.*

(i) $|x-y| = 0 \iff x = y$. *(La distance satisfait la propriété de* séparation*.)*

(ii) $|x-y| = |y-x|$. *(La distance est* symétrique*.)*

(iii) $|x-z| \leq |x-y| + |y-z|$. *(L'*inégalité triangulaire*.)*

(iv) $|x-y| \geq \big||x| - |y|\big|$.

Preuve. (i) Par la Proposition 9.6(i), on a

$$|x-y| = 0 \iff x - y = 0 \iff x = y.$$

(ii) Par la Proposition 9.6(ii), on a

$$|x-y| = |(-1)(y-x)| = |-1|\,|y-x| = 1 \cdot |y-x| = |y-x|.$$

(iii) Par la Proposition 9.6(iv), on a

$$|x-z| = |(x-y) + (y-z)| \leq |x-y| + |y-z|.$$

(iv) En échangeant les rôles de x et y si nécessaire, on peut supposer que $|x| \geq |y|$. Alors $\big||x| - |y|\big| = |x| - |y|$. En prenant $z = 0$ à la partie (iii), on a

$$|x| = |x-0| \leq |x-y| + |y-0| = |x-y| + |y|,$$

et donc

$$|x-y| \geq |x| - |y| = \big||x| - |y|\big|.$$

□

Proposition 9.9. *Soit $z \in \mathbb{R}_{\geq 0}$. Alors*

$$z = 0 \iff \forall \varepsilon \in \mathbb{R}_{>0},\ z < \varepsilon.$$

Preuve. Si $z = 0$, alors $z < \varepsilon$ pour tout $\varepsilon \in \mathbb{R}_{>0}$. Maintenant, supposons que $z \neq 0$ (preuve indirecte). Alors, $z > 0$. Ainsi, par le Théorème 7.21, il existe un $\varepsilon \in \mathbb{R}$, tel que $0 < \varepsilon < z$. Ainsi, la négation de $\forall \varepsilon \in \mathbb{R}_{>0},\ z < \varepsilon$ est vraie. □

Corollaire 9.10. *Pour tous $x, y \in \mathbb{R}$, on a*

$$x = y \iff \forall \varepsilon > 0,\ |x-y| < \varepsilon.$$

Preuve. On a

$$\begin{aligned} x = y &\iff |x-y| = 0 && \text{(Prop. 9.8(i))} \\ &\iff \forall \varepsilon > 0,\ |x-y| < \varepsilon. && \text{(Prop. 9.9 avec } z = |x-y|) \end{aligned}$$

□

Exercices.

9.3.1. Démontrez que, pour tout $x, y \in \mathbb{R}$, on a $|x - y| \leq |x| + |y|$.

9.3.2. Soit $z \in \mathbb{R}_{\geq 0}$. Démontrez que

$$z = 0 \iff \forall n \in \mathbb{N},\ z < \frac{1}{n}.$$

9.4 Limites

Nous sommes maintenant prêt à investiguer la définition précise de la limite d'une suite.

Définition 9.11 (Limite d'une suite)**.** Soit $(x_k)_{k=1}^{\infty}$, une suite dans $\mathbb{R}$ et $L \in \mathbb{R}$. On dit que (x_k) *converge vers* L si

$$\forall \varepsilon > 0,\ \exists N \in \mathbb{N} \text{ tel que } \forall n \geq N,\ |x_n - L| < \varepsilon.$$

Quand (x_k) converge vers L, on dit que L est la *limite* de la suite (x_k) et on écrit

$$\lim_{k \to \infty} x_k = L.$$

On dit que la suite *converge* s'il existe un L vers laquelle la suite converge. S'il n'existe pas de tel L, alors on dit que la suite *diverge*. Plus précisément, une suite (x_k) diverge si

$$\forall L \in \mathbb{R}\ \exists \varepsilon > 0 \text{ tel que } \forall N \in \mathbb{N}\ \exists n \geq N \text{ tel que } |x_n - L| \geq \varepsilon.$$

S'habituer à la définition formelle de limite peut prendre du temps, mais il est important de maîtriser ce concept. Intuitivement, la suite (x_k) converge vers L si, pour n'importe quelle distance ε, les termes de la suite se retrouve éventuellement à une distance ε de L.

Proposition 9.12. *On a*

$$\lim_{k \to \infty} \frac{1}{k} = 0.$$

Preuve. Soit $\varepsilon > 0$. Par la Proposition 9.1, il existe $N \in \mathbb{N}$ tel que $N > \frac{1}{\varepsilon}$. Alors, pour tout $n \geq N$, on a

$$\left| \frac{1}{n} - 0 \right| = \frac{1}{n} \leq \frac{1}{N} < \varepsilon$$

Ainsi, $\lim_{k \to \infty} \frac{1}{k} = 0$. □

Exemple 9.13. On va montrer que

$$\lim_{k \to \infty} \frac{2k - 3}{k} = 2.$$

Notons que

$$\left|\frac{2k-3}{k}-2\right| = \left|\frac{2k-3}{k}-\frac{2k}{k}\right| = \left|\frac{-3}{k}\right| = \frac{3}{k},$$

pour tout $k > 0$. Fixons $\varepsilon > 0$. Par la Proposition 9.1, il existe un $N \in \mathbb{N}$ avec $N > \frac{3}{\varepsilon}$. Alors, pour tout $n \geq N$, on a

$$\left|\frac{2n-3}{n}-2\right| = \frac{3}{n} \leq \frac{3}{N} < \varepsilon,$$

comme souhaité.

