Chapitre 3

Les grands ensembles de nombres

Ce chapitre étudie les grands ensembles de nombres sur lesquels sont basées les mathématiques. Certains de ces ensembles seront familiers, d'autres nouveaux. À l'exception d'un ensemble (les entiers modulo n), les autres sont imbriqués les uns dans les autres : le premier apparaît comme un sous-ensemble du second, le second du troisième, etc.

Mais pourquoi étudier « encore » ces ensembles qui sont bien connus ? Les revoir un après l'autre permet de comprendre ce que le nouvel ensemble apporte par rapport au précédent. L'introduction de chacun permet aussi de se familiariser avec de nouvelles constructions mathématiques et comprendre les propriétés fondamentales qui caractérisent ces ensembles. Il a fallu beaucoup de temps pour reconnaître ces propriétés fondamentales et c'est le XXe siècle qui a regroupé ces propriétés en « structures mathématiques » qui aujourd'hui portent les noms de *groupes*, *anneaux*, *corps*, etc. Le chapitre notera au passage ces structures qui seront étudiées plus en profondeur dans un chapitre ultérieur.

3.1 Les entiers naturels

Il y a généralement deux façons d'introduire l'ensemble $\mathbb{N}$ des entiers naturels. La première, axiomatique, postule l'existence de cet ensemble avec un certain nombre de propriétés. Cette approche, que ce chapitre présente, est due au mathématicien italien Peano [1] et au mathématicien allemand Dedekind [2]. Une seconde approche part de l'ensemble des nombres réels $\mathbb{R}$, au préalable construit par une axiomatique appropriée, puis définit $\mathbb{N}$ comme étant le plus petit sous-ensemble inductif de $\mathbb{R}$, c'est-à-dire le plus petit (au sens de l'inclusion) vérifiant le fait que ses sous-ensembles non vides contiennent toujours un plus petit élément. (Cette propriété n'est pas vérifiée par d'autres ensembles de nombres, par exemple l'ensemble des nombres rationnels. Cet ensemble possède un sous-ensemble , celui des rationnels positifs, qui ne contient pas de plus petit élément.)

1. Giuseppe Peano (1858-1932). Mathématicien italien. Ses axiomes ont été publiés en 1889.
2. Richard Dedekind (1831-1916). Un des concepteurs (notamment avec Cantor) de la théorie moderne des ensembles.

Nous aurons besoin des concepts suivants :

Rappel

- fonction, fonction injective.

L'*ensemble des entiers naturels* (ou entiers non négatifs) $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ peut être construit à partir d'une courte liste d'axiomes. Ces axiomes, appelés *axiomes de Peano*, ont eu un impact majeur sur le développement axiomatique des mathématiques actuelles. Les voici.

Définition 5 (Les axiomes de Peano)**.** *Il existe un ensemble* $\mathbb{N}$ *muni d'une fonction* $s : \mathbb{N} \to \mathbb{N}$ *ayant les propriétés suivantes :*

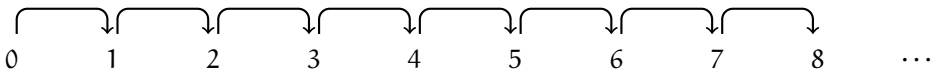
(P1) Il existe un élément $0 \in \mathbb{N}$ *tel que* $0 \neq s(n)$ *pour tout* $n \in \mathbb{N}$*.*

(P2) La fonction s *est injective.*

(P3) (Axiome de récurrence). Tout sous-ensemble E *de* $\mathbb{N}$ *contenant* 0 *et tel que* $s(n) \in E$ *si* $n \in E$ *coïncide avec* $\mathbb{N}$*.*

La paire $(\mathbb{N}, s)$ *est appelée le système des entiers naturels.*

La fonction s est appelée la fonction « successeur ». Avec les noms et caractères usuels pour les éléments de cet ensemble $\mathbb{N}$ ($0 =$ zéro, $1 =$ un, $2 =$ deux, ...), la fonction successeur donne $s(0) = 1$, $s(1) = 2$, $s(2) = 3$, et ainsi de suite. Ainsi $s(n)$ est l'entier suivant n. Les deux premiers axiomes peuvent être mis en mots comme suit. L'axiome (P1) énonce que l'entier 0 est le seul élément de $\mathbb{N}$ à ne pas avoir de prédecesseur (ou encore ne suit aucun autre élément de $\mathbb{N}$). (L'unicité de l'entier n'ayant pas de prédécesseur est démontrée comme suit. Supposons $\hat{0}$ un élément distinct de 0 pour lequel il n'existe aucun $n \in \mathbb{N}$ tel que $s(n) = \hat{0}$. Alors l'ensemble $E \subset \mathbb{N}$ défini par $E = \{0, s(0), s(s(0)), \ldots\}$ contient 0 et satisfait donc aux conditions énoncées dans (P3). Cependant E ne contient pas $\hat{0}$ et ne peut donc pas coïncider avec $\mathbb{N}$. Donc un tel élément $\hat{0}$ ne peut exister dans $\mathbb{N}$.) L'axiome (P2) dit que, si m et n ont le même successeur ($s(m) = s(n)$), alors ils sont égaux ($m = n$). Mais, attention, les noms usuels (zéro, un, deux, ...) ne sont pas nécessaires ; le nom d'un seul élément est fixé, l'élément 0. (Dans d'autres versions, ce nom demeure libre.) L'exercice 1 montrera que la paire $(\mathbb{N}, s)$ peut correspondre à d'autres ensembles. La fonction successeur peut être visualisée par l'utilisation de flèches, une flèche $a \to b$ indiquant que $s(a) = b$. Ainsi



Le dernier axiome (P3) mène au *principe d'induction*.

Théorème 1. *Soit un ensemble d'énoncés logiques* $\{p(n), n \in \mathbb{N}\}$ *étiquetés par les éléments de l'ensemble* $(\mathbb{N}, s)$*. Alors, si*

(i) $p(0)$ *est vraie et*

(ii) $p(n)$ *est vraie* $\Rightarrow p(n+1)$ *est vraie,*

alors $p(n)$ *est vraie pour tout* $n \in \mathbb{N}$*, c'est-à-dire l'ensemble de vérité de* p *est tout* $\mathbb{N}$*.*

Preuve. Soit E l'ensemble des entiers n pour lesquels les énoncés $p(n)$ sont vrais :

$$E = \{n \mid p(n) \text{ est vrai}\}.$$

L'hypothèse *(i)* affirme que E contient l'élément 0 ; l'hypothèse *(ii)*, elle, dit que si n est dans E (c'est-à-dire si $p(n)$ est vrai), alors $n+1$ y est aussi (c'est-à-dire que $p(n+1)$ est vrai). Donc l'ensemble E satisfait l'énoncé de l'axiome (P3) et est donc l'ensemble $\mathbb{N}$ en entier : $E = \mathbb{N}$. Ainsi l'énoncé logique $p(n)$ est vrai pour tous les $n \in \mathbb{N}$. □

Voici maintenant la construction des propriétés de l'ensemble des nombres naturels $(\mathbb{N}, s)$ tel que défini à partir des axiomes de Peano. Cette méthode (appelée la méthode axiomatique) trouve ses origines chez Euclide. La preuve de ces propriétés est parfois longue ; nous en donnerons un exemple. Par la suite, l'ensemble des naturels sera noté simplement $\mathbb{N}$, même si la fonction successeur s jouera un rôle fondamental dans les définitions de $+$ et $\times$.

L'addition **—** Soit a un élément de $\mathbb{N}$ différent de 0 (donc autre que l'élément minimal). L'axiome (P3) montre que a est le successeur d'un élément b ($a = s(b)$). L'élément b est appelé l'antécédent ou le prédécesseur de a et est noté $a-1$. Remarquer que cette écriture n'a pas de sens si $a = 0$, puisque ce dernier n'a pas d'antécédent (n'est le successeur d'aucun naturel d'après (P1)).

Étant donné deux entiers naturels a et n, l'addition est définie par récurrence comme suit :
— si $n = 0$: $a + n = a$;
— si $n \neq 0$: $a + n = s(a + (n-1))$.
Ainsi, si le successeur de a est noté $a+1$, la somme $a+n$ consiste à prendre n fois le successeur de a ;

$$\begin{aligned} a + n &= s(a + (n-1)) = s(s(a + ((n-1)-1))) \\ &= \ldots = s(s(\ldots(s(a + (0))\ldots))) \\ &= \underbrace{s(s(\ldots(s}_{n \text{ fois}}(a)\ldots))) = ((\ldots((\underbrace{a+1}_{n \text{ fois}}) + 1)\ldots) + 1)). \end{aligned}$$

Proposition 2. *L'opération d'addition* $+$ *sur* $\mathbb{N}$ *a les propriétés suivantes :*

(i) 0 *est un neutre :* $0 + a = a + 0 = a$ *;*

(ii) communativité : $a + b = b + a$ *;*

(iii) associativité : $(a + b) + c = a + (b + c)$ *;*

qui valent pour tous les éléments $a, b, c \in \mathbb{N}$*.*

Les preuves de ces propriétés sont fort laborieuses ! Nous n'en donnons que quelques-unes.

Preuve. Soit $p(n), n \in \mathbb{N}$, les énoncés logiques $n+0 = 0+n = n$. Montrer que 0 est un élément neutre pour l'opération $+$ consiste à montrer la véracité des énoncés $p(n)$, pour tout $n \in \mathbb{N}$. L'énoncé $p(0)$ (qui dit $0+0 = 0+0 = 0$) est vrai puisqu'un nombre est toujours égal à lui-même et par la définition de $a + n$ lorsque $n = 0$. Supposons maintenant que l'énoncé pour n soit vrai : $p(n)$ est vrai, c'est-à-dire $0 + n = n + 0 = n$. Étudions les deux membres de l'égalité de l'énoncé $p(n + 1)$. D'abord l'égalité de droite suit de la première ligne de la définition de l'addition : $(n + 1) + 0 = n + 1$. L'égalité de gauche se développe comme suit :

$$0 + (n + 1) = s(0 + n) \overset{\star}{=} s(n + 0) = s(n) = n + 1$$

où « $\star$ » indique l'utilisation de l'hypothèse d'induction ($p(n)$ est vrai). Donc $(n + 1) + 0 = 0 + (n + 1) = n + 1$ est vraie si $n + 0 = 0 + n = n$ l'est, ou encore, $p(n + 1)$ est vrai si $p(n)$ l'est. Par le principe d'induction, tous les énoncés $p(n)$ sont vrais et l'élément 0 est donc le neutre pour l'addition. □

La preuve précédente a aussi montré que l'addition de n'importe quel nombre avec 0 est commutative : $0 + n = n + 0$ pour tout $n \in \mathbb{N}$. Mais il reste pas mal de travail pour montrer la commutativité et l'associativité de l'addition pour tous les entiers. Nous les tiendrons pour acquises.

La multiplication — Tout comme l'addition, la multiplication est définie par récurrence. Soit $a \in \mathbb{N}$ un élément fixé quelconque. On définit l'opération $a \cdot n$ comme suit :

— si $n = 0 : a \cdot n = 0$;
— si $n \neq 0 : a \cdot n = (a \cdot (n - 1)) + a$.

On notera que la multiplication des entiers naturels n'est pas à proprement parler une opération nouvelle. Elle est définie à partir de l'addition. Les propriétés qui suivent sont connues. À partir des propriétés de l'addition énoncées dans le théorème précédent, les preuves des énoncés ci-dessous sont plus faciles. Nous en donnons un exemple.

Théorème 3. *Le triplet* $(\mathbb{N}, +, \cdot)$ *défini ci-dessous possède les propriétés :*

(i) $s(0) = 1$ *est un neutre pour* $\cdot$ *:* $1 \cdot a = a \cdot 1 = a$;

(ii) communativité : $a \cdot b = b \cdot a$;

(iii) associativité : $(a \cdot b) \cdot c = a \cdot (b \cdot c)$;

(iv) distributivité de $\cdot$ *sur* $+$ *:* $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$

pour tous les éléments $a, b, c \in \mathbb{N}$.

Preuve. Soient $p(n), n \in \mathbb{N}$, les énoncés logiques $(a + b) \cdot n = (a \cdot n) + (b \cdot n)$. L'énoncé $p(0)$ est vrai puisque, par la première partie de la définition de $\cdot$, le membre de gauche de cet énoncé est 0 et le membre de droite est $0 + 0$ qui est aussi 0 par la définition de l'addition. Supposons

la véracité de $p(n-1)$. Alors

$$\begin{aligned}(a+b)\cdot n &\overset{1}{=} ((a+b)\cdot(n-1))+(a+b)\\ &\overset{2}{=} (a\cdot(n-1)+b\cdot(n-1))+(a+b)\\ &\overset{3}{=} [(a\cdot(n-1))+a]+[(b\cdot(n-1))+b]\\ &\overset{4}{=} a\cdot n+b\cdot n\end{aligned}$$

où chacune des étapes se justifie comme suit : l'étape 1 est la définition de la multiplication par n, l'étape 2 utilise l'hypothèse d'induction (l'énoncé $p(n)$ est vrai), l'étape 3 suit par la commutativité et l'associativité de l'addition (théorème 2) et, enfin, l'étape 4 utilise à nouveau la définition de la multiplication. □

L'exponentiation — L'exponentiation est un cas particulier de la multiplication. Mais on peut la définir directement par récurrence. Soit a un entier naturel différent de 0. Alors le symbole a^n est défini par

— si $n = 0$: $a^0 = 1$;
— si $n \neq 0$: $a^n = (a^{n-1})\cdot a$.

Relation d'ordre sur $\mathbb{N}$ — Dans la construction axiomatique de $\mathbb{N}$, la relation d'ordre habituelle $\leq$ est formalisée comme suit. Soit $a, b \in \mathbb{N}$. On écrit $a \leq b$ (ou $b \geq a$) s'il existe $c \in \mathbb{N}$ tel que $a + c = b$. Si $a \leq b$ et $a \neq b$, on écrit $a < b$ (ou $b > a$).

Théorème 4. *L'ensemble* $\mathbb{N}$ *muni de la relation* $\leq$ *est un ensemble totalement ordonné, c'est-à-dire :*

(i) antisymétrie : si $a \leq b$ *et* $b \leq a$, *alors* $a = b$;
(ii) transitivité : si $a \leq b$ *et* $b \leq c$, *alors* $a \leq c$;
(iii) réflexivité : $a \leq a$ *et*
(iv) totalité : $a \leq b$ *ou* $b \leq a$,

pour tout a, b *et* c.

Preuve. À nouveau, seules certaines de ces propriétés sont prouvées. Pour montrer l'antisymétrie, supposons l'existence d'entiers c et d tels que $a + c = b$ et $b + d = a$. Alors $a + (c + d) = b + d = a$ par l'associativité de $+$. L'unicité du neutre (voir l'exercice 2 (b)) implique $c + d = 0$. Si d n'est pas 0, alors d possède un prédécesseur et $0 = c + d = s(c + (d - 1))$. Ceci montre que 0 possède un prédécesseur, une contradiction. Ainsi $d = 0$ et $c + 0 = 0$ implique, à nouveau par l'unicité du neutre, que $c = 0$. Donc $a = b$. La réflexivité suit du fait que 0 est un élément de $\mathbb{N}$ et que $x + 0 = x$, c'est-à-dire que $x \leq x$. Pour la transitivité, les relations $a \leq b$ et $b \leq c$ assurent l'existence d'éléments d et $e \in \mathbb{N}$ tels que $a + d = b$ et $b + e = c$. Alors $a + (d + e) = (a + d) + e = b + e = c$ et donc $a \leq c$. □

Le principe du bon ordre — L'induction mathématique est généralement jugée difficile au premier abord, car elle semble être ni intuitive ni naturelle. Pourtant, elle est équivalente à un principe (dit du bon ordre) qui, non seulement est intuitif, mais semble tellement naturel que

d'aucuns se demandent pourquoi il faut le démontrer. On pourrait donc prendre ce dernier comme axiome et en déduire le principe d'induction comme théorème.

Théorème 5 (Principe du bon ordre de $\mathbb{N}$)**.** *Tout sous-ensemble non vide de $\mathbb{N}$ contient un plus petit élément.*

Preuve. (Par induction.) Soit S un sous-ensemble non vide de $\mathbb{N}$ et supposons qu'il ne contienne pas de plus petit élément. Soit E l'ensemble des entiers naturels qui n'appartiennent pas à S, c'est-à-dire le complément de S dans $\mathbb{N}$. Soit l'énoncé logique $p(n)$ disant « les entiers $0, 1, \ldots, n$ sont dans E ».

Clairement l'énoncé $p(0)$ est vrai car, 0 étant le plus petit élément de $\mathbb{N}$, s'il était dans S, il serait son plus petit élément.

Supposons maintenant que $p(n)$ soit vrai : l'ensemble $\{0, 1, \ldots, n\}$ est un sous-ensemble de E. Alors $n + 1$ doit également être dans E, sinon il serait le plus petit élément de S qui n'a pas de plus petit élément. Donc $\{0, 1, \ldots, n, n + 1\}$ est un sous-ensemble de E et $p(n + 1)$ est également vraie. Ainsi E est un ensemble contenant 0 et qui, s'il contient n, contient aussi $n+1$. Par définition de $\mathbb{N}$, $E = \mathbb{N}$. Ceci entraîne que S est vide, ce qui est contraire à l'hypothèse. □

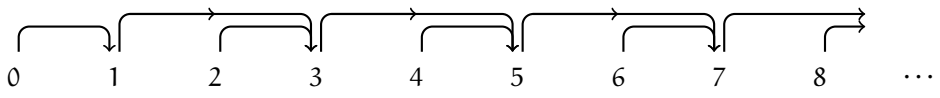
Finalement nous énonçons sans preuve l'équivalence annoncée.

Théorème 6. *Le principe d'induction et le principe du bon ordre sont équivalents.*

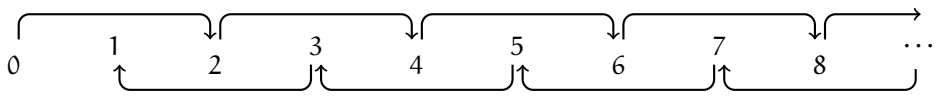
EXERCICES

1. Voici des ensembles (infinis) sur lesquels une définition d'une fonction $s : \mathbb{N} \to \mathbb{N}$ est dessinée : une flèche allant de a à b signifie que $s(a) = b$. Laquelle de ces paires $(\mathcal{E}, s)$ satisfont les trois axiomes de $(\mathbb{N}, s)$? Si une paire ne satisfait pas à la définition, dire quel(s) axiome(s) n'est (ne sont) pas satisfait(s) ? Attention : les symboles utilisés pour étiqueter les éléments de ces ensembles $\mathcal{E}$ ne devraient pas vous induire en erreur. Vous pouvez les changer à votre guise.

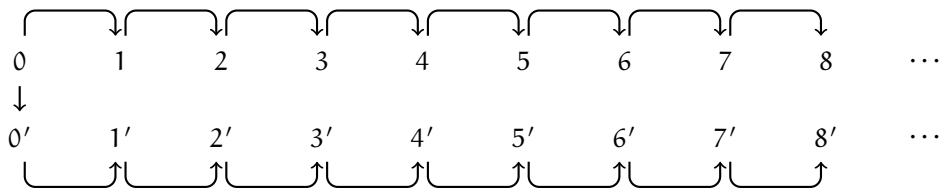
(a)



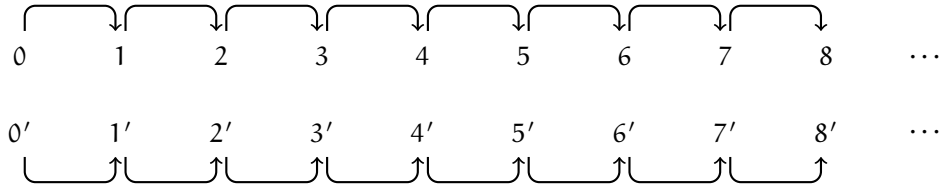
(b)



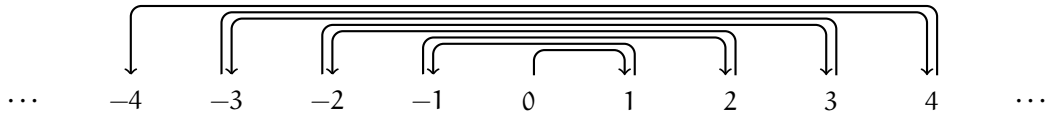
(c)



(d)



(e)



2. **(a)** Montrer à partir de la définition des entiers naturels $(\mathbb{N}, s)$: soit $a, b, c \in \mathbb{N}$ vérifiant $a + c = b + c$. Alors $a = b$.

(b) Utiliser la proposition 2 pour montrer que 0 est le seul élément de $\mathbb{N}$ qui est un neutre pour l'addition. (En d'autres mots, si $\hat{0} \in \mathbb{N}$ et vérifie $\hat{0} + n = n + \hat{0} = n$ pour tout $n \in \mathbb{N}$, alors $\hat{0} = 0$.)

3. Le théorème 3 énonce les propriétés du neutre, de la commutativité et de l'associativité de la multiplication des entiers et, enfin, de la distributivité. Le texte a donné la preuve de la distributivité de la multiplication par la droite d'une somme. (Attention : la preuve n'a cependant pas montré que $c \cdot (a + b) = c \cdot a + c \cdot b$ est vrai !) Montrer les énoncés suivants en utilisant que la proposition 2 et ce qui a été déjà montré (dans les notes ou par vous !) pour la multiplication.

(a) Montrer que $1 \cdot n = n$ pour tout $n \in \mathbb{N}$. Puis montrer que $n \cdot 1 = n$ pour tout $n \in \mathbb{N}$.

(b) Le développement ci-dessous montre la commutativité de la multiplication. Justifier par l'énoncé approprié chacune des étapes. Soit $p(n)$ l'énoncé $a \cdot b = b \cdot a$ pour tout $a, b \leq n$. Les

énoncés $p(0)$ et $p(1)$ ont déjà été établis. Soit $a + b \leq n$. Si $p(n-1)$ est vrai, alors

$$\begin{aligned} a \cdot b &= a \cdot (b-1) + a \\ &= (b-1) \cdot a + a \\ &= ((b-1) \cdot (a-1) + (b-1)) + a \\ &= (b-1) \cdot (a-1) + (a + (b-1)) \\ &= ((b-1) \cdot (a-1) + 1 \cdot (a-1)) + b \\ &= ((b-1) + 1) \cdot (a-1)) + b \\ &= b \cdot a. \end{aligned}$$

4. Voici une preuve par induction. Est-elle juste ?

Théorème 7. *Dans un champ, les vaches sont toujours de même couleur.*

Preuve. Soient $p(n), n \in \mathbb{N}$, les énoncés logiques « dans un champ contenant n vaches, ces vaches sont de même couleur ». Clairement les énoncés $p(0)$ et $p(1)$ sont vrais. Supposons maintenant l'énoncé $p(n)$ vrai et soit $\{v_1, v_2, \ldots, v_{n+1}\}$ l'ensemble des $n+1$ vaches d'un champ contenant $n+1$ vaches. Le sous-ensemble $\{v_1, v_2, \ldots, v_n\}$ est de même couleur puisqu'il contient n vaches (énoncé $p(n)$!). Le sous-ensemble $\{v_2, \ldots, v_n, v_{n+1}\}$ contient lui aussi n vaches et ces vaches sont donc toutes de la même couleur (encore l'énoncé $p(n)$). Puisque ces deux sous-ensembles contiennent des vaches de même couleur et ont des vaches en commun, alors l'ensemble original $\{v_1, v_2, \ldots, v_{n+1}\}$ ne contient que des vaches de même couleur. Ainsi $p(n)$ est vrai implique que $p(n+1)$ est vrai. □

5. Prouver par induction.

(a) $1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2}$.

(b) À partir d'un certain rang n que l'on déterminera, $2^n < n!$.

(c) $21 \mid (4^{n+1} + 5^{2n-1})$ pour tout entier $n \geq 1$.

(d) Pour tout $a, b, n \in \mathbb{N}$, on a $(ab)^n = a^n b^n$.

6. Montrer les énoncés suivants.

(a) $0 < a$ pour tout élément non nul $a \in \mathbb{N}$. (On dit que 0 est le minimum, ou le plus petit élément, de $\mathbb{N}$.)

(b) Si $a < b$, alors $a + 1 \leq b$ et $a \leq b - 1$.

(c) Si $a \leq b$, alors $a + c \leq b + c$ pour tout $c \in \mathbb{N}$.

(d) $a \leq b \Rightarrow ac \leq bc$ pour tout $c \in \mathbb{N}$.

À cause des propriétés **(c)** et **(d)**, on dit que la relation d'ordre est compatible avec l'addition et la multiplication.

3.2 Les entiers relatifs $\mathbb{Z}$ et les rationnels $\mathbb{Q}$

Nous savons que la soustraction et la division d'entiers naturels ne donnent un entier naturel que pour certaines paires d'entiers. Par exemple, la soustraction $m - n$ ne sera dans $\mathbb{N}$ que si $m \geq n$. Similairement, la division de m par n ne sera dans $\mathbb{N}$ que si n est un facteur de m (ou comme nous l'avons écrit plutôt, si $n \mid m$). Ainsi $\mathbb{N}$ n'est pas un ensemble de nombres fermé sous la soustraction ni la division, qui sont les opérations inverses de l'addition et la multiplication. La construction des entiers relatifs $\mathbb{Z}$ ajoute des nombres à l'ensemble $\mathbb{N}$ de façon à ce que *(i)* la soustraction de n'importe quelle paire d'entiers dans $\mathbb{Z}$ demeure dans $\mathbb{Z}$ et *(ii)* que si la paire m, n est formée d'entiers de $\mathbb{N}$ satisfaisant $m \geq n$, alors la soustraction $m - n$ de m et n, vus comme éléments de $\mathbb{Z}$, donne le même résultat que leur soustraction, vus comme éléments de $\mathbb{N}$.

La construction de l'ensemble $\mathbb{Q}$ des rationnels réalise un programme similaire : il étend l'ensemble $\mathbb{Z}$ des entiers relatifs pour que la division soit définie pour toute paire de nombres de $\mathbb{Z}$ (en autant que le diviseur ne soit pas nul) et que le résultat coïncide à celui dans $\mathbb{Z}$ si la division de cette paire était définie dans cet ensemble. Ce type d'extension ($\mathbb{N} \to \mathbb{Z}$ et $\mathbb{Z} \to \mathbb{Q}$) est utilisé souvent en mathématiques. Les techniques pour produire l'extension ne sont pas toujours les mêmes, mais pour les deux que nous discuterons dans la présente section, la technique est la même et elle utilisera :

Rappel

- les relations d'équivalence.

Les constructions de $\mathbb{Z}$ et de $\mathbb{Q}$ sont si semblables que nous ne ferons que celle pour $\mathbb{Q}$, en supposant que celle pour $\mathbb{Z}$ a déjà été complétée. (Cette dernière sera faite en exercice.)

Avant de faire la construction formelle, il est utile de réfléchir à un aspect des fractions déjà introduit à l'école primaire. Il s'agit du fait qu'un nombre rationnel, qu'il soit entier ou non, possède plusieurs représentations. Par exemple, les nombres 2 et $\frac{1}{2}$ sont notés indifféremment par

$$2 = \frac{4}{2} = \frac{-18}{-9} = \frac{54/9}{39/13} = \frac{246\,913\,578}{123\,456\,789} = \cdots$$
$$\frac{1}{2} = \frac{2}{4} = \frac{-9}{-18} = \frac{39/13}{54/9} = \frac{123\,456\,789}{246\,913\,578} = \cdots$$

L'équivalence entre ces notations est maîtrisée très tôt même si, au point de vue mathématique, elle n'a pas de définition formelle. Une telle définition n'est pas trop difficile à donner. Elle est

basée sur l'observation que tout nombre rationnel est habituellement donné par deux entiers relatifs. Et si un entier relatif, tel que 2, peut être écrit comme un seul entier, il peut aussi être écrit comme un quotient, par exemple $\frac{2}{1}$. Qu'est-ce qui fait que les deux nombres

$$\frac{n_1}{d_1} = \frac{2}{1} \qquad \text{et} \qquad \frac{n_2}{d_2} = \frac{-18}{-9}$$

soient identifiés ? C'est que les numérateurs et dénominateurs de ces deux fractions vérifient

$$n_1 d_2 = n_2 d_1.$$

Et cette relation sera vérifiée pour toute paire de quotients $\frac{n_1}{d_1}$ et $\frac{n_2}{d_2}$ que nous avons appris à identifier. Nous sommes prêts à formaliser la construction de $\mathbb{Q}$.

Définition 6. *Soit* $X = \{(n, d) \,|\, n \in \mathbb{Z} \text{ et } d \in \mathbb{Z}^\star\}$ *et soit* $\sim$ *la relation d'équivalence sur* X *donnée par*

$$(n_1, d_1) \sim (n_2, d_2) \qquad \Longleftrightarrow \qquad n_1 \times d_2 = n_2 \times d_1.$$

L'ensemble $\mathbb{Q}$ *est l'ensemble des classes d'équivalence de cette relation* $\sim$ *sur* X*.*

La définition affirme que $\sim$ est une relation d'équivalence. En voici la vérification. La relation $\sim$ est réflexive car, si $(n, d) \in X$, alors $n \times d = n \times d$ et donc $(n, d) \sim (n, d)$. Elle est symétrique car, si (n_1, d_1) et $(n_2, d_2) \in X$, alors

$$(n_1, d_1) \sim (n_2, d_2) \quad \Rightarrow \quad n_1 \times d_2 = n_2 \times d_1 \quad \Rightarrow \quad n_2 \times d_1 = n_1 \times d_2 \quad \Rightarrow \quad (n_2, d_2) \sim (n_1, d_1).$$

Enfin, elle est transitive : supposons que $(n_1, d_1) \sim (n_2, d_2)$ et que $(n_2, d_2) \sim (n_3, d_3)$ et donc

$$n_1 \times d_2 = n_2 \times d_1 \qquad \text{et} \qquad n_2 \times d_3 = n_3 \times d_2.$$

Alors

$$\begin{aligned}(n_1 \times d_2) \times d_3 &= (n_2 \times d_1) \times d_3 \\ &= d_1 \times (n_2 \times d_3) \\ &= d_1 \times (n_3 \times d_2)\end{aligned}$$

et, puisque d_2 n'est pas nul (les éléments de X sont de la forme (n, d) avec $d \neq 0$), alors

$$n_1 \times d_3 = n_3 \times d_1$$

et $\sim$ est transitive et donc une relation d'équivalence.

La définition des nombres rationnels est donc telle que le nombre rationnel $\frac{1}{2}$ est en fait une classe d'équivalence (un ensemble infini dans le cas présent) :

$$\overline{(1, 2)} = \big\{(1,)2, (2, 4), (-9, -18), (123\,456\,789, 246\,913\,578), \dots\big\}.$$

(Évidemment, en pratique, on utilise simplement le symbole $\frac{1}{2}$ pour cette classe d'équivalence même si, par construction, il y a une infinité de représentants dans cette classe.)

L'addition dans $\mathbb{Q}$ — La définition ci-dessus de l'ensemble $\mathbb{Q}$ ne dit pas comment ni additionner ni multiplier deux classes d'équivalence. Nous connaissons cependant quelles doivent être les définitions de ces opérations. Par exemple, pour l'addition, nous devons avoir

$$\frac{n_1}{d_1} + \frac{n_2}{d_2} = \frac{n_1 d_2 + n_2 d_1}{d_1 d_2} \qquad (+_{\mathbb{Q}1})$$

et donc, en termes de classes d'équivalence :

$$\overline{(n_1, d_1)} + \overline{(n_2, d_2)} = \overline{(n_1 d_2 + n_2 d_1, d_1 d_2)}. \qquad (+_{\mathbb{Q}2})$$

Cette définition a l'avantage de définir une opération clairement commutative :

$$\overline{(n_1, d_1)} + \overline{(n_2, d_2)} = \overline{(n_1 d_2 + n_2 d_1, d_1 d_2)} = \overline{(n_2 d_1 + n_1 d_2, d_2 d_1)} = \overline{(n_2, d_2)} + \overline{(n_1, d_1)}.$$

Mais il faut se demander si elle est bien définie : le résultat sera-t-il le même si un autre représentant de la classe d'équivalence de $\overline{(n_1, d_1)}$? Par exemple, supposons que $(n_1, d_1) \sim (n_0, d_0)$. Est-ce que

$$\overline{(n_1, d_1)} + \overline{(n_2, d_2)} = \overline{(n_0, d_0)} + \overline{(n_2, d_2)}?$$

Voici deux reformulations de la même question. Après utilisation de la définition de l'addition de deux classes d'équivalence, elle devient

$$\overline{(n_1 d_2 + n_2 d_1, d_1 d_2)} \stackrel{?}{=} \overline{(n_0 d_2 + n_2 d_0, d_0 d_2)}$$

et, par la définition de la relation d'équivalence $\sim$

$$(n_1 d_2 + n_2 d_1) \times (d_0 d_2) \stackrel{?}{=} (n_0 d_2 + n_2 d_0) \times (d_1 d_2).$$

Puisque $(n_1, d_1) \sim (n_0, d_0)$, c'est-à-dire $n_0 d_1 = n_1 d_0$, le membre de gauche de cette dernière question peut être transformé comme suit

$$\begin{aligned}(n_1 d_2 + n_2 d_1) \times (d_0 d_2) &= (n_1 d_0 d_2 + n_2 d_0 d_1) \times d_2 \\ &= (n_0 d_1 d_2 + n_2 d_0 d_1) \times d_2 \\ &= (n_0 d_2 + n_2 d_0) \times (d_1 d_2)\end{aligned}$$

qui est l'égalité que nous devions montrer. Ainsi, quel que soit le représentant pris pour faire l'addition $(+_{\mathbb{Q}2})$, la classe d'équivalence obtenue sera la même. [3]

Après cette vérification, les autres propriétés de l'addition sur $\mathbb{Q}$ sont aisément vérifiées : l'associativité, l'existence d'un neutre et l'existence d'un inverse pour tout élément $\frac{n}{d} \leftrightarrow \overline{(n, d)} \in \mathbb{Q}$. Ce sera un exercice à la fin de la section.

La multiplication dans $\mathbb{Q}$ — La multiplication est facile à définir. Elle doit « imiter » la règle usuelle

$$\frac{n_1}{d_1} \times \frac{n_2}{d_2} = \frac{n_1 \cdot n_2}{d_1 \cdot n_2}$$

3. Les deux formules $(+_{\mathbb{Q}1})$ et $(+_{\mathbb{Q}2})$ sont équivalentes. Il est possible que vous n'ayez jamais pris conscience que la vérification que nous venons de faire doit être faite tant pour l'une que pour l'autre.

et donc

$$\overline{(n_1, d_1)} \times \overline{(n_2, d_2)} = \overline{(n_1 \cdot n_2, d_1 \cdot d_2)}. \qquad (\times_{\mathbb{Q}2})$$

Les propriétés usuelles (commutativité, associativité, existence d'un neutre, existence d'un inverse pour tout élément différent de l'élément nul) découlent facilement de cette définition. Il faut cependant vérifier que la définition $(\times_{\mathbb{Q}2})$ est bien définie, c'est-à-dire, si un autre représentant de la classe d'équivalence de $\overline{(n_1, d_1)}$, comme (n_0, d_0), est utilisé, le résultat de la multiplication demeure le même. Il faut donc montrer que les classes d'équivalence

$$\overline{(n_0 \cdot n_2, d_0 \cdot d_2)} \qquad \text{et} \qquad \overline{(n_1 \cdot n_2, d_1 \cdot d_2)}$$

sont égales. Puisque (n_0, d_0) et (n_1, d_1) appartiennent à la même classe, $n_0 d_1 = n_1 d_0$ et donc

$$(n_1 \cdot n_2) \times (d_0 \cdot d_2) = (n_0 \cdot n_2) \times (d_1 \cdot d_2)$$

qui termine la preuve.

Relation d'ordre sur $\mathbb{Q}$ **—** Lequel des deux nombre suivants est le plus grand :

$$\frac{21}{31} \quad \text{et} \quad \frac{25}{37} \, ?$$

Et de ceux-ci :

$$\frac{25\,877}{119\,287} \quad \text{et} \quad \frac{8\,101}{35\,998} \, ?$$

Quelles que soient les réponses [4], ces questions en soulèvent une autre : est-il possible de déterminer l'ordre sur $\mathbb{Q}$ en ne faisant que des opérations entre entiers relatifs, c'est-à-dire sans faire de division ? La réponse est simple : il suffit de faire un dénominateur commun. Par exemple

$$\frac{21}{31} = \frac{21 \cdot 37}{31 \cdot 37} = \frac{777}{31 \cdot 37} \geq \frac{25}{37} = \frac{25 \cdot 31}{37 \cdot 31} = \frac{775}{31 \cdot 37}.$$

L'ordre sur $\mathbb{Q}$ peut donc être aisément défini en copiant ce calcul. Soient $\overline{(n_1, d_1)}$ et $\overline{(n_2, d_2)}$ deux éléments de $\mathbb{Q}$. Sans perte de généralité, il est possible de supposer que d_1 et d_2 sont positifs. S'ils ne l'étaient pas, il suffirait de considérer l'élément $(-n_1, -d_1) \sim (n_1, d_1)$. Alors, si d_1 et d_2 sont positifs, l'ordre sur $\mathbb{Q}$ est donné par

$$\overline{(n_1, d_1)} \leq \overline{(n_2, d_2)} \qquad \Longleftrightarrow \qquad n_1 d_2 \leq n_2 d_1. \qquad (\leq_{\mathbb{Q}})$$

Cette définition fait de l'ensemble $\mathbb{Q}$ un ensemble bien ordonné.

La structure algébrique $(\mathbb{Q}, +, \times, \leq)$ **—** Pour résumer les propriétés de l'ensemble $\mathbb{Q}$ muni des opérations $+$ et $\times$ et de l'ordre $\leq$, nous introduisons une définition qui reviendra souvent par la suite.

Définition 7. *Un ensemble* E *muni d'une opération binaire* $*$ *qui, à chaque paire* $a, b \in E$ *associe un élément* $a * b \in E$*, est un* groupe *si les propriétés suivantes sont satisfaites :*

(G1) associativité : $(a * b) * c = a * (b * c)$*;*

4. $\frac{21}{31} \simeq 0,6774$ et $\frac{25}{37} \simeq 0,6757$; $\frac{25\,877}{119\,287} \simeq 0,217$ et $\frac{8\,101}{35\,998} \simeq 0,225$.

(G2) existence d'un neutre : il existe un élément $e \in E$ *tel que* $e * a = a * e = a$*;*

(G3) existence d'un inverse : pour tout $a \in E$*, il existe un élément* $a' \in E$ *tel que* $a*a' = a'*a = e$ *pour tout* $a, b, c \in E$*.*

Enfin si l'opération binaire $*$ *est commutative (*$a * b = b * a$ *pour tout* a *et* b *dans* E*), le groupe* E *est dit abélien.*

L'ensemble $\mathbb{Q}$ donne deux exemples de structure de groupe. Si l'élément 0 dénote la classe d'équivalence $\overline{(0,1)}$, alors $(\mathbb{Q}, +)$ est un groupe avec élément neutre 0. L'inverse de l'élément $\overline{(n,d)}$ est alors $\overline{(-n,d)}$. Enfin, si l'élément 1 dénote la classe d'équivalence $\overline{(1,1)}$, alors $(\mathbb{Q} \setminus \{0\}, \times)$ est un groupe avec élément neutre 1. L'inverse de l'élément $\overline{(n,d)}$ est alors $\overline{(d,n)}$. Nous rencontrerons d'autres groupes au prochain chapitre.