Exemple 9.14. On va démontrer que

$$\lim_{k\to\infty} \frac{3k^2+8k-5}{4k^2+1} = \frac{3}{4}.$$

Notons que

$$\left|\frac{3k^2+8k-5}{4k^2+1}-\frac{3}{4}\right| = \left|\frac{3k^2+8k-5}{4k^2+1}-\frac{3\left(k^2+\frac{1}{4}\right)}{4\left(k^2+\frac{1}{4}\right)}\right| = \left|\frac{8k-\frac{23}{4}}{4k^2+1}\right|.$$

Maintenant, avec $k \geq 1$, on a $8k \geq 8 > \frac{23}{4}$. Aussi, $0 < 4k^2 < 4k^2+1$. Ainsi,

$$\left|\frac{8k-\frac{23}{4}}{4k^2+1}\right| = \frac{8k-\frac{23}{4}}{4k^2+1} \leq \frac{8k}{4k^2} = \frac{2}{k}.$$

Maintenant, considérons un $\varepsilon > 0$. Par la Proposition 9.1, il existe $N \in \mathbb{N}$ avec $N > \frac{2}{\varepsilon}$. Alors, pour tout $n \geq N$, on a

$$\left|\frac{3n^2+8n-5}{4n^2+1}-\frac{3}{4}\right| \leq \frac{2}{n} \leq \frac{2}{N} < \varepsilon,$$

tel que souhaité.

Exemple 9.15. On va montrer que la suite $(x_k)_{k=1}^{\infty}$ donnée par $x_k = 2k+1$ diverge. Donc, on doit montrer qu'elle ne converge vers *aucun* nombre réel. Soit $L \in \mathbb{R}$. On va démontrer que la suite ne converge pas vers L.

Pour tout $k \geq |L|$, on a, par l'inégalité triangulaire,

$$|x_k - L| + |L| \geq |x_k| = |2k+1| = 2k+1 \geq 2|L|+1,$$

et donc

$$|x_k - L| \geq |L| + 1.$$

Ainsi, on peut prendre $\varepsilon = |L|+1$, et peu importe le $N \in \mathbb{N}$ qu'on choisit, on peut toujours trouver un n plus grand que $|L|$ et N, et on obtient

$$|x_n - L| \geq L + 1 = \varepsilon.$$

Donc la suite (x_k) ne converge pas vers L.

Proposition 9.16 (Unicité de la limite)**.** *Si une suite converge, alors sa limite est unique. En d'autres mots, si une suite $(x_k)_{k=1}^{\infty}$ converge vers L_1 et vers L_2, alors $L_1 = L_2$.*

Preuve. Supposons que (x_k) converge à la fois vers L_1 et L_2. Soit $\varepsilon > 0$. Alors il existe un nombre naturel N_1 tel que

$$n \geq N_1 \implies |x_n - L_1| < \frac{\varepsilon}{2}.$$

Similairement, il existe un nombre naturel N_2 tel que

$$n \geq N_2 \implies |x_n - L_2| < \frac{\varepsilon}{2}.$$

Soit $N = \max\{N_1, N_2\}$. Alors, pour tout $n \geq N$, on a

$$|x_n - L_1| < \frac{\varepsilon}{2} \quad \text{et} \quad |x_n - L_2| < \frac{\varepsilon}{2},$$

et donc, par l'inégalité triangulaire, on a

$$|L_1 - L_2| \leq |L_1 - x_n| + |x_n - L_2| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.$$

Puisque $\varepsilon > 0$ était choisi arbitrairement, on conclut par le corollaire 9.10 que $L_1 = L_2$. □

Proposition 9.17. *Supposons que $r \in \mathbb{N}$ et que $(x_k)_{k=1}^{\infty}$ est une suite de nombre réel. Alors $(x_k)_{k=1}^{\infty}$ converge vers L si et seulement si $(x_{k+r})_{k=1}^{\infty}$ converge vers L*

Preuve. Supposons que $\lim_{k\to\infty} x_k = L$. Soit $\varepsilon > 0$. Alors il existe $N \in \mathbb{N}$ tel que

$$n \geq N \implies |x_n - L| < \varepsilon.$$

Mais alors, pour tout $n \geq N$, on a $n + r > n \geq N$ et donc

$$|x_{n+r} - L| < \varepsilon.$$

Ainsi, $\lim_{k\to\infty} x_{k+r} = L$. L'implication inverse est laissée en exercice 9.4.9. □

Remarque 9.18. La Proposition 9.17 nous dit que l'on peut toujours ignorer un nombre fini de termes au début d'une suite lorsqu'il s'agit de calculer une limite.