La structure de groupe permet de résumer succinctement les propriétés de $\mathbb{Q}$.

Théorème 8. *La structure algébrique* $(\mathbb{Q}, +, \times, \geq)$ *satisfait les propriétés suivantes :*

(i) $(\mathbb{Q}, +)$ *est un groupe abélien ;*

(ii) $(\mathbb{Q} \setminus \{0\}, \times)$ *est un groupe abélien ;*

(iii) distributivité : $(a + b) \times c = a \times c + b \times c$ *pour tout* $a, b, c \in \mathbb{Q}$*;*

(iv) $(\mathbb{Q}, \geq)$ *est un ensemble totalement ordonné.*

EXERCICES

7. Cet exercice termine les vérifications des propriétés de $\mathbb{Q}$. Vérifier :

(a) l'associativité de $+$ telle que définie par $(+_{\mathbb{Q}2})$;

(b) que $\overline{(0,1)}$ est un neutre additif;

(c) l'existence d'un inverse additif pour tout élément $\overline{(n,d)} \in \mathbb{Q}$;

(d) la commutativité de $\times$ telle que définie par $(\times_{\mathbb{Q}2})$;

(e) l'associativité de $\times$;

(f) que $\overline{(1,1)}$ est un neutre multiplicatif;

(g) l'existence d'un inverse multiplicatif pour tout élément $\overline{(n,d)} \in \mathbb{Q} \setminus \{0\}$;

(h) la distributivité de $\times$ sur $+$;

(i) que l'ordre $\geq$ défini par $(\leq_{\mathbb{Q}})$ ne dépend pas des représentants des classe d'équivalence choisis;

(j) que $\geq$ est un ordre sur $\mathbb{Q}$.

(Il y en a beaucoup... Faites en quelques-uns pour vous assurer que vous avez compris !)

8. **(a)** Quels sont les éléments $\overline{(n,d)}$ qui correspondent à des entiers relatifs ? Et à des entiers naturels ?

(b) Vérifier que l'addition $+$ sur $\mathbb{Q}$ coïncident avec celle sur $\mathbb{Z}$ pour les éléments de $\mathbb{Q}$ qui correspondent aux entiers relatifs.

(c) Même question pour la multiplication sur $\mathbb{Q}$.

9. La construction de $\mathbb{Z}$ à partir de l'ensemble $\mathbb{N}$ des entiers naturels ressemblent beaucoup à celle que nous avons faite pour $\mathbb{Q}$. L'ensemble $\mathbb{Z}$ complète l'ensemble $\mathbb{N}$ de façon à ce que la soustraction $a - b$ existe pour toute paire d'éléments a, b dans $\mathbb{Z}$. À nouveau, deux objets permettent la construction : un ensemble $Y = \{(a, b) \mid a, b \in \mathbb{N}\}$ et une relation $\approx$ sur Y :

$$(a_1, b_1) \approx (a_2, b_2) \qquad \Longleftrightarrow \qquad a_1 + b_2 = a_2 + b_1.$$

(a) Montrer que la relation $\approx$ est une relation d'équivalence.

(b) Soit $\mathbb{Z}$ l'ensemble des classes d'équivalence de $\approx$. Quels sont les éléments $\overline{(a, b)}$ qui correspondent à des entiers naturels ? À quelle classe d'équivalence correpond l'élément $0 \in \mathbb{N}$?

(c) Définir une opération $+$ sur $\mathbb{Z}$ qui, restreinte aux classes correspondant à des éléments de $\mathbb{N}$, coïncide avec l'addition sur $\mathbb{N}$. Vérifier que cette addition est bien définie.

(d) Vérifier les propriétés usuelles de l'addition sur $\mathbb{Z}$.

(e) Définir similairement une opération $\times$ sur $\mathbb{Z}$. Vérifier que cette multiplication est bien définie.

(f) Vérifier les propriétés usuelles de la multiplication sur $\mathbb{Z}$. Est-ce que tout élément de $\mathbb{Z}$ possède un inverse multiplicatif ?

(g) Vérifier la distributivité de $\times$ sur $+$.

(h) Définir un ordre sur $\mathbb{Z}$.

(i) Est-ce que $(\mathbb{Z}, +)$ est un groupe.

(j) Est-ce que $(\mathbb{Z}, \times)$ est un groupe.

3.3 L'ensemble $\mathbb{Z}_n$ des entiers modulo n

Cette section interrompt l'étude des grands ensembles imbriqués $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ (la prochaine section reprendra cette étude). Elle bâtit sur la familiarité, développée à la section précédente, des ensembles définis à l'aide d'une relation d'équivalence et introduit l'ensemble $\mathbb{Z}_n$ des entiers modulo n. Il y a une infinité de ces ensembles, infinité étiquetée par les entiers positifs $n \geq 2$. Il est possible de définir sur chacun des opérations $+$ et $\times$. Et, pour certains n que nous caractériserons, les opérations $-$ et $\div$ seront également définies pour toute paire d'éléments de $\mathbb{Z}_n$.

Certains exemples de $\mathbb{Z}_n$ sont familiers. Le plus commun est $\mathbb{Z}_{24}$ utilisé pour le calcul des heures. Si $\overline{0}$ correspond à minuit, alors $\overline{12}$ sera midi et le milieu de l'après-midi sera autour de

$\overline{15}$. L'heure parisienne est toujours en avance de six heures sur celle de Montréal. Ainsi, quand un Montréalais se lève à 6 heures du matin ($= \overline{6}$), il est déjà midi ($= \overline{12}$) à Paris. Pour obtenir ce $\overline{12}$, une simple addition a été faite : $\overline{6}+\overline{6} = \overline{12}$. Cependant, quand le Montréalais se couche vers dix heures du soir ($= \overline{22}$), l'heure parisienne indique 4 heures du matin ($= \overline{4}$). Ainsi $\overline{22}+\overline{6} = \overline{4}$. La règle d'addition des heures est bien connue : lorsque le résultat d'une addition excède $\overline{23}$, on en retranche un multiple de 24 jusqu'à ce que le résultat soit un élément de l'ensemble $\{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{22}, \overline{23}\}$. Cette opération a déjà été introduite de façon formelle : si le résultat de la somme est a, on cherche r tel que

$$a = q \cdot 24 + r, \qquad \text{avec } r \in \{0, 1, 2, \ldots, 23\},$$

c'est-à-dire on cherche le reste de la division de a par 24. L'heure désirée sera ce reste r.

Rappel

- division avec reste ;
- relation d'équivalence ;
- opération bien définie ;
- théorème de Bézout.

Voici un autre exemple qui sera familier à ceux qui connaissent un peu de musique. Les notes sur un piano portent toutes un nom, même si plusieurs portent le même nom. Par exemple, sur un clavier, les notes consécutives se nomment

$$\ldots, \text{ si, do, do}\sharp, \text{ ré, ré}\sharp, \text{ mi, fa, fa}\sharp, \text{ sol, sol}\sharp, \text{ la, la}\sharp, \text{ si, do, do}\sharp, \text{ ré, } \ldots$$

Les noms importent peu. Ce qui l'est est la constitution des accords, par exemple l'accord majeur. Il est constitué d'une note, de celle à distance quatre vers la droite (= une *tierce majeure* plus haut disent les musiciens) et de celle à distance sept toujours vers la droite (= une *quinte juste*). L'accord majeur dont la première note est do est donc constitué des notes do, mi et sol. Et l'accord dont la première est la est constitué de la, do$\sharp$ et mi. Ainsi les douze noms distincts (do à si) représente les douze notes possibles et les notes des accords sont identifiées par la division avec reste par 12.

Définition de $\mathbb{Z}_n$ — Soit $n \geq 2$ un entier et soit $\equiv$ la relation sur $\mathbb{Z}$ donnée par

$$a \equiv b \bmod n \qquad \Longleftrightarrow \qquad \text{il existe } k \in \mathbb{Z} \text{ tel que } a = k \cdot n + b.$$

Cette relation $\equiv$ est *réflexive* car $a = 0 \cdot n + a$ (c'est-à-dire le choix $k = 0$ indique que a est équivalent à a). Elle est aussi *symétrique* puisque, si $a = k \cdot n + b$, alors $b = (-k) \cdot n + a$ et, maintenant, l'entier relatif à choisir est $-k$ pour obtenir que b est équivalent à a. Enfin elle est *transitive* : si $a \equiv b \bmod n$ et $b \equiv c \bmod n$, c'est qu'il existe k et $\ell \in \mathbb{Z}$ tels que $a = k \cdot n + b$ et $b = \ell \cdot n + c$ et donc

$$a = k \cdot n + b = k \cdot n + \ell \cdot n + c = \underbrace{(k + \ell)}_{\in \mathbb{Z}} \cdot n + c$$

et donc $a \equiv c \bmod n$. Ainsi $\equiv$ est une *relation d'équivalence* sur l'ensemble $\mathbb{Z}$.

Quelles sont les classes d'équivalence de $\equiv$? Ces classes sont les ensembles des entiers différant les uns des autres par un multiple de n. Par exemple, si $n = 5$, il y aura 5 classes d'équivalence, chacune contenant un nombre infini d'éléments :

$$\begin{aligned}
&\{\ldots, -15, -10, -5, 0, 5, 10, 15, \ldots\},\\
&\{\ldots, -14, -9, -4, 1, 6, 11, 16, \ldots\},\\
&\{\ldots, -13, -8, -3, 2, 7, 12, 17, \ldots\},\\
&\{\ldots, -12, -7, -2, 3, 8, 13, 18, \ldots\},\\
&\{\ldots, -11, -6, -1, 4, 9, 14, 19, \ldots\}.
\end{aligned}$$

Tout élément de $\mathbb{Z}$ appartient à une et une seule de ces classes d'équivalence. Si a et b sont dans la même classe d'équivalence, on dit que a est égal à b modulo n et on écrit, comme ci-dessus, $a \equiv b \bmod n$. Il est usuel d'écrire $\overline{a}$ pour la classe d'équivalence $\{\ldots, a - 2n, a - n, a, a + n, a + 2n, \ldots\}$. Ainsi les classes d'équivalence des entiers modulo 5 possèdent plusieurs noms ! La première ci-dessus peut être dénotée $\overline{0}$, mais aussi $\overline{-15}$ et $\overline{98765}$ et $\overline{-67890}$ et la quatrième est $\overline{3} = \overline{-12} = \overline{98768} = \overline{-67887}$. Et puisque $\overline{-12}$ désigne l'ensemble $\{\ldots, -12, -7, -2, 3, 8, 13, 18, \ldots\}$, on a que

$$-12 \in \overline{-12}, \text{ mais aussi } -12 \in \overline{3} \text{ et } 98768 \in \overline{-12} \text{ et } 3 \in \overline{-67887}.$$

Définition 8. *L'ensemble $\mathbb{Z}_n$, aussi noté $(\mathbb{Z}/\equiv)$ et $(\mathbb{Z}/n\mathbb{Z})$, est l'ensemble des classes d'équivalence de la relation d'équivalence $\equiv$ sur $\mathbb{Z}$. L'ensemble $\mathbb{Z}_n$ contient n éléments distincts.*

***Gymnastique* —** Les symboles « $\cdot \equiv \cdot \bmod n$ » se comportent à certains égards comme les symboles « $\cdot = \cdot$ ». Pour ces derniers, on sait que, pour tout $a, b, c, d \in \mathbb{Z}$, les implications logiques suivantes sont vraies :

$$\begin{aligned}
a = b \quad \text{et} \quad c = d \qquad &\Longrightarrow \qquad a + c = b + d,\\
a = b \quad \text{et} \quad c = d \qquad &\Longrightarrow \qquad a \cdot c = b \cdot d.
\end{aligned}$$

Ces relations deviennent les suivantes pour $\mathbb{Z}_n$.

Proposition 9. *Soit $n \geq 2$ et $a \equiv b \bmod n$ et $c \equiv d \bmod n$. Alors*

$$a + c \equiv b + d \bmod n \qquad \textit{et} \qquad a \cdot c \equiv b \cdot d \bmod n.$$

Preuve. Les hypothèses impliquent l'existence de k et ℓ tels que $a = k \cdot n + b$ et $c = \ell \cdot n + d$. Ainsi

$$a + c = (k \cdot n + b) + (\ell \cdot n + d) = \underbrace{(k + \ell)}_{\in \mathbb{Z}} \cdot n + (b + d)$$

et donc

$$a + c \equiv b + d \bmod n.$$

Similairement

$$\begin{aligned} a \cdot c &= (k \cdot n + b) \cdot (\ell \cdot n + d) \\ &= k \cdot \ell \cdot n^2 + \ell \cdot b \cdot n + k \cdot d \cdot n + b \cdot d \\ &= \underbrace{(k \cdot \ell \cdot n + \ell \cdot b + k \cdot d)}_{\in \mathbb{Z}} \cdot n + (b \cdot d) \end{aligned}$$

et donc

$$a \cdot c \equiv b \cdot d \bmod n$$

ce qui termine la preuve. □

Corollaire 10. *Soit* $n \geq 2$ *et* $a \equiv b \bmod n$. *Alors* $a^k \equiv b^k \bmod n$ *pour tout* $k \geq 0$.

Voici un exercice amusant (quoique pas très utile...) [5]. Le corollaire ci-dessus permet de calculer les deux dernières décimales de grands nombres, par exemple 2^{500}. Les deux dernières décimales d'un nombre sont données par le reste de la division de ce nombre par 100. Par exemple

$$2^{10} = 1024 \equiv 24 \bmod 100.$$

Un calcul direct montre que $24 \cdot 24 = 576$ et $76 \cdot 76 = 5776$. Alors

$$\begin{aligned} 2^{20} &= 2^{10} \cdot 2^{10} \equiv 24 \cdot 24 \equiv 76 \bmod 100 \\ 2^{40} &= 2^{20} \cdot 2^{20} \equiv 76 \cdot 76 \equiv 76 \bmod 100 \\ 2^{80} &= 2^{40} \cdot 2^{40} \equiv 76 \cdot 76 \equiv 76 \bmod 100 \\ 2^{160} &= 2^{80} \cdot 2^{80} \equiv 76 \cdot 76 \equiv 76 \bmod 100 \\ 2^{320} &= 2^{160} \cdot 2^{160} \equiv 76 \cdot 76 \equiv 76 \bmod 100 \\ 2^{480} &= 2^{160} \cdot 2^{320} \equiv 76 \cdot 76 \equiv 76 \bmod 100 \\ 2^{500} &= 2^{20} \cdot 2^{480} \equiv 76 \cdot 76 \equiv 76 \bmod 100 \end{aligned}$$

et les deux dernières décimales de 2^{500} sont 76. Impressionant, non ?

L'addition dans $\mathbb{Z}_n$ — L'addition sur $\mathbb{Z}$ permet de définir une opération d'addition sur $\mathbb{Z}_n$ simplement par la règle

$$\overline{a} + \overline{b} \overset{\text{déf}}{=} \overline{a + b}.$$

Mais attention ! Cette définition utilise des représentants des classes d'équivalence pour définir l'opération addition. Que se passe-t-il si d'autres représentants sont choisis ? En d'autres mots l'opération $+$ sur $\mathbb{Z}_n$ est-elle *bien définie* ? Répondre par l'affirmative à cette question consiste en montrer que, si $c \in \overline{a}$ et $d \in \overline{b}$, alors

$$\overline{a} + \overline{b} = \overline{c} + \overline{d}.$$

À nouveau $c \in \overline{a}$ et $d \in \overline{b}$ affirment l'existence de k et $\ell \in \mathbb{Z}$ tels que

$$c = k \cdot n + a \qquad \text{et} \qquad d = \ell \cdot n + b.$$

5. L'exercice 14 donne un exemple de ce genre de calcul qui est plus utile.

Alors

$$c + d = (k + \ell) \cdot n + (a + b) \qquad (\star)$$

et $c + d \in \overline{a + b}$. Ainsi

$$\overline{c} + \overline{d} \overset{\text{déf}}{=} \overline{c + d} \overset{\star}{=} \overline{a + b} \overset{\text{déf}}{=} \overline{a} + \overline{b}.$$

L'addition $+$ est donc bien définie. (Remarquez que cette preuve est pratiquement identique à celle de la proposition 9. Aurions-nous pu l'utiliser sans refaire de calcul ?)

La proposition suivante est aisée.

Proposition 11. *$(\mathbb{Z}_n, +)$ est un groupe, c'est-à-dire que pour tout $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_n$*

(i) $\overline{0}$ est le neutre : $\overline{0} + \overline{a} = \overline{a} + \overline{0} = \overline{a}$;

(ii) existence d'un inverse : $\overline{a} + \overline{-a} = \overline{-a} + \overline{a} = \overline{0}$;

(iii) associativité : $(\overline{a} + \overline{b}) + \overline{c} = \overline{a} + (\overline{b} + \overline{c})$;

De plus, l'addition respecte la

(iv) commutativité : $\overline{a} + \overline{b} = \overline{b} + \overline{a}$.

Voici les tables d'addition pour $\mathbb{Z}_2$, $\mathbb{Z}_3$ et $\mathbb{Z}_6$:

$+$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$

(3.1)

$\mathbb{Z}_n$ ne possède pas d'ordre compatible avec $+$ — Contrairement à $\mathbb{Z}$ qui a été utilisé pour donner à $\mathbb{Z}_n$ son addition, l'ensemble $\mathbb{Z}_n$ ne possède d'ordre compatible avec l'addition, c'est-à-dire un ordre $\leq$ tel que, si $\overline{a} \leq \overline{b}$, alors $\overline{a} + \overline{d} \leq \overline{b} + \overline{d}$ pour tout $\overline{d} \in \mathbb{Z}_n$. Étudions d'abord l'ordre le plus simple qui pourrait être proposé : $\overline{0} < \overline{1} < \cdots < \overline{n-1}$. Entre autre, cet ordre donne $\overline{n-2} < \overline{n-1}$. Et si 1 est additionné à chacun des membres de l'inégalité, le résultat $\overline{1} + \overline{n-2} < \overline{1} + \overline{n-1}$ devient $\overline{n-1} < \overline{0}$ qui contredit l'ordre proposé. Mais un autre ordre pourrait-il fonctionner ?

Supposons un autre ordre $<$ qui ordonne les n classes $\overline{0}, \overline{1}, \ldots, \overline{n-1}$. Alors il est possible d'écrire $a_0 < a_1 < \cdots < a_{n-1}$ où chacun des a_i est une de ces n classes. Notons que, dans un ordre (total), il existe une et une seule façon d'ordonner les n éléments pour que toutes ces inégalités soient simultanément vraies. En additionnant $\overline{1}$ à chacun des membres de cette collection d'inégalités, la collection d'inégalités $a_0 + \overline{1} < a_1 + \overline{1} < \cdots < a_{n-1} + \overline{1}$ est obtenue et une de ces nouvelles inégalités est sûrement en contradiction avec les inégalités originales. En effet, soit i l'indice désignant l'addition de a_0 avec $\overline{1}$: $a_i = a_0 + \overline{1}$. Ce a_i est distinct de a_0, car seul $\overline{0}$ est un neutre pour $+$. Mais $a_0 < a_i$ selon l'ordre proposé, alors que dans les nouvelles inégalités, a_i devrait être plus petit que tous les autres éléments. Donc il n'existe pas d'ordre sur $\mathbb{Z}_n$ compatible avec l'addition.