Proposition 9.19 (Inégalité de Bernoulli)**.** *Pour $x \in \mathbb{R}_{\geq 0}$ et $k \in \mathbb{Z}_{\geq 0}$, on a*

$$(1 + x)^k \geq 1 + kx.$$

Preuve. L'énoncé est clairement vrai pour $k = 0$ et $k = 1$, donc on suppose que $k \geq 2$. Quoique l'on a prouvé le théorème du binôme seulement pour les entiers (Théorème 4.12), la même preuve fonctionne pour des $a, b \in \mathbb{R}$. Ainsi, on a

$$(1 + x)^k = \sum_{m=0}^{k} \binom{k}{m} x^m = 1 + kx + \sum_{m=2}^{k} \binom{k}{m} x^m \geq 1 + kx.$$ □

Proposition 9.20. *Si $x \in \mathbb{R}$ avec $|x| < 1$, alors $\lim_{k\to\infty} x^k = 0$.*

Preuve. Le cas avec $x = 0$ est facile (voir la Proposition 9.26(i)), donc on suppose que $0 < |x| < 1$. Alors, pour tout $N \geq 0$, par la Proposition 9.19, on a

$$\left(\frac{1}{|x|}\right)^N = \left(1 + \frac{1-|x|}{|x|}\right)^N \geq 1 + \left(\frac{1-|x|}{|x|}\right) N > \left(\frac{1-|x|}{|x|}\right) N. \tag{9.1}$$

Maintenant, prenons un $\varepsilon > 0$. Par la Proposition 9.1, il existe un nombre naturel N tel que

$$N > \frac{|x|}{1-|x|}\,\frac{1}{\varepsilon}. \tag{9.2}$$

Puis, pour tout $n \geq N$, on a

$$\begin{aligned} |x^n - 0| &= |x|^n \\ &\leq |x|^N && \text{(par la Proposition 9.7)} \\ &< \frac{|x|}{1-|x|}\,\frac{1}{N} && \text{(par (9.1))} \\ &< \varepsilon. && \text{(par (9.2))} \end{aligned}$$

□

Définition 9.21 (Suite borné, croissante, décroissante, monotone)**.** Soit $(x_k)_{k=1}^{\infty}$ une suite.

(i) La suite est *bornée* s'il existe $\ell, u \in \mathbb{R}$ tel que $\forall k \in \mathbb{N}$, $\ell \leq x_k \leq u$. De manière équivalente, elle est bornée s'il existe $\ell \in \mathbb{R}$ tel que $\forall k \in \mathbb{N}$, $|x_k| \leq \ell$.

(ii) La suite est *croissante* si $x_{k+1} \geq x_k$ pour tout $k \in \mathbb{N}$.

(iii) La suite est *décroissante* si $x_{k+1} \leq x_k$ pour tout $k \in \mathbb{N}$.

(iv) La suite est *monotone* si elle croissante ou décroissante.

Théorème 9.22. *Toute suite monotone et bornée converges.*

Preuve. On va démontrer que toute suite décroissante et bornée converge. La preuve pour une suite croissante et bornée est similaire, et se trouve dans [BG10, Th. 10.19].

Soit $(x_k)_{k=1}^{\infty}$ décroissante et bornée. Alors, l'ensemble

$$A = \{x_k : k \in \mathbb{N}\} \subseteq \mathbb{R}$$

est borné. Ainsi, par la Proposition 7.38, elle admet une borne inférieure s. On va montrer que $\lim_{k\to\infty} x_k = s$.

Soit $\varepsilon > 0$. Alors $s + \varepsilon > s$, et donc $s + \varepsilon$ n'est *pas* un minorant de A. Ainsi, il existe un $N \in \mathbb{N}$ tel que $x_N < s + \varepsilon$. Puisque la séquence est décroissante, on a $x_n \leq x_N$ pour tout $n \geq N$. Ainsi, pour tout $n \geq N$, on a

$$s - \varepsilon < s \leq x_n \leq x_N < s + \epsilon,$$

et donc $|x_n - s| < \varepsilon$ par la Proposition 9.6(v). □

Notez qu'une suite croissante est toujours minoré (par le premier terme), donc elle est bornée si et seulement si elle est majoré. Similairement, une suite décroissante est bornée si et seulement si elle est minoré.

Exemples 9.23. (i) La suite $\left(4+\frac{1}{n}\right)_{n=1}^{\infty}$ est décroissante et minoré par 4. Donc, elle converge.

(ii) La suite $\left(8-\frac{2}{3k^2+5}\right)_{k=1}^{\infty}$ est croissante et majoré par 8. Donc, elle converge.