La multiplication dans $\mathbb{Z}_n$ **—** La construction de l'opération multiplication dans $\mathbb{Z}_n$ suit la méthode utilisée pour l'addition.

$$\overline{a} \times \overline{b} \stackrel{\text{déf}}{=} \overline{a \times b}.$$

(La multiplication sera notée indifféremment par $\cdot$ et $\times$.) À nouveau, il faut vérifier que cette définition est *bien définie*, c'est-à-dire que, si $c \in \overline{a}$ et $d \in \overline{b}$, alors

$$\overline{a \times b} = \overline{c \times d}. \qquad (\times_{\mathbb{Z}_n})$$

Mais $c \in \overline{a}$ et $d \in \overline{b}$ signifient respectivement $a \equiv c \bmod n$ et $b \equiv d \bmod n$ et la proposition 9 donne immédiatement

$$a \times b \equiv c \times d \bmod n$$

ce qui veut dire précisément que $a \times b$ et $c \times d$ sont dans la même classe d'équivalence qui est une autre façon de lire l'équation $(\times_{\mathbb{Z}_n})$.

Comme précédemment la proposition suivante découle aisément des propriétés correspondantes sur $\mathbb{Z}$.

Proposition 12. $(\mathbb{Z}_n, +, \times)$ *satisfait les propriétés suivantes pour tout* $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_n$

(i) $\overline{1}$ *est le neutre de* $\times$ *:* $\overline{1} \times \overline{a} = \overline{a} \times \overline{1} = \overline{a}$*;*

(ii) associativité : $(\overline{a} \times \overline{b}) \times \overline{c} = \overline{a} \times (\overline{b} \times \overline{c})$*;*

(iii) commutativité : $\overline{a} \times \overline{b} = \overline{b} \times \overline{a}$*;*

(iv) distributivité de $\times$ *sur* $+$ *:* $(\overline{a} + \overline{b}) \times c = (\overline{a} \times \overline{c}) + (\overline{b} \times c)$.

Voici les tables de multiplication de $\mathbb{Z}_2$, $\mathbb{Z}_3$ et $\mathbb{Z}_6$.

$\times$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

(3.2)

La proposition ci-dessus a omis une propriété : $(\mathbb{Z}_n, \times)$ n'est pas en général un groupe. En effet, tout élément n'a pas nécessairement un inverse multiplicatif. Cette omission n'est pas un oubli. La table de multiplication de $\mathbb{Z}_6$ le démontre facilement. Si $\overline{2}$ possédait un inverse multiplicatif dans $\mathbb{Z}_6$, il y aurait un élément $\overline{a} \in \mathbb{Z}_6$ tel que $\overline{2} \cdot \overline{a} = \overline{1}$. Mais il ne se trouve aucun nombre $\overline{1}$ sur la ligne donnant la multiplication par $\overline{2}$. Donc il n'existe pas d'inverse multiplicatif de $\overline{2}$ dans $\mathbb{Z}_6$! Cependant un inverse existe pour tout élément non nul de $\mathbb{Z}_2$ et $\mathbb{Z}_3$. Par exemple, dans $\mathbb{Z}_3$, le nombre $\overline{2}$ est son propre inverse multiplicatif puisque $\overline{2} \cdot \overline{2} = \overline{4} = \overline{1}$.

Pour quel n tout élément $\overline{a}$ non nul, c'est-à-dire différent de $\overline{0}$, possède-t-il un inverse multiplicatif dans $\mathbb{Z}_n$? En d'autres mots, pour quel n la paire $(\mathbb{Z}_n \setminus \{\overline{0}\}, \times)$ forme-t-elle un groupe ? La réponse n'est pas trop difficile à obtenir. Soit $\overline{a} \in \mathbb{Z}_n$ un élément non nul. Cet élément $\overline{a}$ aura un inverse multiplicatif s'il existe $\overline{b} \in \mathbb{Z}_n$ tel que $\overline{a} \cdot \overline{b} = \overline{1}$, c'est-à-dire tel que

$a \cdot b \equiv 1 \bmod n$. Cette équivalence signifie qu'il existe un $k \in \mathbb{Z}$ tel que $a \cdot b = 1 + n \cdot k$ ou encore il existe une solution à l'équation diophantienne $a \cdot b - n \cdot k = 1$. Ainsi

$$\begin{aligned}(\mathbb{Z}_n \setminus \{0\}, \times) \text{ est un groupe} &\iff \text{pour tout } \overline{a} \in \mathbb{Z}_n \setminus \{0\}, \text{ il existe } \overline{b} \in \mathbb{Z}_n \text{ tel que } \overline{a} \cdot \overline{b} = \overline{1} \\ &\iff \text{pour tout } \overline{a} \in \mathbb{Z}_n \setminus \{0\}, \text{ l'équation } a \cdot b - n \cdot k = 1 \text{ possède une solution pour } b \text{ et } k \\ &\overset{\text{Bézout}}{\iff} \text{pour tout } \overline{a} \in \mathbb{Z}_n \setminus \{0\}, \ a \text{ et } n \text{ sont relativement premiers} \\ &\iff n \text{ est un nombre premier.}\end{aligned}$$

Le théorème de Bézout (théorème 5 du chapitre 2) a été utilisé à la troisième équivalence. Ainsi, si p est un nombre premier, $(\mathbb{Z}, +, \times)$ possède des inverses additifs pour tous ses éléments et des inverses multiplicatifs pour tous ses éléments sauf $\overline{0}$.

Les propriétés de $(\mathbb{Z}_p, +, \times)$, avec p premier, reviennent souvent et les mathématiciens ont réalisé qu'elles suffisent à beaucoup d'algorithmes mathématiques. Ils ont donc donné un nom à toute structure algébrique qui possèdent ces propriétés.

Définition 9. *Soit $\mathbb{F}$ un ensemble possédant deux éléments distincts nommés 0 et 1 et muni de deux opérations $+$ et $\times$. Le triplet $(\mathbb{F}, +, \times)$ est un* corps *si*

(i) $(\mathbb{F}, +)$ *est un groupe abélien avec 0 comme élément neutre ;*

(ii) $(\mathbb{F} \setminus \{0\}, \times)$ *est un groupe abélien avec 1 comme élément neutre ;*

(iii) l'opération $\times$ est distributive sur l'opération $+$: $(a + b) \times c = (a \times c) + (b \times c)$, pour tout $a, b, c \in \mathbb{F}$.

Le mot anglais pour la structure de corps est field.

Avec cette définition, il est possible de conclure :

Proposition 13. *Soit $+$ et $\times$ les opérations sur $\mathbb{Z}_n$ définies plus haut. Le triplet $(\mathbb{Z}_n, +, \times)$ est un corps si et seulement si n est un nombre premier.*

Le théorème de Bézout permet non seulement de conclure que $(\mathbb{Z}_p, +, \times)$ est un corps si p est un nombre premier. Il permet aussi de trouver l'inverse des éléments de $\mathbb{Z}_p \setminus \{0\}$. Soit $\overline{a} \in \mathbb{Z}_p$ un élément non nul. Puisque p est premier et $\overline{a}$ est non nul, le $\operatorname{pgcd}(a, p)$ est égal à 1. Alors il existe k et $\ell \in \mathbb{Z}$ tels que $k \cdot a + \ell \cdot p = 1$. Alors, modulo p, cette équation dit $k \cdot a \equiv 1 \bmod p$ et $\overline{k}$ est donc l'inverse de $\overline{a}$. L'exercice 11 mettra cette observation à profit.

EXERCICES

10. Vrai ou faux.

(a) Dans $\mathbb{Z}_5$, $\overline{12}$ est l'inverse additif de $\overline{13}$.

(b) Puisque $3 + 2 \equiv 0 \bmod 5$ et $3 - 3 \equiv 0 \bmod 5$, $\overline{3}$ possède deux inverses $\overline{2}$ et $\overline{-3}$ et l'inverse additif de $\overline{3}$ dans $\mathbb{Z}_5$ n'est pas unique.

(c) Dans $\mathbb{Z}_5$, $\overline{2}$ est l'inverse multiplicatif de $\overline{3}$.

(d) $\mathbb{N}$ est un corps.

(e) $\mathbb{Z}$ est un corps.

(f) $\mathbb{Q}$ est un corps.

11. (a) Montrer que si a et n ne sont pas relativement premiers, alors il existe un b tel que $1 \leq b < n$ tel que $a \cdot b \equiv 0 \bmod n$. En conclure que, si $\text{pgcd}(a, n) \neq 1$, alors a ne possède pas d'inverse multiplicatif dans $\mathbb{Z}_n$.

(b) Dire, pour les a et n ci-dessous, si $\overline{a}$ possède un inverse multiplicatif dans $\mathbb{Z}_n$ et, si oui, l'obtenir.

(i) $a = 3, n = 7$;
(ii) $a = 3, n = 10$;
(iii) $a = 4, n = 15$;
(iv) $a = 39, n = 77$;
(v) $a = 123\,456\,789, n = 987\,654\,321$;
(vi) $a = 13\,717\,421, n = 109\,739\,369$.

12. (a) Quelles sont les deux dernières décimales de 9^{100} ? Suggestion : commencer par calculer ces décimales pour 9^{10}.

(b) Et que dire des deux dernières décimales de $9^{10000000}$?

13. Prouver le corollaire 10.

14. *Critère de divisibilité par 9*. Prouver chacune des affirmations suivantes en justifiant par la propriété appropriée.

(a) $10 \equiv 1 \bmod 9$.

(b) $10^k \equiv 1 \bmod 9$ pour tout $k \geq 0$.

(c) $a \cdot 10^k \equiv a \bmod 9$ pour tout $k \geq 0$ et $a \in \mathbb{Z}$.

(d) $a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0 \equiv a_k + a_{k-1} + \cdots + a_2 + a_1 + a_0 \bmod 9$.

(e) Soit $(a_k a_{k_1} \ldots a_2 a_1 a_0)_{10}$ la représentation en base 10 d'un nombre entier. Il est divisible par 9 si et seulement si la somme de ses chiffres $(a_k + a_{k-1} + \cdots + a_2 + a_1 + a_0)$ est un multiple de 9.

15. (a) Montrer que l'énoncé suivant est faux en trouvant un contre-exemple avec un $a \neq 0$: si $ab \equiv ac \bmod n$, alors $b \equiv c \bmod n$.

(b) Si $\text{pgcd}(a, n) = 1$, alors $ab \equiv ac \bmod n$ implique $b \equiv c \bmod n$.

16. Tous les nombres et variables dans les équations de (a) et (b) sont des éléments de $\mathbb{Z}_5$.

(a) Résoudre l'équation $\overline{4} \cdot x = \overline{2}$.

(b) Résoudre le système d'équations à deux variables

$$\overline{1} \cdot x + \overline{2} \cdot y = \overline{3}$$
$$\overline{4} \cdot x + \overline{1} \cdot y = \overline{0}.$$

(c) Refaire les exercices (a) et (b) si les nombres et variables sont dans $\mathbb{Z}_3$.

(d) Est-ce que le système de (b) possède une solution dans $\mathbb{Z}_7$?

17. Soit $\mathbb{Z}_n^\star$ le sous-ensemble de $\mathbb{Z}_n$ des éléments qui possèdent un inverse multiplicatif dans $(\mathbb{Z}_n, \times)$.

(a) Donner les éléments de $\mathbb{Z}_4^\star$, $\mathbb{Z}_6^\star$ et $\mathbb{Z}_8^\star$.

(b) Montrer que, si $\overline{a}$ et $\overline{b}$ sont dans $\mathbb{Z}_n^\star$, leur produit l'est aussi.

(c) Montrer que $\mathbb{Z}_n^\star$ est un groupe pour l'opération $\times$ de $\mathbb{Z}_n$.

18. Soit d un diviseur de a, b et n. Alors $a \equiv b \bmod n$ si et seulement si $\frac{a}{d} \equiv \frac{b}{d} \bmod \frac{n}{d}$.

19. (a) Soit la relation définie sur l'ensemble $\mathbb{Q}$ par $\frac{p}{q} \sim \frac{r}{s}$ si il existe un entier n tel que $\frac{p}{q} = \frac{r}{s} + n$. Montrer que $\sim$ est une relation d'équivalence. On notera par $\widehat{\frac{p}{q}}$ la classe d'équivalence de $\frac{p}{q}$ et par $\mathbb{Q}/\mathbb{Z}$ l'ensemble de ces classes d'équivalence. Ainsi $\widehat{\frac{3}{4}} = \{\ldots, -\frac{5}{4}, -\frac{1}{4}, \frac{3}{4}, \frac{7}{4}, \frac{11}{4}, \ldots\}$.

(b) On tente de définir deux opérations $\widehat{+}$ et $\widehat{\cdot}$ sur l'ensemble $\mathbb{Q}/\mathbb{Z}$:

$$\widehat{\frac{p}{q}} \,\widehat{+}\, \widehat{\frac{r}{s}} = \widehat{\left(\frac{p}{q} + \frac{r}{s}\right)} \qquad \text{et} \qquad \widehat{\frac{p}{q}} \,\widehat{\cdot}\, \widehat{\frac{r}{s}} = \widehat{\left(\frac{p}{q} \cdot \frac{r}{s}\right)}.$$

Sont-elles « bien définies » ?

3.4 Les nombres réels

Certaines opérations algébriques ne sont pas possibles au sein des nombres rationnels. Par exemple l'équation $x^2 = n$ où n est un entier positif n'a pas de solutions dans $\mathbb{Q}$ pour tout n et donc l'extraction de la racine carrée n'est pas toujours possible.

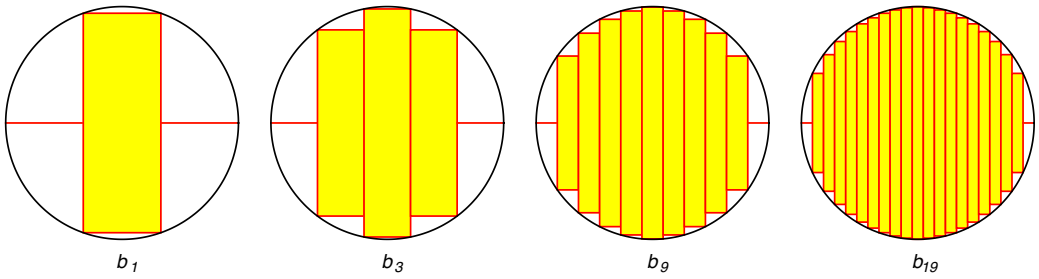
Proposition 14. *Il n'existe pas de* $x \in \mathbb{Q}$ *tel que* $x^2 = 2$.

Preuve (par contradiction). Supposons qu'un tel x existe et que $\frac{n}{d}$ soit sa forme réduite, c'est-à-dire telle que $\operatorname{pgcd}(n, d) = 1$. Alors $\frac{n^2}{d^2} = 2$ ou encore $n^2 = 2d^2$. Puisque n^2 est un carré pair, le nombre n doit être lui-même pair, c'est-à-dire qu'il existe m tel que $n = 2m$. Mais alors $n^2 = 4m^2 = 2d^2$ ou encore $2m^2 = d^2$. Donc d est lui-même pair et les nombres n et d ont un facteur 2 en commun : ceci est une contradiction puisque leur pgcd devrait être 1. □

La présente section est consacrée à la construction de l'ensemble des nombres réels $\mathbb{R}$. Après l'exemple ci-dessus, il pourrait être tentant de définir les nombres réels comme l'ensemble des solutions de toutes les équations algébriques de la forme

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x^1 + a_0 = 0$$

pour tout n et tout ensemble de nombres rationnels $a_n, a_{n-1}, \ldots, a_1, a_0 \in \mathbb{Q}$. Les solutions de ces équations sont appelées *nombres algébriques*. Clairement les nombres rationnels sont des nombres algébriques puisque, si $q \in \mathbb{Q}$, l'équation $x - q = 0$ est de la forme ci-dessus (pour $n = 1$) et a comme solution le nombre rationnel q. Mais l'ensemble de nombres qui constitue la base de l'analyse (et du calcul différentiel et intégral) est plus riche. Cet ensemble doit permettre de prendre certaines limites. Par exemple, il est possible de montrer que l'aire d'un cercle de rayon 1 (et donc égale à π) n'est pas un nombre algébrique. Pourtant cette aire peut être approximée par une suite de nombres croissants *qui converge vers* π. Les figures ci-contre indiquent intuitivement cette convergence. Si l'ensemble $\mathbb{R}$ est pour fournir la base des



concepts de limite et de convergence, les nombres réels devront inclure plus que les nombres algébriques. En fait, contrairement aux extensions des ensembles $\mathbb{N} \to \mathbb{Z}$ et $\mathbb{Z} \to \mathbb{Q}$ qui étaient de nature algébrique (la première assurant l'existence d'inverses additifs, la seconde d'inverses multiplicatifs), l'extension $\mathbb{Q} \to \mathbb{R}$ n'est pas algébrique. Avant de décrire la nature de cette extension, voici un extrait d'un article étudiant l'introduction des nombres réels à l'école secondaire (traduit librement de l'anglais) :

> Le cas de l'extension des nombres rationnels aux réels est particulièrement frappante. Contrairement aux extensions précédentes, le saut ici n'est pas algébrique, puisqu'il requiert formellement les propriétés théoriques telles la convergence et la complétude. Ceci s'est révélé un obstacle crucial, qui débuta avec le débat sur les mesures incommensurables dans les mathématiques grecques. [...] D'une part, la définition formelle des nombres réels n'est probablement pas à la portée des niveaux primaires et secondaires. D'autre part, l'ensemble des nombres réels ne peut pas être construits à partir d'exigences empiriques ou algébriques. Malgré cela, les réels sont un sujet indispensable de l'éducation mathématique pour les raisons suivantes : (1) leur importance inhérente au coeur des connaissances mathématiques contemporaines ; et (2) leurs relations indissociables avec de nombreux sujets, élémentaires et d'égale importance (le périmètre d'un cercle, les racines carrées, le

> théorème de Pythagore) et plus avancés comme les limites et la continuité. Ceci soulève la question, tant pour l'enseignement que pour les manuels et les curriculums : *comment l'équilibre peut-il être atteint entre la rigueur et l'intuition dans le cas particulièrement délicat de la construction des nombres réels en classe ?* [6]

La section 3.2 a construit l'ensemble $\mathbb{Q}$ comme un ensemble de classes d'équivalence $\overline{(n, d)}$. Mais comme l'exercice 21 le montre, il est possible de choisir un représentant particulier de chaque classe d'équivalence (le représentant (n_0, d_0) tel que $\text{pgcd}(n_0, d_0) = 1$) et de noter cette classe sous la forme $\frac{n_0}{d_0}$ qui nous est familière. C'est ce que nous ferons par la suite.

La plus petite borne supérieure — L'extension $\mathbb{Q} \to \mathbb{R}$ semble vouloir reproduire le principe du bon ordre. Rappelons que ce principe affirme que tout ensemble non vide de $\mathbb{N}$ possède un plus petit élément. Ceci n'est certainement pas vrai pour les sous-ensembles non vides de $\mathbb{Z}$; par exemple le sous-ensemble $\{\ldots, -5, -3, -1, 1, 3, 5, \ldots\}$ des nombres impairs n'a pas de plus petit élément. Il est facile de contrer cette difficulté.

Définition 10. *Soit $(\mathbb{E}, <)$ un ensemble ordonné de nombres et F un sous-ensemble de $\mathbb{E}$. L'ensemble F est dit borné supérieurement s'il existe $e \in \mathbb{E}$ tel que $f \leq e$ pour tout $f \in F$. Le nombre e est alors appelé une borne supérieure de F.*

Avec cette définition, l'ensemble des entiers relatifs $\mathbb{Z}$ possède la propriété : tout sous-ensemble $F \subset \mathbb{Z}$ non vide et borné supérieurement possède un plus grand élément. (On pourrait également définir les ensembles bornés inférieurement ; alors les ensembles $G \subset \mathbb{Z}$ non vides et bornés inférieurement auraient toujours un plus petit élément.)

Même si $\mathbb{Z}$ possède cette propriété, l'ensemble des rationnels $\mathbb{Q}$ ne la possède plus. L'ensemble

$$F = \{x \in \mathbb{Q} \mid x^2 < 2\} \subset \mathbb{Q}$$

ne possède pas de plus grand élément. Pourtant il est non vide (0 est dans F) et est borné supérieurement, par exemple par 2. La définition suivante raffine le concept d'« avoir un plus grand élément ».