Proposition 9.24. *Supposons qu'une suite $(x_k)_{k=1}^{\infty}$ converge vers L.*

(i) Si $(x_k)_{k=1}^{\infty}$ est croissante, alors $x_k \leq L$ pour tout $k \in \mathbb{N}$.

(ii) Si $(x_k)_{k=1}^{\infty}$ est décroissante, alors $x_k \geq L$ pour tout $k \in \mathbb{N}$.

Preuve. On va seulement démontrer la partie (i), car la preuve de la partie (ii) est similaire.

Supposons que $(x_k)_{k=1}^{\infty}$ est croissante et que $\lim_{k\to\infty} x_k = L$. On démontre le résultat par contradiction. Supposons qu'il existe un $m \in \mathbb{N}$ tel que $x_m > L$. Soit $\varepsilon = x_m - L$. Alors, pour tout $N \in \mathbb{N}$, on peut choisir $n = \max\{N, m\}$ (donc $n \geq N$). Puisque la suite est croissante, on a $x_n \geq x_m > L$. Mais alors,

$$|x_n - L| = x_n - L \geq x_m - L = \varepsilon.$$

Donc, la suite $(x_k)_{k=1}^{\infty}$ ne converge pas vers L, une contradiction. □

Proposition 9.25. *Toute suite convergente est bornée.*

Preuve. Supposons que $(x_k)_{k=1}^{\infty}$ converge. En prenant $\varepsilon = 1$ dans la définition de limite, il existe un $N \in \mathbb{N}$ tel que pour tout $n \geq N$, on a $|x_n - L| < 1$. Notez que

$$|x_n - L| < 1 \implies |x_n| - |L| \leq \big||x_n| - |L|\big| \leq |x_n - L| < 1 \implies |x_n| < |L| + 1,$$

où, dans la deuxième égalité après l'implication, on a fait appel à la Proposition 9.8(iv). Maitenant, posons

$$M = \max\{|x_1|, |x_2|, \ldots, |x_{N-1}|, |L| + 1\},$$

lequel est bien défini car le maximum d'un ensemble fini existe toujours. Puis, on a $|x_k| \leq M$ pour tout $k \in \mathbb{N}$, et donc la suite est bornée. □

Proposition 9.26. *Supposons que $\lim_{k\to\infty} a_k = A$, $\lim_{k\to\infty} b_k = B$ et $c \in \mathbb{R}$.*

(i) $\lim_{k\to\infty} c = c$.

(ii) $\lim_{k\to\infty}(ca_k) = cA$.

(iii) $\lim_{k\to\infty}(a_k + b_k) = A + B$.

(iv) $\lim_{k\to\infty}(a_k b_k) = AB$.

(v) Si $A \neq 0$, alors $\lim_{k\to\infty} \frac{1}{a_k} = \frac{1}{A}$.

Preuve. On va démontrer les parties (i), (iii), et (v). Les preuves des autres parties se trouvent dans [BG10, Prop. 10.23].

Preuve de (i): Pour tout $\varepsilon > 0$, on a $|c - c| = 0 < \varepsilon$, et donc on peut prendre n'importe quel $N \in \mathbb{N}$ pour la définition de limite (Définition 9.11).

Preuve de (iii): Soit $\varepsilon > 0$. Alors, il existe $N_1 \in \mathbb{N}$ tel que

$$n \geq N_1 \implies |a_n - A| < \frac{\epsilon}{2},$$

et il existe $N_2 \in \mathbb{N}$ tel que

$$n \geq N_2 \implies |b_n - B| < \frac{\epsilon}{2}.$$

Posons $N = \max\{N_1, N_2\}$. Alors, pour tout $n \geq N$, on a

$$\begin{aligned} |(a_n + b_n) - (A + B)| &= |(a_n - A) + (b_n - B)| \\ &\leq |a_n - A| + |b_n - B| \qquad \text{(par l'inégalité triangulaire)} \\ &< \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon. \end{aligned}$$

Preuve de (v): Supposons que $A \neq 0$. Choisissons $N_1 \in \mathbb{N}$ tel que, pour tout $n \geq N_1$, on a $|a_n - A| < \frac{|A|}{2}$. Notons que

$$|a_n - A| < \frac{|A|}{2} \implies |A| - |a_n| \leq \big||A| - |a_n|\big| \leq |A - a_n| < \frac{|A|}{2} \implies \frac{|A|}{2} < |a_n|,$$

où, dans la deuxième inégalité après la première implication, on a employé la Proposition 9.8(iv). Ainsi, pour tout $n \geq N_1$, on a

$$0 < \frac{|A|}{2} < |a_n| \implies 0 < \frac{1}{|a_n|} < \frac{2}{|A|}.$$

Ainsi, pour $n \geq N_1$,

$$\left|\frac{1}{a_n} - \frac{1}{A}\right| = \left|\frac{A - a_n}{A a_n}\right| = \frac{|A - a_n|}{|A|\,|a_n|} \leq \frac{2}{|A|^2}|A - a_n|.$$

Soit $\varepsilon > 0$. Puisque $\lim_{k\to\infty} a_k = A$, on peut choisir $N_2 \in \mathbb{N}$ tel que

$$n \geq N_2 \implies |A - a_n| < \frac{|A|^2}{2}\varepsilon.$$

Posons $N = \max\{N_1, N_2\}$. Puis, pour tout $n \geq N$, on a

$$\left|\frac{1}{a_n} - \frac{1}{A}\right| \leq \frac{2}{|A|^2}|A - a_n| < \frac{2}{|A|^2}\frac{|A|^2}{2}\varepsilon = \varepsilon. \qquad \square$$

La Proposition 9.26 est particulièrement utile, puisqu'elle nous permet de calculer de nouvelles limites à partir d'anciennes.

Proposition 9.27. *Pour $\ell \in \mathbb{N}$, on a*

$$\lim_{k\to\infty} \frac{1}{k^\ell} = 0.$$

Preuve. On démontre le résultat par induction sur ℓ. Le cas de base $\ell = 1$ est la Proposition 9.12. Maintenant, supposons que le résultat est vrai pour un certain $\ell \in \mathbb{N}$. Alors, par la Proposition 9.26(iv), on a

$$\lim_{k\to\infty} \frac{1}{k^{\ell+1}} = \left(\lim_{k\to\infty} \frac{1}{k}\right)\left(\lim_{k\to\infty} \frac{1}{k^\ell}\right) = 0 \cdot 0 = 0,$$

et donc le résultat est vrai pour $\ell + 1$. Cela complète la preuve de l'étape inductive. □

Exemple 9.28. On a

$$\begin{aligned}\lim_{k\to\infty} \frac{4k^2 - 5k + 2}{3k^2} &= \lim_{k\to\infty} \left(\frac{4k^2}{3k^2} + \frac{-5k}{3k^2} + \frac{2}{3k^2}\right) \\ &= \lim_{k\to\infty} \left(\frac{4}{3}\right) - \frac{5}{3}\left(\lim_{k\to\infty} \frac{1}{k}\right) + \frac{2}{3}\left(\lim_{k\to\infty} \frac{1}{k^2}\right) = \frac{4}{3} + 0 + 0 = \frac{4}{3}.\end{aligned}$$

Exemple 9.29. Considérez la suite $\left((-1)^k\right)_{k=1}^\infty$. Cette suite est bornée car $|(-1)^k| \leq 1$ pour tout $k \in \mathbb{N}$. Toutefois, la séquence ne converge *pas*. On démontre cela par contradiction. Supposons que $\lim_{k\to\infty}(-1)^k = L$. Alors il existe $N \in \mathbb{N}$ tel que

$$\forall n \geq N,\ |(-1)^n - L| < \frac{1}{2}.$$

Puisque $2N, 2N + 1 > N$, alors on a, par l'inégalité triangulaire,

$$2 = \left|(-1)^{2N} - (-1)^{2N+1}\right| \leq \left|(-1)^{2N} - L\right| + \left|L - (-1)^{2N+1}\right| < \frac{1}{2} + \frac{1}{2} = 1,$$

ce qui donne une contradiction.

Exemple 9.30. Considérons les suites $(a_k)_{k=1}^\infty$ et $(b_k)_{k=1}^\infty$, où

$$a_k = 2 - k \qquad \text{et} \qquad b_k = k.$$

Aucune de ces suites n'est bornée, donc elles divergent par la Proposition 9.25. Toutefois, $(a_k + b_k)_{k=1}^\infty$ est la suite constante $(2)_{k=1}^\infty$, laquelle converge vers 2 par la Proposition 9.26(i).

Exercices.

9.4.1. En employant la définition de limite directement, déterminez

$$\lim_{k\to\infty} \frac{8}{3k}.$$

9.4.2. En utilisant la définition de limite directement, déterminez

$$\lim_{k\to\infty} \frac{2k^2+3k-1}{5k^2+5}.$$

9.4.3. Soient $(x_k)_{k=1}^{\infty}$, $(y_k)_{k=1}^{\infty}$ et $(z_k)_{k=1}^{\infty}$, des suites satisfaisant

$$x_k \leq y_k \leq z_k \quad \text{pour tout } k \in \mathbb{N}.$$

De plus, supposons que $\lim_{k\to\infty} x_k = L = \lim_{k\to\infty} z_k$ pour un certain $L \in \mathbb{R}$. Démontrez que $\lim_{k\to\infty} y_k = L$.

9.4.4. Une fonction $f\colon \mathbb{R} \to \mathbb{R}$ est dite *croissante* si

$$\forall x, y \in \mathbb{R},\ \big(x \leq y \implies f(x) \leq f(y)\big).$$

Démontrez que, si $(x_k)_{k=1}^{\infty}$ est une suite croissante et que $f\colon \mathbb{R} \to \mathbb{R}$ est une fonction croissante dont l'image est bornée, alors la suite $(f(x_k))_{k=1}^{\infty}$ converge.