Définition 11. *Soit $(\mathbb{E}, <)$ un ensemble ordonné de nombres et F un de ses sous-ensembles. S'il existe un $e \in \mathbb{E}$ tel que*

(i) e est une borne supérieure pour F et,

(ii) si $d < e$, alors d n'est pas une borne supérieure de F,

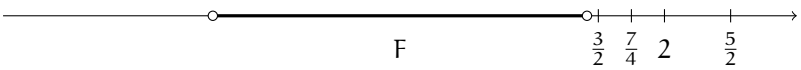
alors e est appelé la plus petite borne supérieure [7] *de F ou encore le* supremum *de F. On écrit $e = \sup F$.*

Définition 12. *Un ensemble ordonné $(\mathbb{E}, <)$ possède la propriété de la plus petite borne supérieure si tout sous-ensemble $F \subset \mathbb{E}$ non vide et borné supérieurement possède un supremum.*

6. AS González-Martín, V Giraldo, AM Souto, *The introduction of real numbers in secondary education : an institutional analysis of textbooks*, Res. Math. Educ. **15**, 230–248 (2013).

7. Les mots « plus petite borne supérieure » utilisés au Québec pour le supremum sont une traduction de l'anglais « least upper bound ». Pour ce concept de supremum, la France utilise simplement « borne supérieure ».

L'ensemble F décrit ci-dessus montre clairement que l'ensemble $\mathbb{Q}$ n'a pas la propriété de la plus petite borne supérieure. Par exemple la figure ci-dessous dépeint par un trait épais l'ensemble F sur une droite rationnelle. Les extrémités du segment n'appartiennent pas à $\mathbb{Q}$. (La proposition ci-dessus a montré que le nombre réel $\sqrt{2} \sim 1.41421\ldots$ n'est pas un nombre rationnel.) L'ensemble F possède une infinité de bornes supérieures rationnelles dont certaines sont marquées ($\frac{5}{2}, 2, \frac{7}{4}$ et $\frac{3}{2}$), mais pas de plus petite borne supérieure. (Nous le montrerons plus bas.)



Définition de l'ensemble des nombres réels $\mathbb{R}$ **—** L'ensemble des nombres réels $\mathbb{R}$ sera construit pour que

(i) $\mathbb{Q}$ apparaisse naturellement comme un sous-ensemble de $\mathbb{R}$ et

(ii) $\mathbb{R}$ possède la propriété de la plus petite borne supérieure.

La définition de $\mathbb{R}$ donnée ici est celle des *coupures de Dedekind*. La présentation suit celle de Walter Rudin. [8]

Définition 13. *Une coupure (de Dedekind) est tout sous-ensemble* α *de* $\mathbb{Q}$ *satisfaisant*

(i) α *est non vide et* $\alpha \neq \mathbb{Q}$*;*

(ii) si $p \in \alpha$, $q \in \mathbb{Q}$ *et* $q < p$, *alors* $q \in \alpha$*;*

(iii) si $p \in \alpha$, *alors il existe* $r \in \alpha$ *tel que* $p < r$.

L'ensemble des nombres réels $\mathbb{R}$ *est l'ensemble des coupures de Dedekind.*

Pour la suite de cette section, les lettres latines $p, q, r, \ldots$ dénoteront des éléments de $\mathbb{Q}$, alors que les lettres grecques $\alpha, \beta, \gamma, \ldots$ dénoteront des éléments de $\mathbb{R}$.

Quelques observations sur la définition. La condition *(iii)* implique qu'une coupure n'a pas de plus grand élément. Et puisque *(i)* affirme qu'une coupure $\alpha \subset \mathbb{Q}$ est toujours un sous-ensemble distinct de $\mathbb{Q}$, c'est qu'il existe un nombre rationnel q qui n'appartient pas à α et alors *(ii)* dit que ce q est plus grand que tout $p \in \alpha$. (Il ne peut être égal à un $p \in \alpha$, car q n'est pas dans α.) Donc une coupure α est un sous-ensemble de $\mathbb{Q}$ non vide et borné supérieurement.

La définition de coupure est difficile. Il vaut la peine d'en donner des exemples. Le premier exemple consiste à montrer que $\mathbb{Q}$ est naturellement inclus dans l'ensemble $\mathbb{R}$ ou, plus précisément, pour chaque élément de $\mathbb{Q}$ correspond une élément de $\mathbb{R}$ (et deux éléments distincts de $\mathbb{Q}$ correspondent à des éléments distincts de $\mathbb{R}$). Soit la correspondance

$$q \in \mathbb{Q} \quad \longrightarrow \quad \alpha_q = \{p \in \mathbb{Q} \mid p < q\} \in \mathbb{R}.$$

Elle associe à chaque élément de $\mathbb{Q}$ un sous-ensemble de $\mathbb{Q}$. Ce sous-ensemble est une coupure et donc un élément de $\mathbb{R}$. C'est ce que nous allons montrer maintenant. Tout d'abord, ce sous-ensemble α_q contient l'élément (rationnel) $q - 1 \in \mathbb{Q}$ qui est plus petit que q. De plus $q \notin \alpha_q$ et $\alpha_q \neq \mathbb{Q}$ (et donc *(i)* est vérifiée !). Soit $p \in \alpha_q$ (ceci veut dire $p < q$) et soit $r \in \mathbb{Q}$ tel que

8. W Rudin, *Principles of mathematical analysis*, 3e édition, McGraw-Hill (1976).

$r < p$; alors $r < p < q$ et donc $r < q$ et, par définition de α_q, $r \in \alpha_q$ (et *(ii)* vérifiée). Enfin si $p \in \alpha_q$, alors $p < q$ et

$$r = p + \left(\frac{q-p}{2}\right) < q$$

où le terme entre parenthèse est la moitié de la distance entre p et q. Donc r est entre p et q, c'est-à-dire $p < r < q$ et $r \in \alpha_q$ (et *(iii)* ✓). La correspondance $q \in \mathbb{Q} \to \alpha_q \in \mathbb{R}$ est donc une fonction qui envoie un élément de $\mathbb{Q}$ dans un élément de $\mathbb{R}$.

Si p et q sont distincts avec $p < q$, alors les deux coupures α_p et α_q sont distinctes. En effet l'élément $r = p + (q-p)/2$ est dans α_q, mais pas dans α_p. En fait $\alpha_p \subset \alpha_q$ puisque tout élément $r \in \alpha_p$ est plus petit que p et donc plus petit que q. Ainsi la fonction $q \to \alpha_q$ est injective. C'est donc une correspondance bijective entre $\mathbb{Q}$ et l'ensemble des α_q définis pour $q \in \mathbb{Q}$.

Une dernière propriété des α_q doit être soulignée. Chacun des α_q possède une plus petite borne supérieure dans $\mathbb{Q}$. La plus petite borne supérieure de α_q est simplement q :

$$\sup \alpha_q = q.$$

Pour s'en assurer, il faut montrer que q est une borne supérieure de α_q et qu'il n'y en a pas de plus petite. Par définition de l'ensemble α_q, tout élément $p \in \alpha_q$ est plus petit que q et donc q est une borne supérieure pour α_q. Supposons que r soit une autre borne supérieure de α_q et qu'elle soit plus petite que q : $r < q$. Alors le nombre $r + \frac{q-r}{2}$ est entre r et q :

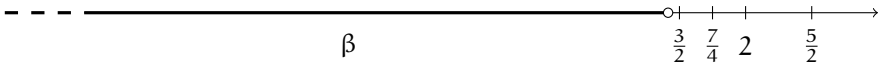
$$r < r + \frac{q-r}{2} < q$$

et donc il existe un nombre dans α_q (le nombre $r + \frac{q-r}{2}$) qui est plus grand que la borne supérieure r : ceci est une contradiction. Ainsi q est la plus petite borne supérieure de α_q et toutes les coupures de type α_q pour $q \in \mathbb{Q}$ possèdent un supremum qui est lui-même un élément de $\mathbb{Q}$.

L'ensemble F n'est pas une coupure, car la condition *(ii)* n'est pas satisfaite pour cet ensemble. En effet le nombre 0 est dans F, le nombre -2 est dans $\mathbb{Q}$ et est plus petit que 0, mais -2 n'est pas dans F puique $(-2)^2 = 4 \not< 2$. Il est facile d'étendre F pour en faire une coupure. Soit

$$\beta = \{x \in \mathbb{Q} \mid x^2 < 2\} \cup \{x \in \mathbb{Q} \mid x < 0\}.$$

La représentation graphique de β est alors



Ce β est une coupure. Il vaut la peine de le montrer, car ce n'est pas un exercice facile (à cause de la propriété *(iii)*). Tout d'abord, β est non vide car 0 appartient à β et $\beta \neq \mathbb{Q}$ puisque $2 \notin \beta$ (*(i)* ✓). Soit $p \in \beta$ et $q \in \mathbb{Q}$ tel que $q < p$. Si q est négatif, alors il est automatiquement dans β. Si cependant q n'est pas négatif, il est un rationnel positif ; alors $q < p$ implique $q^2 < p^2 < 2$ et donc $q \in \beta$ (*(ii)* ✓). La vérification de *(iii)* est la plus délicate. Pour tout $p \in \beta$, il faut trouver un

rationnel plus grand qui demeure dans β et donc un rationnel r plus grand que p satisfaisant $r^2 < 2$. En voici un :

$$r = p + \left(\frac{2 - p^2}{p + 2}\right).$$

Pour vérifier qu'il est plus grand que p, notons que, puisque $p^2 < 2$, le numérateur du terme entre parenthèses est positif et r est donc plus grand que p. Il reste à montrer que $r^2 < 2$. Réécrivons l'expression de r :

$$r = p + \frac{2 - p^2}{p + 2} = \frac{p^2 + 2p + 2 - p^2}{p + 2} = \frac{2p + 2}{p + 2}.$$

Alors r sera dans β si $2 - r^2$ est positif :

$$2 - r^2 = 2\frac{(p+2)^2}{(p+2)^2} - \frac{(2p+2)^2}{(p+2)^2} = \frac{(2p^2 + 8p + 8) - (4p^2 + 8p + 4)}{(p+2)^2} = \frac{-2p^2 + 4}{(p+2)^2} = \frac{2(2 - p^2)}{(p+2)^2} > 0$$

et r est bien dans β (et, enfin, *(iii)* ✓). Conclusion : β est une coupure.

Cet exemple est important car, contrairement aux α_q avec $q \in \mathbb{Q}$, l'ensemble β ne possède pas de plus petite borne supérieure dans $\mathbb{Q}$. Une telle « plus petite borne supérieure » devrait être un rationnel dont le carré est 2 et la proposition 14 montre que ce rationnel n'existe pas.

Cet exemple fournit également un lien avec l'intuition issue de notre premier contact avec les nombres réels. L'ensemble β est, dans l'ensemble $\mathbb{R}$ que nous venons de définir, le nombre que nous nommons $\sqrt{2}$. Ce nombre réel peut être défini comme étant la longueur de l'hypothénuse d'un triangle rectangle dont les deux côtés adjacents à l'angle droit sont de longueur 1. Il peut aussi être défini comme

$$\sqrt{2} = 1.414\,213\,562\,373\,095\,048\,801\,688\,724\,209\,698\,078\,569\,671\,875\,376\ldots$$

Le sous-ensemble β contient toutes les approximations 1, 1.4, 1.414, 1.414 2, ..., 1.414 213 562, ..., 1.414 213 562 373 095 048, etc. Toutes ces approximations ont été obtenues en arrondissant vers le bas et donc en préservant le fait que ces approximations satisfont $x^2 < 2$. Et ces approximations sont telles que toute borne supérieure de β dans $\mathbb{Q}$ devra être plus grande que le nombre $\sqrt{2}$ que nous connaissons.

L'ordre $\leq$ sur $\mathbb{R}$ — Soient p et q deux nombres rationnels distincts. Alors $p < q$ ou $q < p$ puisque $\mathbb{Q}$ est totalement ordonné. Si $p < q$, alors $\alpha_p \subset \alpha_q$. En effet, si r est dans α_p, c'est que $r < p$. Si de plus $p < q$, alors $r < p < q$ et $r \in \alpha_q$ aussi. Ainsi $r \in \alpha_p$ implique $r \in \alpha_q$; une autre façon d'écrire cette implication est $\alpha_p \subset \alpha_q$. Cette observation sur les coupures obtenues à partir des nombres rationnels indique la voie pour l'ordre sur $\mathbb{R}$.

Définition 14. *La coupure $\alpha \in \mathbb{R}$ est dite plus petite ou égale à la coupure $\beta \in \mathbb{R}$ si $\alpha \subseteq \beta$ vues comme sous-ensembles de $\mathbb{Q}$:*

$$\alpha <_{\mathbb{R}} \beta \quad \longleftrightarrow \quad \alpha \subseteq \beta.$$

On note $\alpha <_{\mathbb{R}} \beta$ si $\alpha \leq_{\mathbb{R}} \beta$ mais $\alpha \neq \beta$.

Nous avons écrit $<_{\mathbb{R}}$ pour souligner que nous définissions ici une relation d'ordre sur le nouvel ensemble $\mathbb{R}$. Mais nous omettrons par la suite l'indice $\mathbb{R}$.

Proposition 15. *La paire* $(\mathbb{R}, \leq)$ *est un ensemble totalement ordonné.*

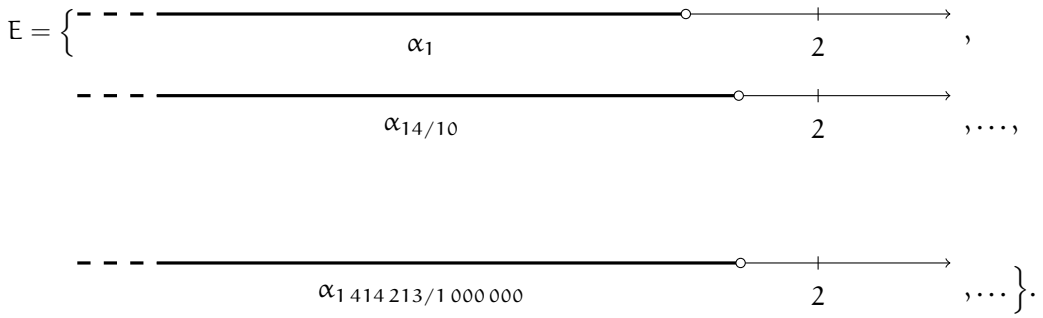
Preuve. Les quatre propriétés d'ordre total doivent être prouvées (voir la définition à la section 1.4). Les quatre preuves découlent des propriétés des ensembles. Si $\alpha \leq \beta$ et $\beta \leq \alpha$, c'est que, par définition, $\alpha \subseteq \beta$ et $\beta \subseteq \alpha$. Puisque le sous-ensemble α est inclus dans le sous-ensemble β et vice versa, les deux sous-ensembles coïncident : $\alpha = \beta$ (antisymétrie ✓).

Soient α et β deux coupures. Si elles sont égales, alors l'énoncé de la totalité est vraie puisque $\alpha \leq \beta$ *et* $\beta \leq \alpha$ sont les deux vraies. Supposons que les deux coupures soient distinctes. Alors il existe un élément $q \in \mathbb{Q}$ qui appartient à un des deux ensembles sans appartenir à l'autre. Supposons, sans perte de généralité, que $q \in \beta$ mais que $q \notin \alpha$. L'observation faite immédiatement après la définition de coupure montre que q est alors plus grand que tout élément de α. Ainsi, si p est dans α, alors $p < q$ et p est dans β ; à nouveau, ceci peut s'énoncer comme $\alpha \subset \beta$ et donc l'énoncé $\alpha \leq \beta$ est vrai (totalité ✓).

La transitivité et la réflexivité sont laissées en exercice. □

$\mathbb{R}$ ***possède la propriété de la plus petite borne supérieure*** — L'ensemble $\mathbb{R}$ des coupures de Dedekind muni de l'ordre $\leq$ possède la propriété de la plus petite borne supérieure. Cette propriété est fort abstraite pour l'ensemble $\mathbb{R}$, puisque les éléments de $\mathbb{R}$ sont des sous-ensembles de $\mathbb{Q}$. Elle dit : si E est un sous-ensemble de coupures de $\mathbb{R}$ qui est non vide et borné supérieurement, alors il existe une coupure $\sigma \in \mathbb{R}$ qui est la plus petite borne supérieure de E. Nous allons construire « explicitement » la coupure qui est la plus petite borne supérieure.

Voici un exemple d'un sous-ensemble $E \subset \mathbb{R}$.



Cet ensemble de coupures a été construit à partir de coupures rationnelles (c'est-à-dire obtenues par la correspondance $q \in \mathbb{Q} \leftrightarrow \alpha_q \in \mathbb{R}$) telles que leur union redonne l'ensemble

$$\{x \in \mathbb{Q} \mid x^2 < 2\} \cup \{x \in \mathbb{Q} \mid x < 0\}$$

qui a été dessiné plus tôt. Évidemment il est bien difficile de voir la différence entre $\alpha_{14/10}$ et $\alpha_{1\,414\,213/1\,000\,000}$ sur cette figure, mais ces deux coupures ne sont pas les mêmes ! L'ensemble

E est non vide (en fait, il contient un nombre infini de coupures) et il est borné supérieurement, par exemple par la coupure α_2. Il peut être utile de garder cet exemple en tête en lisant la preuve qui suit (et qui est donnée pour un E général).

Soit E l'ensemble de coupures non vide et borné supérieurement. Cet énoncé dit deux choses :

(1) il contient au moins une coupure $\alpha_0 \subset \mathbb{Q}$ (donc un sous-ensemble non vide) et
(2) il existe $\beta \in \mathbb{R}$ une coupure telle que tout élément α de E est inférieure ou égale à β : $\alpha \leq \beta$ si $\alpha \in E$.

Définissons alors σ comme l'union de tous les éléments de E (qui sont des sous-ensembles de $\mathbb{Q}$). Ainsi un nombre rationnel p est dans σ si et seulement il existe un $\alpha \in E$ qui contient ce p. Nous allons montrer que σ est lui-même une coupure et que c'est la plus petite borne supérieure de E.

Montrons d'abord que σ est une coupure. Puisque α_0 est une coupure contenue dans E et que les coupures sont non vides, alors σ est non vide. De plus, un élément p quelconque d'une coupure $\alpha \in E$ a la propriété que p appartient à la borne supérieure β puisque $p \in \alpha$ et $\alpha \leq \beta$ (qui veut dire $\alpha \subseteq \beta$). Ainsi $\sigma \subset \beta$ et σ ne peut pas être tout $\mathbb{Q}$. Ainsi la propriété *(i)* d'une coupure est satisfaite par σ. Si $p \in \sigma$, alors il existe un $\alpha_1 \in E$ qui contient ce p. Si $q \in \mathbb{Q}$ et $q < p$, alors $q \in \alpha_1$ et donc $q \in \sigma$ (propriété *(ii)* ✓). Finalement, pour ce même $p \in \sigma$, il existe $r \in \alpha_1$ tel que $p < r$ et, à nouveau, puisque $\alpha_1 \subset \sigma$, il faut que $r \in \sigma$ (propriété *(iii)* ✓). Donc σ est une coupure.

La dernière étape a pour but de montrer que σ est la plus petite borne supérieure de E. Que σ soit une borne supérieure est assez clair : σ a été obtenue en faisant l'union de tous les éléments de E et donc $\alpha \subset \sigma$ (c'est-à-dire $\alpha \leq \sigma$) pour tout $\alpha \in E$. Soit maintenant une coupure γ telle que $\gamma < \sigma$. Puisque l'inégalité est stricte, il existe un élément q qui est dans σ, mais pas dans γ. Puisque q est dans σ, il appartient à un $\alpha_2 \in E$ et $\gamma < \alpha_2$ et γ ne peut pas être une borne supérieure pour l'ensemble E. Ainsi, toute coupure $\gamma < \sigma$ n'est pas une borne supérieure et σ est donc la plus borne supérieure de E : $\sup E = \sigma$.