9.4.5. Soit $(x_k)_{k=1}^{\infty}$ une suite et soit $L \in \mathbb{R}$.

(i) Démontrez que, si $\lim_{k\to\infty} x_k = L$, alors $\lim_{k\to\infty} |x_k| = |L|$.

(ii) Donnez un exemple de suite $(x_k)_{k=1}^{\infty}$ qui diverge, mais pour laquelle la suite $(|x_k|)_{k=1}^{\infty}$ converge.

9.4.6. En employant n'importe quel résultat déjà prouvé, déterminez

$$\lim_{k\to\infty} \frac{3k^3+8k^2-3k-11}{6k^3}.$$

9.4.7. Définissons la suite $\{x_k\}_{k=1}^{\infty}$ par

$$x_k = \begin{cases} 0 & \text{si } k \text{ est impair,} \\ 1 & \text{si } k \text{ est pair.} \end{cases}$$

Démontrez que la suite $\{x_k\}_{k=1}^{\infty}$ diverge.

9.4.8. Considérez la suite $(a_k)_{k=1}^{\infty}$, où $a_k = (-1)^k$. Trouvez une suite $(b_k)_{k=1}^{\infty}$ telle que $(a_k + b_k)_{k=1}^{\infty}$ converge.

9.4.9. Complétez la preuve de la Proposition 9.17 en démontrant que, si $(x_{k+r})_{k=1}^{\infty}$ converge vers L, alors $(x_k)_{k=1}^{\infty}$ converge vers L.

9.5 Racine carrée

L'axiome de complétude (l'Axiome 7.35) nous permet de démontrer l'existence de certains nombres réels, tels que les racines carrées. Pour tout $r \in \mathbb{R}_{>0}$, on définit la *racine carrée* de r comme étant

$$\sqrt{r} := \sup\{x \in \mathbb{R} : x^2 < r\}.$$

On définit $\sqrt{0} := 0$.

Théorème 9.31. *Le nombre réel $\sqrt{r}$ est bien définie, positif, et $(\sqrt{r})^2 = r$.*

Esquisse de la preuve. Considérons le cas de $r = 2$. La preuve pour les autres valeurs de r sont similaires. On démontre tout d'abord que $\sqrt{2}$ est bien définie. Posons

$$A = \{x \in \mathbb{R} : x^2 < 2\}.$$

On veut montrer que $\sup A$ existe. Puisque $1^2 = 1 < 2$, on sait que A n'est pas vide. Or,

$$x \geq 2 \implies x^2 \geq 4 > 2.$$

Donc, $x < 2$ pour tout $x \in A$. Cela veut dire que A est majoré. Ainsi, par l'axiome de complétude (l'Axiome 7.35), l'ensemble A admet un supremum. Donc, $\sqrt{2}$ est bien définie.

Il reste à vérifier que $(\sqrt{2})^2 = 2$. Pour ce faire, il faut montrer que l'énoncé $(\sqrt{2})^2 < 2$ ou $(\sqrt{2})^2 > 2$ mène à une contradiction, en employant la définition du supremum. Voir [BG10, Th. 10.25] pour les détails. □

Remarque 9.32. Notez que $-\sqrt{2}$ est également un nombre dont le carré est égal à 2. La notation $\sqrt{2}$ se réfère à la racine carrée *positive*.

Proposition 9.33. *Soit $r \in \mathbb{R}_{\geq 0}$. Alors, le nombre $\sqrt{r}$ est unique. Plus précisément, si $x \in \mathbb{R}_{\geq 0}$ satisfait $x^2 = r$, alors $x = \sqrt{r}$.*

Preuve. Premièrement, considérons le cas $r = 0$. Par l'Axiome 7.13(ii), si $x > 0$, alors $x^2 > 0$. Donc, $x = 0 = \sqrt{0}$ est la seule solution pour $x^2 = 0$.

Maintenant, prenons un $r > 0$ et $x \in \mathbb{R}_{\geq 0}$ satisfaisant $x^2 = r = (\sqrt{r})^2$. Alors

$$0 = x^2 - (\sqrt{r})^2 = (x - \sqrt{r})(x + \sqrt{r}).$$

Puisque $x + \sqrt{r} > 0$, cela implique que $x - \sqrt{r} = 0$, et donc $x = \sqrt{r}$. □

Proposition 9.34. *Si $r \in \mathbb{R}$, $r < 0$, alors il n'y a pas de $x \in \mathbb{R}$ tel que $x^2 = r$.*

Preuve. Si $x = 0$, alors $x^2 = 0 \neq r$. D'une autre part, si $x \neq 0$, alors par la Proposition 2.11 pour $\mathbb{R}$, on a $x^2 > 0$. Donc, $x^2 \neq r$. □

La Proposition 9.34 dit que tout nombre négatif réel n'admet pas de racine carrée réelle. Lors de cours à venir, vous allez aborder les *nombres complexes*. Il s'ensuivra que, en travaillant avec les nombres complexes, *toutes* les racines carrées existent. En particulier, les nombres négatifs réels admettent des racines carrées parmi les nombres complexes.