Ces arguments démontrent donc :

Théorème 16. *La paire $(\mathbb{R}, <)$ possède la propriété de la plus petite borne supérieure.*

Ces arguments sont difficiles et il faut les lire plusieurs fois pour les comprendre. Heureusement la preuve de ce théorème est la partie la plus difficile de la construction des nombres réels.

L'addition dans $\mathbb{R}$ — L'addition est aisément définie. Soient α et β deux éléments de $\mathbb{R}$ (deux coupures). Leur somme est définie comme l'ensemble

$$\alpha + \beta \stackrel{\text{def}}{=} \{a + b \mid a \in \alpha, b \in \beta\}.$$

C'est donc la somme de toutes les paires d'éléments, le premier provenant de l'ensemble α, le second de β. Puisque la somme de deux nombres rationnels est un nombre rationnel, $\alpha + \beta \subset \mathbb{Q}$.

La première étape consiste à montrer que $\alpha + \beta$ est une coupure, c'est-à-dire qu'elle vérifie les trois propriétés des coupures de Dedekind. Puisque ni α ni β ne sont vides, l'ensemble $\alpha + \beta$ ne l'est pas non plus. Si $p \notin \alpha$ et $q \notin \beta$, alors p est une borne supérieure de α et q de β. Donc $a < p$ pour tout élément $a \in \alpha$ et $b < q$ pour tout élément $b \in \beta$. Alors $a + b < p + q$ pour tout $a \in \alpha$ et $b \in \beta$ et $p + q$ est une borne supérieure de $\alpha + \beta$ et $\alpha + \beta \neq \mathbb{Q}$ (propriété *(i)* ✓).

Soit $c \in \alpha + \beta$. C'est donc qu'il existe $a \in \alpha$ et $b \in \beta$ tels que $c = a + b$. Si $d \in \mathbb{Q}$ et $d < c$, alors $d - b < c - b = a$ et $d - b \in \alpha$. Ainsi $d = (d - b) + b$ s'écrit comme une somme d'un élément $d - b \in \alpha$ et d'un élément $b \in \beta$ et c'est donc élément $\alpha + \beta$ (propriété *(ii)* ✓). Finalement, pour ce même $c = a + b$ dans $\alpha + \beta$, il est possible de trouver $a' \in \alpha$ avec $a < a'$ et, similairement, $b' \in \beta$ avec $b < b'$. Alors $c = a + b < a' + b'$ avec $a' + b' \in \alpha + \beta$ (propriété *(iii)* ✓). Ainsi $\alpha + \beta$ est une coupure.

Soit α_0 la coupure correspondant au neutre additif de $\mathbb{Q}$ dans la correspondance $q \leftrightarrow \alpha_q$. Cet élément de $\mathbb{R}$ est le neutre de l'addition dans $\mathbb{R}$. Avec cette notation, les propriétés de l'addition s'énoncent comme suit.

Théorème 17. *La paire $(\mathbb{R}, +)$ est un groupe abélien, c'est-à-dire $+$ satisfait :*

(i) existence d'un neutre : $\alpha_0 + \beta = \beta + \alpha_0 = \beta$;

(ii) associativité : $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$;

(iii) existence d'un inverse additif : pour $\alpha \in \mathbb{R}$, il existe $\alpha' \in \mathbb{R}$ tel que $\alpha + \alpha' = \alpha' + \alpha = \alpha_0$;

(iv) commutativité : $\alpha + \beta = \beta + \alpha$

pour tout $\alpha, \beta, \gamma \in \mathbb{R}$.

Preuve. Nous ne prouvons qu'une de ces propriétés ici. L'ensemble $\alpha + \beta$ est l'ensemble des éléments $a + b$ où $a \in \alpha$ et $b \in \beta$. L'ensemble $\beta + \alpha$, lui, contient les éléments de la forme $b + a$ où $a \in \alpha$ et $b \in \beta$. Mais $a + b = b + a$ dans les rationnels. Alors tout élément de $\alpha + \beta$ est contenu dans $\beta + \alpha$ et vice versa. Donc la commutativité est vérifiée. □

La définition des coupures et de l'ordre $<$ impliquent que certaines propriétés « évidentes » requièrent maintenant une preuve. Par exemple

Proposition 18. *Si α, β, γ sont des éléments de $\mathbb{R}$ et $\beta < \gamma$, alors $\alpha + \beta < \alpha + \gamma$.*

Preuve. Par les définitions de $<$ et $+$, l'inégalité $\beta < \gamma$ implique $\beta \subseteq \gamma$ et $\beta \neq \gamma$, et donc $\alpha + \beta \subseteq \alpha + \gamma$. Reste à montrer que $\alpha + \beta \neq \alpha + \gamma$. Mais, si les sous-ensembles $\alpha + \beta$ et $\alpha + \gamma$ étaient égaux, l'existence de l'inverse additif de α impliquerait que $\beta = \gamma$, ce qui est faux. Donc $\alpha + \beta < \alpha + \gamma$. □

Le multiplication dans $\mathbb{R}$ — La définition de la multiplication n'est guère plus difficile que celle de l'addition. Elle sera faite en exercice. Elle possède les propriétés usuelles et le théorème qui suit regroupe les propriétés de l'ensemble des nombres réels $\mathbb{R}$. Rappelons que la coupure α_1 est le sous-ensemble de $\mathbb{Q}$ contenant les rationnels plus petits que 1.

Théorème 19. *Le quadruplet $(\mathbb{R}, +, \times, \leq)$ possède les propriétés suivantes :*

(i) $(\mathbb{R}, +)$ *est un groupe abélien de neutre* α_0 *;*

(ii) $(\mathbb{R} \setminus \{\alpha_0\}, \times)$ *est un groupe abélien de neutre* α_1 *;*

(iii) l'opération $\times$ *est distributive sur l'opération* $+$*.*

L'ordre $\leq$ *est un ordre total. Ainsi* $(\mathbb{R}, +, \times, \leq)$ *est un corps totalement ordonné possédant la propriété de la plus petite borne supérieure.*

EXERCICES

20. Vrai ou faux.

(a) L'ensemble $\alpha_0 = \{p \in \mathbb{Q} \mid p < 0\}$ est un élément de $\mathbb{R}$.

(b) Le sous-ensemble $\{p \in \mathbb{Q} \mid p \leq 0\}$ est un élément de $\mathbb{R}$.

(c) Le sous-ensemble de $\mathbb{Q}$ constitué des rationnels négatifs est une coupure.

(d) $\{p \in \mathbb{Q} \mid p^2 < 4\}$ est une coupure de Dedekind.

(e) $\sup \{p \in \mathbb{Q} \mid p^2 < 4\} = 4$.

(f) $\{p \in \mathbb{Q} \mid p^3 < 1\}$ est une coupure de Dedekind.

(g) Soit $E \subset \mathbb{Q}$ un sous-ensemble de $\mathbb{Q}$ possédant une plus petite borne supérieure. Alors cette plus petite borne supérieure est unique.

21. (a) Montrer que, dans tout ensemble $\overline{(n, d)} \in \mathbb{Q}$, il existe une paire (n_0, d_0) telle que $\text{pgcd}(n_0, d_0) = 1$? (On dit alors que $\frac{n_0}{d_0}$ est la forme réduite de $\frac{n}{d}$.)

(b) La paire (n_0, d_0) est-elle unique ? Si non, quelle condition doit-on ajouter pour qu'une unique paire soit réduite ?

22. Dans cet exercice, on utilise les notions de nombres rationnels et irrationnels développées depuis l'école secondaire. Ainsi la solution de $x^2 = 2$ est notée $\sqrt{2}$ et la proposition 14 dit que ce $\sqrt{2}$ est irrationnel. Montrer que

(a) $\sqrt{3}$ est irrationnel ;

(b) $\sqrt{12}$ est irrationnel ;

(c) $a + b\sqrt{2}$ est irrationnel pour tout $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^\star$;

(d) le produit de deux irrationnels peut être rationnel ;

(e) la somme d'un rationnel et d'un irrationnel est irrationnelle ;

(f) le produit d'un rationnel et d'un irrationnel est irrationnel.

23. Terminer la preuve du théorème 15.

24. (a) Montrer l'associativité de l'addition dans $\mathbb{R}$.

(b) Montrer que α_0 est le neutre de l'addition dans $\mathbb{R}$.

Note : la preuve de l'existence d'un inverse additif n'est pas suggérée en exercice, car elle est plus difficile et repose sur la propriété archimédienne de $\mathbb{Q}$ que nous n'avons pas introduite : pour tout $q \in \mathbb{Q}$, il existe $n \in \mathbb{N}$ tel que $q < n$. Euclide reconnaît que cette propriété n'est pas évidente et l'énonce comme la définition 4 au début du livre V des *Éléments*.

25. Soit α et β deux coupures. Montrer que

(a) $\sup(\alpha + \beta) = \sup \alpha + \sup \beta$;

(b) $\sup(\alpha \cup \beta) = \max(\sup \alpha, \sup \beta)$;

(c) $\sup(\alpha \cap \beta) = \min(\sup \alpha, \sup \beta)$.

26. Cet exercice définit la multiplication $\times$ sur $\mathbb{R}$.

(a) Montrer que définir la multiplication par

$$\alpha \times \beta \stackrel{!}{=} \{a \cdot b \mid a \in \alpha, b \in \beta\}$$

ne peut pas fonctionner. Suggestion : penser aux nombres négatifs.

(b) Après ce faux départ, il est raisonnable de commencer en définissant le produit entre deux coupures α et β lorsque les deux sont plus grandes que le neutre α_0. Montre que, si $\alpha > \alpha_0$ et $\beta > \alpha_0$, alors

$$\alpha \times \beta \stackrel{\text{def}}{=} \{p \mid p < a \cdot b \text{ pour certains } a \in \alpha, b \in \beta \text{ et } a, b > 0\}$$

est une coupure.

(c) Soit $\alpha_1 = \{p \in \mathbb{Q} \mid p < 1\}$. Montrer que, si $\alpha > \alpha_0$, alors $\alpha_1 \times \alpha = \alpha \times \alpha_1 = \alpha$.

(d) Montrer que, restreinte aux coupures $> \alpha_0$, la multiplication définie en **(b)** est associative et commutative.

(e) Suggérer une définition de $\alpha \times \alpha_0$ pour une coupure quelconque α. (La coupure α_0 est le neutre additif.) Suggérer une définition de $\alpha \times \beta$ quand une ou les deux coupures α et β sont $< \alpha_0$.

(f) Les définitions suggérées préservent-elles l'associativité ? la commutativité ? la propriété du neutre α_1 ?

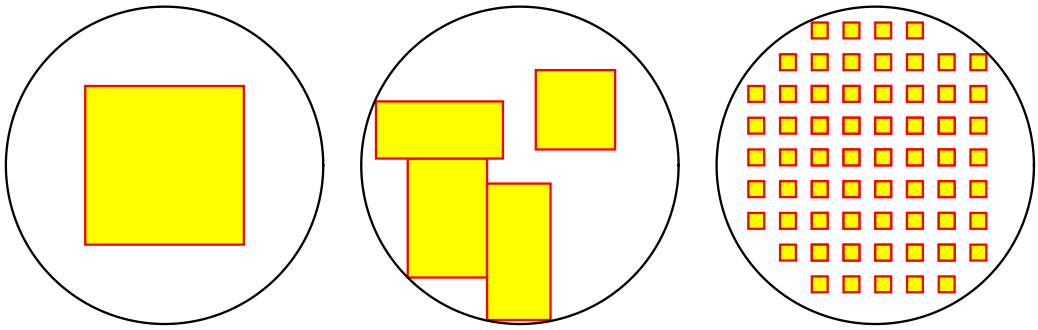
27. Soit C le cercle de rayon 1. On appellera une mosaïque $\mathcal{M}$ un ensemble fini de rectangles vérifiant les propriétés suivantes :

(M1) tous les rectangles sont à l'intérieur ou sur le cercle C ;

(M2) toutes les bases des rectangles sont horizontales ;

(M3) les côtés des rectangles ont des longueurs $\in \mathbb{Q}$;

(M4) si deux rectangles distincts s'intersectent, alors leur intersection ne contient que des parties de leurs côtés.



Voici quelques mosaïques. Soit $a(\mathcal{M})$ la somme des aires des rectangles de la mosaïque $\mathcal{M}$ et soit α l'union du neutre α_0 et de l'ensembles des aires de toutes les mosaïques, chacune respectant les conditions (M1) à (M4).

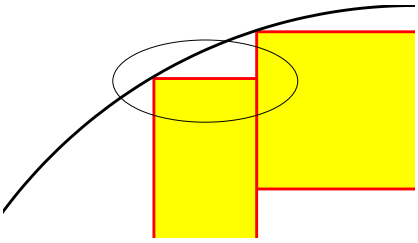
(a) Montrer que $\alpha \subset \mathbb{Q}$.

(b) Montrer que α est non vide et bornée supérieurement.

(c) Montrer que α vérifie la propriété *(ii)* des coupures. Suggestion : réduire l'aire de la mosaïque d'aire p, rectangle par rectangle.

(d)

Montrer que α vérifie la propriété *(iii)* des coupures ; en conclure que α est une coupure. Suggestion : pour le cas où la mosaïque d'aire p possède des rectangles touchant le cercle C, considérer le rectangle ayant le plus petit côté parmi ceux touchant le cercle. Ce rectangle aura l'apparence ci-dessous. Construire une nouvelle mosaïque d'aire $r > p$.



(e) Quel est le supremum de α ?

28. Est-ce que $(\mathbb{R}, +, \times)$ est un corps ? Si oui, le prouver ; si non, dire pourquoi.

3.5 Les nombres complexes

Cette dernière section introduit l'ensemble des nombres complexes. C'est un ensemble avec lequel certains des étudiants pourraient ne pas être familiers et une partie de la section sera donc consacrée à apprendre à « calculer » avec les nombres complexes. Mais avant, il est utile d'introduire ces nombres en réfléchissant au travail accompli à ce point.

Les ensembles suivants ont maintenant été introduits :

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}.$$

Le passage de $\mathbb{N}$ à $\mathbb{Z}$ a permis de donner à chaque élément de $\mathbb{N}$ un inverse additif. Celui de $\mathbb{Z}$ à $\mathbb{Q}$ a donné un inverse multiplicatif à chaque élément de $\mathbb{Z}$. Même si nous avons noté que l'ensemble $\mathbb{Q}$ ne contenait pas d'éléments vérifiant $x^2 = 2$, le but du passage de $\mathbb{Q}$ à $\mathbb{R}$ était d'assurer que le nouvel ensemble ait la propriété de la plus petite borne supérieure. Il y a, dans l'ensemble $\mathbb{R}$, une coupure qui joue le rôle de $\sqrt{2}$, mais était-ce nécessaire de construire l'ensemble $\mathbb{R}$ pour « ajouter » à $\mathbb{Q}$ une solution de $x^2 = 2$? Précisons cette question.

Premièrement, est-il possible d'étendre $\mathbb{Q}$ pour que le nouvel ensemble contienne une solution à $x^2 = 2$, sans pour autant requérir la propriété de la plus petite borne supérieure ? Et si oui, est-ce que le nouvel ensemble $\mathbb{S}$ se situe entre $\mathbb{Q}$ et $\mathbb{R}$: $\mathbb{Q} \subset \mathbb{S} \subset \mathbb{R}$? Et l'ensemble $\mathbb{S}$ est-il un corps ? Ces questions peuvent paraître étroites puisque l'équation $x^2 = 2$ est quelque peu arbitraire. Pourquoi ne pas ajouter une solution de $x^7 = 1\,958\,763$? Ou encore de $x^3 + \sqrt{2}x^2 - 7x - 1 = 0$? Donc, deuxièmement, il est utile de demander s'il existe un ensemble de nombres contenant toutes les racines de polynômes dont les coefficients seraient des éléments de $\mathbb{R}$. Cette question est nettement plus ambitieuse, mais les deux questions sont liées : celle de l'existence d'un corps contenant une solution de $x^2 = 2$ et celle d'un corps contenant les solutions de toutes les équations $p(x) = 0$ où p est un polynôme à coefficients réels.

La réponse à la première famille de questions est oui, il existe tel un corps ; il est souvent noté $\mathbb{Q}(\sqrt{2})$. Sa construction est facile et amusante. De plus cette construction sera copiée lors de notre construction de l'ensemble des nombres complexes $\mathbb{C}$. Il faut que le lecteur arrête momentanément sa lecture pour aller faire l'exercice 29. Et il faudra aussi que les objets mathématiques suivants soient revus.

Rappel

- coordonnées polaires ;
- inégalité du triangle ;
- développement en série de Taylor des fonctions exp, sin et cos ;
- identité trigonométrique pour les sinus et cosinus d'une somme d'angles.

Définition de l'ensemble $\mathbb{C}$ **—** Les nombres réels ont été construits comme étant les sous-ensembles de $\mathbb{Q}$ satisfaisant les axiomes des coupures de Dedekind. À partir de maintenant, nous identifierons la coupure α à sa plus petite borne supérieure $\sup \alpha$ et nous dénoterons ces supremums par des lettres latines a, b, c.

Le lecteur a maintenant fait l'exercice 29. Nous en copions la démarche, non plus avec la racine $\sqrt{2}$ de l'équation $x^2 = 2$, mais plutôt avec une racine de $x^2 = -1$ que nous noterons i. Ainsi

$$i^2 = -1.$$

Le nombre i n'appartient pas à l'ensemble des nombres réels. En effet, le produit d'un nombre avec lui-même est toujours positif dans les réels (ou nul si le nombre est lui-même nul). Donc il n'y a pas de réel dont le carré est -1. Ajouter ce « nouveau nombre » à l'ensemble $\mathbb{R}$ est une opération semblable à ajouter le « nouveau nombre » $\sqrt{2}$ à l'ensemble $\mathbb{Q}$ pour obtenir l'ensemble $\mathbb{Q}(\sqrt{2})$. Pour toute la présente section, la lettre i est réservée pour cette racine.

L'ensemble $\mathbb{C}$ est l'ensemble des combinaisons $a + b \cdot i$ où $a, b \in \mathbb{R}$:

$$\mathbb{C} \stackrel{\text{def}}{=} \{a + b \cdot i \mid a, b \in \mathbb{R}\}.$$

Nous noterons par des lettres de la fin de l'alphabet $(x, y, z, \dots)$ les éléments de $\mathbb{C}$ et par les lettres du début $(a, b, c, \dots)$ les coefficients réels qui permettent d'écrire un nombre complexe, par exemple $z = a + b \cdot i \in \mathbb{C}$ avec $a, b \in \mathbb{R}$. Puisque i n'est pas un nombre réel, les parties a et b de $z = a + b \cdot i$ sont bien déterminées ; a et b se nomment les parties réelle et imaginaire du nombre $z = a + b \cdot i$ et on écrit

$$a = \operatorname{Re} z \qquad \text{et} \qquad b = \operatorname{Im} z.$$

Pour que deux nombres z_1 et z_2 de $\mathbb{C}$ soient distincts, il faut et il suffit que leurs parties réelles ou leurs parties imaginaires soient distinctes. Ainsi les équations

$$(-i)^2 = (-1)^2 \cdot i^2 = (+1) \cdot (-1) = -1$$

montrent que l'équation $x^2 = -1$ a deux solutions distinctes dans $\mathbb{C}$: i et $-i$.