Chapitre 10

Nombres rationnels et irrationnels

Dans ce chapitre, on aborde brièvement le concept des nombres rationnels, lesquelles sont des nombres pouvant s'écrire comme un quotient de deux entiers. On considèrera les nombres irrationnels également.

10.1 Nombres rationnels

Définition 10.1. Un nombre réel $r \in \mathbb{R}$ est *rationnel* si $r = \frac{m}{n}$ pour certains $m, n \in \mathbb{Z}$, $n \neq 0$. Un nombre réel qui n'est pas rationnel est dit *irrationnel*. L'ensemble des nombres rationnels est dénoté $\mathbb{Q}$.

Proposition 10.2. *On a* $\mathbb{Z} \subseteq \mathbb{Q}$.

Preuve. Pour $n \in \mathbb{Z}$, on a $n = \frac{n}{1} \in \mathbb{Q}$. □

Proposition 10.3. *Tout nombre rationnel* $r \in \mathbb{Q}$ *peut s'écrire de la forme* $r = \frac{m}{n}$ *où* $n > 0$, *et* m *et* n *n'ont aucun facteur en commun (autre que* ± 1*).*

Esquisse de la preuve. Soit $r \in \mathbb{Q}$. Par définition $r = \frac{a}{b}$ pour des $a, b \in \mathbb{Z}$, $b \neq 0$. Si $b < 0$, alors on peut écrire $r = \frac{-a}{-b}$ et le dénominateur est positif. Ainsi, on peut supposer que le dénominateur est positif. Ensuite, on factorise le numérateur et le dénominateur en produits de nombres premiers et on annule tous les facteurs premiers en commun. □

Lorsque r est écrit sous la forme $r = \frac{m}{n}$ où $n > 0$, et m et n n'ont aucun facteur en commun, on dit que la représentation $\frac{m}{n}$ est sous forme *irréductible* (ou *simplifiée*).

Proposition 10.4. *Soit $r, s \in \mathbb{Q}$. Alors*

(i) $r + s \in \mathbb{Q}$,

(ii) $rs \in \mathbb{Q}$,

(iii) $-r \in \mathbb{Q}$,

(iv) $r - s \in \mathbb{Q}$,

(v) si $r \neq 0$, *alors* $r^{-1} \in \mathbb{Q}$.

Preuve. On peut écrire $r = \frac{a}{b}$ et $s = \frac{c}{d}$ pour des $a, b, c, d \in \mathbb{Z}$ avec $b, d \neq 0$. Alors

$$r + s = \frac{a}{b} + \frac{c}{d} = \frac{ad}{bd} + \frac{bc}{bd} = \frac{ad + bc}{bd} \in \mathbb{Q}.$$

Cela démontre la partie (i). La preuve des autres parties est laissée en exercice. □

Théorème 10.5. *Soient $x, y \in \mathbb{R}$ tels que $x < y$. Alors, il existe $r \in \mathbb{Q}$ tel que $x < r < y$.*

Preuve. Si $x = 0$, alors, par la Proposition 9.3, on peut trouver un $n \in \mathbb{N}$ tel que $x = 0 < \frac{1}{n} < y$.

Maintenant, supposons que $x > 0$. Par la Proposition 9.3, il existe $m \in \mathbb{N}$ tel que $\frac{1}{m} < y - x$. De plus, puisque $\mathbb{N}$ n'est pas borné, il existe un $n \in \mathbb{N}$ tel que $n > mx$. Par le principe du bon ordre (Théorème 2.33), on peut choisir un n minimal avec cette propriété, et donc $n - 1 \leq mx < n$. En divisant par m, on obtient

$$\frac{n}{m} - \frac{1}{m} \leq x < \frac{n}{m}.$$

L'inégalité de gauche implique que

$$\frac{n}{m} \leq x + \frac{1}{m} < x + (y - x) = y.$$

Et on a donc

$$x < \frac{n}{m} < y,$$

tel que souhaité.

Maintenant, supposons que $x < 0$. Si $y > 0$, alors il suffit de prendre $r = 0$. Sinon, on peut supposer que $y \leq 0$. Donc, on a $0 \leq -y < -x$. Par la démonstration ci-haut, il existe un nombre rationnel r tel que $-y < r < -x$. Or, $-r$ est aussi rationnel (par la Proposition 10.4) et on obtient $x < -r < y$, tel que souhaité. □

Le Théorème 10.5 énonce que les nombres rationnels sont *denses* dans les nombres réels. (Le mot *dense* est un terme du domaine de la topologie et s'applique à un contexte plus général.)