Les opérations $+$ et $\times$ dans l'ensemble $\mathbb{C}$ — La définition de l'addition et de la multiplication dans l'ensemble $\mathbb{C}$ copie celles que nous avons données pour l'ensemble $\mathbb{Q}(\sqrt{2})$. Soit $z_1 = a_1 + b_1 \cdot i$ et $z_2 = a_2 + b_2 \cdot i$ deux nombres complexes (avec $a_1, b_1, a_2, b_2 \in \mathbb{R}$). Leur somme est

$$z_1 + z_2 \stackrel{\text{def}}{=} (a_1 + a_2) + (b_1 + b_2) \cdot i$$

et leur produit

$$z_1 z_2 = (a_1 + ib_1)(a_2 + ib_2) = (a_1 a_2 - b_1 b_2) + i(a_1 b_2 + a_2 b_1).$$

Voici deux exemples simples de calcul utilisant ces définitions ; si $z_1 = 1 + 2 \cdot i$ et $z_2 = -3 + i$, alors

$$z_1 + z_2 = (1 + 2 \cdot i) + (-3 + i) = -2 + 3 \cdot i$$

et

$$z_1 z_2 = (1 + 2 \cdot i) \cdot (-3 + i) = (1 \cdot (-3) - (2 \cdot 1)) + (2 \cdot (-3) + 1 \cdot 1) \cdot i = -5 - 5 \cdot i.$$

Le nombre complexe $0 + 0 \cdot i$ est le neutre de l'addition et $1 + 0 \cdot i$ est celui de la multiplication. L'inverse additif de $z = a + b \cdot i$ est simplement $(-a) + (-b) \cdot i$. Comme pour l'inverse multiplicatif de $a + b\sqrt{2}$ dans le corps $\mathbb{Q}(\sqrt{2})$, l'inverse de $z = a + b \cdot i$ doit être de la forme $a' + b' \cdot i$ avec $a', b' \in \mathbb{R}$, si cet inverse est pour appartenir à $\mathbb{C}$. Il est facile de déterminer a' et b' comme suit :

$$\frac{1}{z} = \frac{1}{a + b \cdot i} = \frac{1}{a + b \cdot i} \cdot \frac{a - b \cdot i}{a - b \cdot i}$$

où le dénominateur peut maintenant être réécrit comme $(a+b\cdot i)(a-b\cdot i) = (a^2+b^2)+(ab-ba)\cdot i = a^2+b^2$ par la définition de la multiplication. Donc

$$\frac{1}{z} = \frac{a-b\cdot i}{a^2+b^2} = \underbrace{\frac{a}{a^2+b^2}}_{a'} + \underbrace{\frac{-b}{a^2+b^2}}_{b'}\cdot i.$$

Ces expressions montrent clairement que a' et b' sont des nombres réels et donc que $\frac{1}{z}$ est un nombre complexe. Elles montrent également que le seul nombre complexe $z = a+b\cdot i$ qui n'a pas d'inverse est celui pour lequel $a^2+b^2 = 0$, c'est-à-dire le neutre additif $0+0\cdot i$.

Le théorème ci-dessous suit directement des propriétés similaires valides pour les nombres réels.

Théorème 20. *Le triplet $(\mathbb{C}, +, \times)$ est un corps, c'est-à-dire*
(i) $(\mathbb{C}, +)$ *est un groupe abélien ;*
(ii) $(\mathbb{C}\setminus\{0+0\cdot i\}, \times)$ *est un groupe abélien ;*
(iii) la multiplication $\times$ est distributive sur l'addition $+$.

À nouveau, le lecteur doit interrompre ici sa lecture, le temps de maîtriser l'addition et la multiplication de nombres complexes (exercices 30 et 31).

La conjugaison complexe et la valeur absolue d'un nombre complexe — La conjugaison complexe d'un nombre complexe $z = a+ib$ est dénotée par une barre horizontale au-dessus de ce nombre [9] ($\bar{z}$ est le conjugué complexe de z) et est donnée, lorsque a et b sont les parties réelle et imaginaire de z, par

$$\bar{z} = a - b\cdot i.$$

Proposition 21. *Si y et z sont des nombres complexes, alors*
(i) $\overline{y+z} = \bar{y}+\bar{z}$ *;*
(ii) $\overline{y\cdot z} = \bar{y}\cdot\bar{z}$ *;*
(iii) $z+\bar{z} = 2\,\mathrm{Re}\,z$ *et* $z-\bar{z} = 2\,\mathrm{Im}\,z$ *;*
(iv) $z\cdot\bar{z}$ *est un nombre réel* ≥ 0 *et est égal à zéro que lorsque* $z = 0$.

Preuve. Chacune de ces propriétés est obtenue en écrivant le nombre complexe comme une somme $a+b\cdot i$ et en développant. Par exemple, pour la dernière :

$$z\cdot\bar{z} = (a+b\cdot i)\cdot\overline{(a+b\cdot i)} = (a+b\cdot i)\cdot(a-b\cdot i) = (a^2+b^2)+(ab-ba)\cdot i = a^2+b^2$$

qui est effectivement un nombre réel positif ou nul (et, dans ce dernier cas, il faut que $a = b = 0$, c'est-à-dire que $z = 0$). □

La propriété *(iv)* permet la définition de la valeur absolue d'un nombre complexe notée par $|z|$ et donnée par

$$|z| = +\sqrt{z\bar{z}}$$

9. Attention : dans les sections précédentes, une barre horizontale au-dessus d'un symbole désignait la classe d'équivalence de ce symbole. Ici elle dénote le conjugué complexe du nombre sous la barre.

et, si a et b sont les parties réelle et imaginaire de z, alors

$$|z| = \sqrt{a^2 + b^2}.$$

Le conjugué du conjugué est le nombre original :

$$\bar{\bar{z}} = \overline{\overline{a + b \cdot i}} = \overline{a - b \cdot i} = a + b \cdot i = z.$$

Proposition 22. *Si y et z sont des nombres complexes, alors*

(v) $|z| > 0$ *à moins que* $z = 0$ *et alors* $|z| = 0$ *;*

(vi) $|\bar{z}| = |z|$ *;*

(vii) $|y \cdot z| = |y| \cdot |z|$ *;*

(viii) $|\mathrm{Re}\, z| \leq |z|$ *;*

(ix) $|y + z| \leq |y| + |z|$.

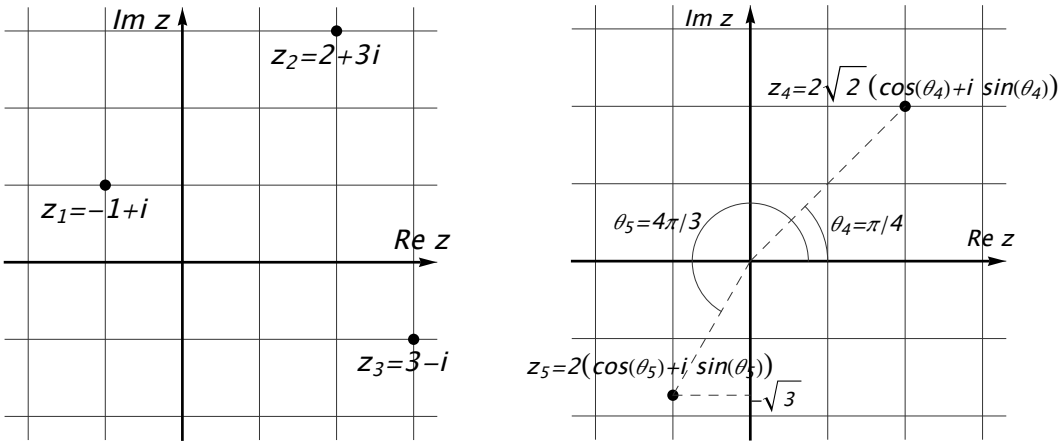
Preuve. C'est la preuve de la dernière identité qui est la plus difficile. Notons d'abord $\overline{y\bar{z}} = \bar{y}z$ et alors $y\bar{z} + \bar{y}z = 2\ \mathrm{Re}\ (y\bar{z})$ par la propriété *(iii)*. Ainsi

$$\begin{aligned} |y + z|^2 &= (y + z)(\bar{y} + \bar{z}) = y\bar{y} + y\bar{z} + \bar{y}z + z\bar{z} \\ &= |y|^2 + 2\ \mathrm{Re}\ (y\bar{z}) + |z|^2 \\ &\leq |y|^2 + 2|y\bar{z}| + |z|^2 \qquad \text{par la propriété } \textit{(viii)} \\ &= |y|^2 + 2|y| \cdot |z| + |z|^2 = (|y| + |z|)^2 \end{aligned}$$

et l'inégalité *(ix)* est obtenue en prenant la racine carrée des deux membres de l'inégalité. □

Cette dernière inégalité *(ix)* ressemble beaucoup à l'inégalité du triangle. Le prochain point montrera que cette ressemblance n'est pas fortuite. Mais avant, encore une interruption de lecture : vous reviendrez à votre lecture quand vous aurez fait les exercices 32 et 33.

Représentations cartésienne et polaire d'un nombre complexe — Chaque élément de $\mathbb{C}$ peut être représenté par un point du plan. En effet, si on appelle a la partie réelle de z et b sa partie imaginaire, alors le nombre complexe z peut être représenté par le point de coordonnées (a, b) dans le plan. Alors l'axe horizontal correspond à la partie réelle des nombres complexes et l'axe vertical à leur partie imaginaire. (Exercice : vérifier sur la figure ci-contre (à gauche) que les trois points dessinés correspondent bien à leur position relative aux axes réel et imaginaire.) Outre cette *représentation cartésienne*, le nombre complexe z possède une *représentation polaire*, similaire à celle utilisée pour les points du plan ab. Soit donc $z = r(\cos\theta + i \sin\theta)$ où r est un nombre réel ≥ 0 et θ est un angle réel choisi tel que $0 \leq \theta < 2\pi$. Puisque la valeur absolue d'un nombre complexe $z = a + b \cdot i$ (de parties réelle a et imaginaire b) est $|z| = \sqrt{a^2 + b^2}$, le nombre r est simplement $r = |z|$. (Ainsi la valeur absolue $|z|$ est la distance entre le point (a, b) et l'origine du plan cartésien ab.) L'angle doit être choisi pour que $a = \mathrm{Re}\, z = r\cos\theta$ et $b = \mathrm{Im}\, z = r\sin\theta$. Attention : il faudra donc prendre la bonne branche de la fonction arctan pour que $\theta = \arctan b/a$ reproduise correctement a et b. La définition usuelle de arctan donne un résultat dans l'intervalle $(-\frac{\pi}{2}, \frac{\pi}{2})$ et, pour couvrir tous les angles dans l'intervalle $[0, 2\pi)$,



un multiple entier de π devra peut-être être ajouté à l'arctangente du quotient b/a. Avec cette mise en garde, le nombre complexe $z = a + b \cdot i$ où a et b sont des nombres réels peut être écrit comme $z = r(\cos\theta + i \sin\theta)$ avec

$$a = r\cos\theta \qquad \text{et} \qquad b = r\sin\theta$$

$$r = |z| = \sqrt{a^2 + b^2} \qquad \text{et} \qquad \theta = \arctan b/a + n\pi, \ \text{ où } n \in \mathbb{Z}.$$

Des exercices ! Vérifiez d'abord que les points marqués sur le graphique ci-contre (à droite) correspondent bien à leur représentation polaire. Puis, allez faire les exercices 34 et 35.

Racines n-ièmes de l'unité et formule d'Euler — La construction des nombres complexes a singularisé la solution d'une équation bien particulière, l'équation $x^2 = -1$, alors que la construction de $\mathbb{Q}(\sqrt{2})$ proposée en exercice avait choisi plutôt une solution de l'équation $x^2 = 2$. Il est donc justifié de se demander si le choix $x^2 = -1$ a permis de gagner les solutions d'autres équations polynomiales. Existe-t-il un nombre complexe z solutionnant l'équation $p(z) = 0$ si p est un polynôme à coefficients réels ? ou même à coefficients complexes ? Nous répondrons à cette question en deux temps. Notre première étape est de montrer que les équations $z^n = y$ possèdent n solutions distinctes dans $\mathbb{C}$, quelque soit $n \geq 1$ et $y \in \mathbb{C}$.

Un nombre (complexe) z est appelé une racine n-ième d'un nombre complexe y si

$$z^n = y.$$

En particulier les solutions de l'équation $z^n = 1$ se nomment les racines n-ièmes de l'unité. La représentation polaire permet de calculer les racines n-ièmes d'un nombre complexe. Pour un $y \neq 0$ donné, il existe n racines distinctes de l'équation $z^n = y$. Si $y = r(\cos\theta + i\sin\theta)$, les racines sont

$$z_k = r^{1/n}\big(\cos((\theta + 2\pi k)/n) + i\sin((\theta + 2\pi k)/n)\big) \qquad (n)$$

pour $k = 0, 1, \ldots, n-1$. Il s'agit bien de n solutions distinctes puisque l'incrément $2\pi/n$ de l'angle polaire balaie n points distincts sur le cercle de rayon $r^{1/n}$ lorsque k va de 0 à $n-1$.

Avant de vérifier cette expression pour les n racines de $z^n = y$, voici quelques exemples. Pour obtenir les solutions de l'équation $z^2 = 4$, il faut poser $n = 2$ et $y = 4$ dans la formule ci-dessus. Le nombre y s'écrit comme $4(\cos 0 + i \sin 0)$ en coordonnées polaires et, donc, $r = 4$ et $\theta = 0$. Alors les $n = 2$ racines de $z^2 = 4$ sont obtenues en posant d'abord $k = 0$:

$$z_0 = (4)^{\frac{1}{2}}(\cos((0 + 2\pi 0)/2) + i \sin((0 + 2\pi 0)/2)) = 2(1 + i \cdot 0) = 2$$

puis $k = 1$:

$$z_1 = (4)^{\frac{1}{2}}(\cos((0 + 2\pi 1)/2) + i \sin((0 + 2\pi 1)/2)) = 2(-1 + i \cdot 0) = -2$$

puisque $\cos \pi = -1$. Évidemment les racines carrées de 4 étaient connues, mais il est agréable de vérifier que la formule générale (n) donne les bonnes solutions. Donnons un exemple qui nécessite les nombres complexes (et non pas seulement les nombres réels). Voici les 3 racines cubiques de 1. Ici $n = 1$, $y = 1$ et puisque $y = 1(\cos 0 + i \sin 0)$, les deux coordonnées polaires sont $r = 1$ et $\theta = 0$. Alors $(1)^{1/3} = 1$ et la formule (n) donne

$$z_0 = (\cos 0 + i \sin 0), \qquad z_1 = (\cos 2\pi/3 + i \sin 2\pi/3) \qquad \text{et} \qquad z_2 = (\cos 4\pi/3 + i \sin 4\pi/3).$$

Puisque $\cos 2\pi/3 = -\frac{1}{2} = \cos 4\pi/3$, $\sin 2\pi/3 = \frac{\sqrt{3}}{2} = -\sin 4\pi/3$, les racines cubiques de l'unité sont

$$z_0 = 1, \qquad z_1 = -\frac{1}{2} + i \cdot \frac{\sqrt{3}}{2} \qquad \text{et} \qquad z_2 = -\frac{1}{2} - i \cdot \frac{\sqrt{3}}{2}.$$

Les solutions z_1 et z_2 sont nouvelles et il est utile de vérifier qu'elles sont vraiment des racines cubiques de 1. Par exemple

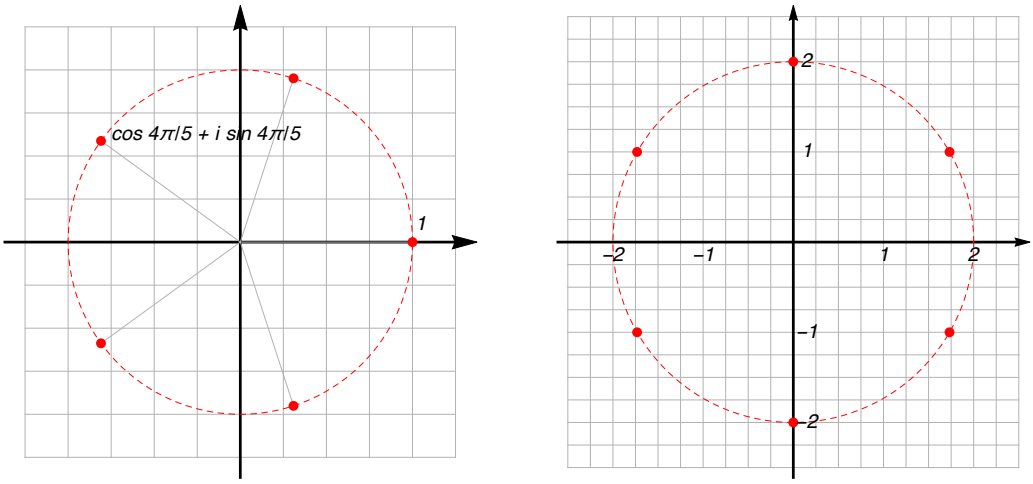
$$\begin{aligned} z_1 \cdot z_1 &= \big(-\frac{1}{2} + i \cdot \frac{\sqrt{3}}{2}\big) \cdot \big(-\frac{1}{2} + i \cdot \frac{\sqrt{3}}{2}\big) \\ &= \big(\frac{1}{4} - \frac{3}{4}\big) + i \cdot \big(-\frac{1}{2}\frac{\sqrt{3}}{2} - \frac{\sqrt{3}}{2}\frac{1}{2}\big) \\ &= -\frac{1}{2} - i\frac{\sqrt{3}}{2} = z_2 \end{aligned}$$

et enfin

$$\begin{aligned} z_1^3 = z_1 \cdot z_2 &= \big(-\frac{1}{2} + i \cdot \frac{\sqrt{3}}{2}\big) \cdot \big(-\frac{1}{2} - i \cdot \frac{\sqrt{3}}{2}\big) \\ &= \big(\frac{1}{4} + \frac{3}{4}\big) + i \cdot \big(+\frac{1}{2}\frac{\sqrt{3}}{2} - \frac{\sqrt{3}}{2}\frac{1}{2}\big) \\ &= 1 \end{aligned}$$

tel qu'annoncé.

Voici une représentation graphique de certaines racines d'équations de la forme $z^n = y$. Le graphique de gauche représente, par des points rouges, les cinq racines cinquièmes de l'unité, c'est-à-dire les cinq racines de l'équation $z^5 = 1$. Les cinq sont sur le cercle unité dans le plan des valeurs réelles et imaginaires puisque le y est ici 1 et $(1)^{1/5} = 1$. L'équation donnant la forme polaire de deux des solutions est aussi donnée, celle pour $k = 0$ et pour $k = 2$. Le



graphique de droite donne toutes les solutions d'une équation de la forme $z^n = y$. Exercice : trouver les n et y pour ce graphique !

La formule de De Moivre, prouvée à l'exercice 35 :

$$z^n = r^n(\cos(n\theta) + i\sin(n\theta))$$

permet de vérifier que les solutions z_k proposées par la formule (n) sont bien des n-ièmes racines de y. Il suffit de remplacer le rayon r par celui des z_k (et donc faire la substitution $r \to r^{1/n}$) et l'angle par ceux des z_k ($\theta \to \theta_k = (\theta + 2\pi k)/n$) :

$$\begin{aligned}
(z_k)^n &= (r^{1/n})^n \cdot (\cos(n\theta_k) + i\sin(n\theta_k))) \\
&= r \cdot (\cos(n(\theta + 2\pi k)/n) + i\sin(n(\theta + 2\pi k)/n)) \\
&= r \cdot (\cos(\theta + 2\pi k) + i\sin(\theta + 2\pi k)) \\
&= r \cdot (\cos(\theta) + i\sin(\theta)) \qquad \text{par la périodicité de sin et cos} \\
&= y.
\end{aligned}$$

Donc, en étendant $\mathbb{R}$ par l'ajout d'une solution de l'équation $x^2 = -1$, les solutions des équations $z^n = y$ ont été également ajoutées, et ce, pour tout $y \in \mathbb{C}$ et $n \geq 1$.