Corollaire 10.6. *Il n'y a pas de plus petit nombre rationnel.*

Preuve. On démontre le résultat par contradiction. Supposons que a est un plus petit nombre positif rationnel. Alors $0 < a$. Puis, par le Théorème 10.5, il existe un $r \in \mathbb{Q}$ tel que $0 < r < a$. Cela contredit le fait que a est le plus nombre positif rationnel. □

Exercices.

10.1.1 ([BG10, Prop. 11.2]). Soient $x, y, z, w \in \mathbb{R}$ tels que $y \neq 0$ et $w \neq 0$. Démontrez que si $\frac{x}{y} = \frac{z}{w}$, alors $xw = zy$.

10.1.2 ([BG10, Prop. 11.3]). Démontrez que si $x, y, z \in \mathbb{R}$ avec $y \neq 0$ et $z \neq 0$, alors $\frac{xz}{yz} = \frac{x}{y}$.

10.1.3 ([BG10, Prop. 11.5]). Supposons que $m, n, s, t \in \mathbb{Z}$ avec $n, t \neq 0$, et que m et n n'ont pas de facteurs communs. Démontrez que si $\frac{m}{n} = \frac{s}{t}$, alors m divise s et n divise t.

10.1.4 ([BG10, Prop. 11.7]). Le nombre rationnel $\frac{m}{n} \in \mathbb{Q}$ est positif (i.e. $\frac{m}{n} \in \mathbb{R}_{>0}$) si et seulement si soit $m > 0$ et $n > 0$, soit $m < 0$ et $n < 0$.

10.2 Nombres irrationels

On sait déjà que des nombres rationnels existent (e.g. les entiers sont des nombres rationnels), mais on n'a pas encore démontré qu'il existe des nombres irrationnels.

Proposition 10.7. *Le nombre réel $\sqrt{2}$ est irrationel.*

Preuve. On démontre cela en procédant par contradiction; donc supposons que $\sqrt{2}$ est rationnel. Par la Proposition 10.3, on peut écrire $\sqrt{2} = \frac{m}{n}$, où $m, n \in \mathbb{Z}$ n'ont pas de facteur commun (autre que ± 1). Alors, on a

$$\frac{m^2}{n^2} = \left(\frac{m}{n}\right)^2 = (\sqrt{2})^2 = 2 \implies m^2 = 2n^2.$$

Ainsi, 2 divise m^2. Alors, par le lemme d'Euclide (Proposition 6.31), 2 divise m. Donc, il existe un $a \in \mathbb{Z}$ tel que $2a = m$. Notons que

$$2a = m \implies 2^2a^2 = m^2 = 2n^2 \implies 2a^2 = n^2.$$

Donc, 2 divise n^2. Et encore une fois, par le lemme d'Euclide (Proposition 6.31), 2 divise n. Mais alors, 2 est un facteur commun de m et n, ce qui contredit notre hypothèse que m et n n'ont pas de facteur commun. □

En fait, la Proposition 10.7 peut être généralisée. Un entier n est dit un *carré parfait* si $n = m^2$ pour un certain $m \in \mathbb{Z}$. Ainsi, on a le résultat suivant.

Théorème 10.8. *Supposons que $a \in \mathbb{N}$ n'est pas un carré parfait, alors $\sqrt{a}$ est irrationnel.*

Preuve. La preuve de ce résultat est laissée en exercice. *Indice*: Suivez l'argument de la preuve de la Proposition 10.7 en utilisant un facteur premier de a. □

Exemple 10.9. Le nombre réel $\sqrt{2}+\sqrt{3}$ est irrationnel. On peut démontrer cela par contradiction. Supposons que $\sqrt{2}+\sqrt{3} \in \mathbb{Q}$. Alors

$$\left(\sqrt{2}+\sqrt{3}\right)^2 = 2+2\sqrt{6}+3 = 5+2\sqrt{6} \in \mathbb{Q}.$$

Donc, $5+2\sqrt{6} = a$ pour un certain $a \in \mathbb{Q}$. Mais alors $\sqrt{6} = \frac{a-5}{2} \in \mathbb{Q}$ par la Proposition 10.4, ce qui contredit le Théorème 10.8.

Notez que $\mathbb{Q}$ ne satisfait *pas* l'axiome de complétude (l'Axiome 7.35). Par exemple, l'ensemble

$$\{r \in \mathbb{Q} : r^2 < 2\}$$

est majoré par un nombre rationnel (disons, par 2), mais il n'admet pas de borne supérieure dans $\mathbb{Q}$. Bien entendu, il admet une plus petite borne supérieure dans $\mathbb{R}$, soit $\sqrt{2}$. Similairement, les nombres irrationals ne satisfont pas l'axiome de complétude.

Exercices.

10.2.1 ([BG10, Prop. 11.13]). Soient m et n des entiers non nuls. Démontrez que $\frac{m}{n}\sqrt{2}$ est irrationnel.

Index

Bibliographie

[BG10] Matthias Beck and Ross Geoghegan. *The Art of Proof*. Undergraduate Texts in Mathematics. Springer, 2010. http://dx.doi.org/10.1007/978-1-4419-7023-7.