Un autre résultat est intimement relié au précédent. Pour l'introduire nous utiliserons des relations obtenues dans les cours de calcul différentiel et intégral pour les fonctions réelles. Il s'agit des développement en série de Taylor des fonctions (réelles) exponentielle et trigonomé-

triques sinus et cosinus :

$$e^z = 1 + z + \frac{1}{2!}z^2 + \frac{1}{3!}z^3 + \cdots = \sum_{i=0}^{\infty} \frac{z^n}{n!}$$
$$\sin z = z - \frac{1}{3!}z^3 + \frac{1}{5!}z^5 - \frac{1}{7!}z^7 + \cdots = \sum_{i=0}^{\infty} \frac{(-1)^i}{(2i+1)!}z^{2i+1}$$
$$\cos z = 1 - \frac{1}{2!}z^2 + \frac{1}{4!}z^4 - \frac{1}{6!}z^6 + \cdots = \sum_{i=0}^{\infty} \frac{(-1)^i}{(2i)!}z^{2i}$$

Ces relations sont habituellement prouvées dans un cours d'analyse. En fait il est possible d'étendre ces fonctions pour que leur domaine soit l'ensemble des nombres complexes (par exemple exp : $\mathbb{C} \to \mathbb{C}$). Alors l'application de ces fonctions à un nombre complexe donne un nombre complexe et les séries de Taylor demeurent valides. Nous accepterons ce fait. Supposons de plus qu'il soit possible d'intervertir l'ordre d'un nombre infini de termes de cette série (en d'autres termes, que la série soit absolument convergente). Alors on peut écrire pour $z = i\theta$:

$$\begin{aligned} e^z = e^{i\theta} &= 1 + i\theta + \frac{(i\theta)^2}{2!} + \frac{(i\theta)^3}{3!} + \frac{(i\theta)^4}{4!} + \frac{(i\theta)^5}{5!} + \frac{(i\theta)^6}{6!} + \ldots \\ &= 1 + i\theta - \frac{\theta^2}{2!} - i\frac{\theta^3}{3!} + \frac{\theta^4}{4!} + i\frac{\theta^5}{5!} - \frac{\theta^6}{6!} + \ldots \\ &= \left(1 - \frac{\theta^2}{2!} + \frac{\theta^4}{4!} - \frac{\theta^6}{6!} + \ldots\right) + i\left(\theta - \frac{\theta^3}{3!} + \frac{\theta^5}{5!} - \ldots\right) \\ &= \cos\theta + i\sin\theta \end{aligned}$$

où, à la dernière étape, nous avons utilisé le développement de Taylor des fonctions sinus et cosinus. Cette identité remarquable est la formule d'Euler [10] :

$$e^{i\theta} = \cos\theta + i\sin\theta.$$

Pour plusieurs, cette relation est une des plus remarquables des mathématiques. Par exemple, puisqu'elle est vraie pour tout θ, il est possible de la particulariser pour certains θ et, en $\theta = \pi$ (et donc $\cos\pi = -1$ et $\sin\pi = 0$), elle unit quatre des constantes fondamentales des mathématiques :

$$e^{i\pi} = -1$$

à savoir les constantes $e, i = \sqrt{-1}, \pi$ et -1.

La formule d'Euler peut être utilisée pour écrire l'exponentielle d'un nombre complexe z quelconque. En effet, pour un $z = a + ib$ avec a et b réels, on a :

$$e^z = e^{a+ib} = e^a e^{ib} = e^a(\cos b + i\sin b).$$

10. Leonhard Euler (1707–1783) est né en Suisse. Il passa une grande partie de sa carrière à Saint-Pétersbourg en Russie. Il a contribué de façon capitale à pratiquement tous les chapitres des mathématiques de l'époque (analyse, théorie des nombres, géométrie, théorie des graphes) et à plusieurs de la physique (mécanique des fluides, optique et astronomie).

Elle permet également de démontrer (ou se rappeler !) les relations trigonométriques pour les sommes d'angles. Soit $y = e^{i\phi}$ et $z = e^{i\theta}$ deux nombres complexes de valeur absolue 1. La formule d'Euler donne pour chacun

$$y = \cos\phi + i\sin\phi \qquad \text{et} \qquad z = \cos\theta + i\sin\theta$$

et leur produit est donc

$$yz = (\cos\phi \cdot \cos\theta - \sin\phi \cdot \sin\theta) + i(\sin\phi \cdot \cos\theta + \cos\phi \cdot \sin\theta).$$

Mais, puisque $yz = e^{i(\phi+\theta)}$, ce produit peut aussi être écrit sous la forme

$$yz = \cos(\phi + \theta) + i\sin(\phi + \theta).$$

Puisque les parties réelle et imaginaire sont complètement déterminées par le nombre complexe lui-même, il faut que les parties réelles des deux expressions coïncident et similairement pour les complexes :

$$\cos(\phi + \theta) = \cos\phi \cdot \cos\theta - \sin\phi \cdot \sin\theta,$$
$$\sin(\phi + \theta) = \sin\phi \cdot \cos\theta + \cos\phi \cdot \sin\theta.$$

***Le théorème fondamental de l'algèbre* —** Il est maintenant temps de répondre à la question : est-ce que l'équation polynomiale $p(z) = 0$ possède une solution $z \in \mathbb{C}$ pour tout polynôme à coefficients complexes ? La réponse est oui et montre que l'extension $\mathbb{R} \to \mathbb{C}$ a non seulement donné une solution à l'équation $x^2 = -1$, mais bien à *toute* équation polynomiale.

Théorème 23 (Théorème fondamental de l'algèbre)**.** *Soit* $p(z) = z^n + a_{n-1}z^{n-1} + \cdots + a_z z^1 + z_0$ *un polynôme de degré* $n \geq 1$ *à coefficients* $a_{n-1}, \ldots, a_1, a_0$ *complexes. Alors* $p(z)$ *possède une racine complexe, c'est-à-dire il existe* $z_0 \in \mathbb{C}$ *tel que* $p(z_0) = 0$*.*

Noter que, si z_0 est une racine de $p(z)$, alors il est possible d'écrire ce polynôme comme $p(z) = (z - z_0)q(z)$ où $q(z)$ est maintenant de degré $n - 1$. En répétant cette factorisation, on obtient le corollaire suivant.

Corollaire 24. *Un polynôme de degré* n *à coefficients complexes possède* n *racines complexes, en comptant chacune avec sa multiplicité.*

Par exemple le polynôme $p(z) = z^4 - 4z^2$ possède la racine 0 avec multiplicité 2 et les racines $+2$ et -2 avec multiplicité 1 puisque ce polynôme s'écrit comme $p(z) = (z-0)^2(z-2)(z+2)$. Ainsi il possède $2 + 1 + 1 = 4$ racines (en comptant la racine 0 deux fois) et 4 est bien le degré du polynôme.

Il existe plusieurs preuves de ce théorème. Toutes sont difficiles. La plus simple n'est tout de même pas inaccessible. Elle requiert des arguments d'analyse qui seront vus plus tard dans votre parcours. Voici cette preuve. Vous pourrez la lire après avoir fait le premier cours d'analyse.

Preuve du théorème 23. Soit $p(z)$ un polynôme tel que donné dans l'énoncé. En représentation polaire, la variable z est écrite sous la forme $re^{i\theta}$ pour certains r et θ. Puisque p est de degré $n \geq 1$, il existe un rayon R à partir duquel le terme z^n sera plus grand en valeur absolue que la somme des autres termes :

$$|z^n| > |a_{n-1}z^{n-1} + \cdots + a_1 z^1 + a_0, \qquad \text{si } |z| > R.$$

Alors il est impossible que $p(z)$ s'annule si $|z| > R$. Si p possède une racine, elle se trouve donc dans le disque $D_R = \{z \in \mathbb{C} \mid |z| \leq R\}$. Il s'agit d'un ensemble fermé (qui contient sa frontière $|z| = R$) et borné (dont les éléments sont tous plus petits en valeur absolue qu'une certaine borne, ici R). Un (grand) théorème d'analyse dit que, sur un tel ensemble fermé et borné, toute fonction atteint ses maximum et minimum, c'est-à-dire qu'il existe un point $z_0 \in D_R$ tel que $|p(z_0)|$ est le minimum parmi toutes les valeurs que $|p(z)|$ prend sur D_R (et similairement pour le maximum de $|p|$ sur D_R).

À partir d'ici, la preuve est par contradiction. Supposons que le minimum de la fonction $|p(z)|$ ne soit pas zéro, mais que ce minimum, atteint en z_0, soit égal à b_0 : $|p(z)| \geq |p(z_0)| = b_0 \neq 0$ pour tout $z \in D_R$. Développons le polynôme autour du point z_0 :

$$p(z) = (z - z_0)^n + b_{n-1}(z - z_0)^{n-1} + \cdots + b_k(z - z_0)^k + b_0$$

pour un certain k ($1 \leq k \leq n$) et certains $b_i \in \mathbb{C}$. Dans un voisinage de z_0, le polynôme $p(z)$ se comporte comme $q(z) = b_0 + b_k(z - z_0)^k$ ou, plus précisément, il existe $R_1 < R$ et une constante $M \in \mathbb{R}$ tels que

$$|p(z) - q(z)| < M|(z - z_0)^{k+1}|, \qquad \text{si } |z - z_0| < R_1.$$

Par l'inégalité du triangle (la propriété *(ix)*), cette inégalité implique la suivante :

$$|p(z)| < |q(z)| + M|(z - z_0)^{k+1}|.$$

Pour étudier le comportement de la fonction $q(z)$ autour du point z_0, écrivons les constantes b_0 et b_k en termes de leurs phases : $b_0 = |b_0|e^{i\theta_0}$ et $b_k = |b_k|e^{i\theta_k}$ et approchons le point z_0 dans le long de la droite $(z - z_0)^k = -r^k e^{i(-\theta_k + \theta_0)}$ où r est suffisamment petit pour que $r^k < R_1$. Alors

$$\begin{aligned}
|q(z)| &= |b_0 + b_k(z - z_0)^k| = |b_0| \cdot \left|1 + \frac{b_k}{b_0}(z - z_0)^k\right| \\
&= |b_0| \cdot \left|1 + \frac{|b_k|e^{i\theta_k}}{|b_0|e^{i\theta_0}} \cdot (-r^k e^{i(-\theta_k + \theta_0)})\right| \\
&= |b_0| \cdot \left|1 - \frac{|b_k|}{|b_0|}r^k\right| \\
&= |b_0| \cdot (1 - \frac{|b_k|}{|b_0|}r^k) \qquad \text{si } r^k < \frac{|b_0|}{|b_k|}, \\
&= (|b_0| - |b_k|r^k).
\end{aligned}$$

Donc, dans un voisinage de z_0,

$$|p(z)| < |b_0| - |b_k|r^k + Mr^{k+1}.$$

Puisque r^k décroît moins vite que r^{k+1} quand $r \to 0$, il existe un petit voisisange de z_0 où $(-|b_k|r^k + Mr^{k+1})$ est un nombre négatif et donc $|p(z)|$ est en fait plus petit que $p(z_0)$ dans ce voisinage. Ceci contredit le fait que $|p(z_0)|$ est la plus petite valeur de ce voisinage. Il faut donc que le minimum de $|p(z)|$ sur le disque D_R soit nul et donc qu'il existe un point z_0 où $p(z_0)$ s'annule. □

EXERCICES (La solution de quelques exercices est donnée à la fin de cette section.)

29. Cet exercice détaille la construction du corps $\mathbb{Q}(\sqrt{2})$. L'ensemble $\mathbb{Q}(\sqrt{2})$ est l'ensemble de nombres de la forme $a + b\sqrt{2}$:

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}.$$

(a) Montrer que $\mathbb{Q}$ est inclus naturellement dans $\mathbb{Q}(\sqrt{2})$. En particulier, dire pour quelles valeurs de a et b il est possible d'obtenir les neutres additif 0 et multiplicatif $1 \in \mathbb{Q}$.

(b) Soit $a + b\sqrt{2}$ et $c + d\sqrt{2}$ deux éléments de $\mathbb{Q}(\sqrt{2})$. Montrer que l'addition définie par

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) \stackrel{\text{def}}{=} (a + c) + (b + d)\sqrt{2}$$

possède toutes les propriétés usuelles : existence d'un neutre, d'inverses, associativité et commutativité.

(c) Montrer que la multiplication définie par

$$(a + b\sqrt{2}) \times (c + d\sqrt{2}) \stackrel{\text{def}}{=} (a \cdot c + 2b \cdot d) + (b \cdot c + a \cdot d)\sqrt{2}$$

possède toutes les propriétés usuelles : existence d'un neutre, d'inverses, associativité et commutativité. Suggestion : une étape est délicate dans cette question. Il faut que l'inverse multiplicatif de $a + b\sqrt{2}$ soit de la forme $a' + b'\sqrt{2}$ avec $a', b' \in \mathbb{Q}$. Pour découvrir les nombres rationnels a' et b', compléter le calcul suggéré par l'équation suivante :

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})}.$$

(d) Vérifier que la multiplication dans $\mathbb{Q}(\sqrt{2})$ est distributive sur son addition.

(e) En conclure que $\mathbb{Q}(\sqrt{2})$ est un corps $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$ strictement plus grand que $\mathbb{Q}$ et plus petit que $\mathbb{R}$. Est-il ordonné ?

30. Évaluer les expressions suivantes en les mettant sous forme $(\textit{partie réelle}) + (\textit{partie imaginaire}) \cdot i$.

(a) $(3-2i)+(-1-i)$

(b) $(1+i\sqrt{2})+(\sqrt{2}-i)$

(c) $(1+i)(1-2i)$

(d) $(2+3i)(2+i)$

(e) $(\sqrt{2}+i\sqrt{3})(\sqrt{3}-i\sqrt{2})-(\sqrt{3}+i\sqrt{2})(\sqrt{2}-i\sqrt{3})$

(f) $(4+i3)\{(2-i)-(i-3)\}$

(g) $(2+ia)\{(3+2i)+(1-i)\}i$; si a est lui-même un nombre complexe, est-ce que la réponse est différente ?

31. Évaluer ; s'il y a un dénominateur, faire les simplifications nécessaires pour qu'il soit réel.

(a) $(1-i)(1+i)$

(b) $(1-i)/(1+i)$

(c)
$$\frac{(1+i\sqrt{3})(2+i\sqrt{3})(\sqrt{3}-i)}{(1-i)^2}$$

(d)
$$2\frac{1-2i}{1+2i}+i\frac{2+i}{2-i}$$

(e)
$$\frac{a+ib}{c+id}-\frac{a-ib}{c-id}$$

(f)
$$\frac{i^2+i^7+i^{11}}{i^4+i^{10}+i^{21}+i^{23}+i^{31}}$$

32. Si $z_1=1-i$, $z_2=-2+i$ et $z_3=\sqrt{5}-i$, évaluer :

(a) $z_1^2+z_2$

(b) $|\bar{z}_1|^2$

(c) $\bar{z}_1z_2+z_1\bar{z}_2$

(d) $|z_1-z_3|$

(e) $|z_1(2+z_2)|$

(f) $\mathrm{Re}\,(z_1+2z_2+z_3)$

(g) $\mathrm{Im}\,(z_1/z_2)$

(h) $|z_1|^2 - i|z_3|^2$

(i) $(z_2/\bar{z}_2 + \bar{z}_2/z_2)$

(j) $(z_1 + \bar{z}_2)(z_2 + \bar{z}_3)$

33. Soient $y = a + b \cdot i$, $z = c + d \cdot i$ deux nombres complexes. Vérifier les énoncés suivants en écrivant chaque expression en termes des a, b, c, d :

(a) $y\bar{z} - \bar{y}z$ est un imaginaire pur, c'est-à-dire sa partie réelle est nulle ;

(b) $y/z + \bar{y}/\bar{z}$ est un nombre réel, c'est-à-dire sa partie imaginaire est nulle ;

(c) $\overline{yz} = \bar{y} \cdot \bar{z}$.

34. Se convaincre que la propriété *(ix)* pour les deux nombres complexes y et z n'est rien d'autre que l'inégalité du triangle si la représentation cartésienne de ces nombres est utilisée.

35. Soient $z = r(\cos\theta + i\sin\theta)$ et $y = s(\cos\phi + i\sin\phi)$, montrer que :

(a) $1/z = (\cos\theta - i\sin\theta)/r$

(b) $\bar{z} = r(\cos\theta - i\sin\theta)$

(c) $zy = rs(\cos(\theta + \phi) + i\sin(\theta + \phi)$

(d) $z/y = r(\cos(\theta - \phi) + i\sin(\theta - \phi)/s$

(e) Formule de De Moivre [11] : $z^n = r^n(\cos(n\theta) + i\sin(n\theta))$. Suggestion : par induction !

36. Trouver les racines carrées et les racines cubiques de $1 + i$.

37. Donner la forme des n racines n-ièmes de l'unité, c'est-à-dire de $z = 1$, et vérifier que, pour $n = 4$, on a bien $u^4 = 1$ pour les quatre racines.

38. Montrer que la somme des n racines n-ièmes de l'unité égale à zéro. Suggestion : écrire $z = e^{2\pi i/n}$ et noter que les n racines n-ièmes sont données par $z_k = z^k, k = 0, 1, \ldots, n-1$. Utiliser alors la somme suivante pour conclure : si $s = 1 + x + x^2 + \cdots + x^{n-1}$, alors $s = (x^n - 1)/(x - 1)$ pour $x \neq 1$.

39. Utiliser la formule d'Euler pour démontrer que

(a) $\cos(2\theta) = \cos^2\theta - \sin^2\theta$;

(b) $\sin(2\theta) = 2\sin\theta\cos\theta$;

(c) $\sin^3\theta = \frac{3}{4}\sin\theta - \frac{1}{4}\sin 3\theta$.

11. Abraham de Moivre (1667–1754) est un mathématicien français. Il contribua à la géométrie analytique et écrivit un traité *Théorie du Hasard*, un ouvrage précurseur de la théorie des probabilités.

SOLUTIONS DE QUELQUES EXERCICES

30. (a) $2-3i$

(c) $3-i$

(e) $2i$

(g) $(-2-4a)+i(8-a)$; si a est un nombre réel, alors la partie réelle du nombre proposé est $(-2-4a)$ et sa partie imaginaire est $(8-a)$. Si, cependant, a possède une partie imaginaire, alors la partie réelle du nombre proposé sera $(-2-4\ \mathrm{Re}\ a+\mathrm{Im}\ a)$ et sa partie imaginaire $(8-\mathrm{Re}\ a-4\ \mathrm{Im}\ a)$.

31. (a) 2

(c) $-5+i\sqrt{3}$

(e) $2i(bc-ad)/(c^2+d^2)$

32. (a) $-2-i$

(c) -6

(e) $\sqrt{2}$

(g) $\frac{1}{5}$

(i) $\frac{6}{5}$

33. (a) $y\bar{z}-\bar{y}a=2i(cb-ad)$ est clairement un nombre imaginaire.

35. (a)
$$\frac{1}{z}=\frac{1}{r(\cos\theta+i\sin\theta)}=\frac{1}{r(\cos\theta+i\sin\theta)}\cdot\frac{\cos\theta-i\sin\theta}{\cos\theta-i\sin\theta}=\frac{1}{r}(\cos\theta-i\sin\theta).$$

(c)
$$\begin{aligned}zy&=rs(\cos\theta+i\sin\theta)(\cos\phi+i\sin\phi)\\&=rs\big((\cos\theta\cos\phi-\sin\theta\sin\phi)+i(\cos\theta\sin\phi+\sin\theta\cos\phi)\big)\\&=rs(\cos(\theta+\phi)+i\sin(\theta+\phi).\end{aligned}$$

36. En coordonnées polaires, le nombre $1+i$ s'écrit $\sqrt{2}e^{i\pi/4}$. Donc ses racines carrées sont $2^{1/4}e^{i\pi/8}$ et $2^{1/4}e^{9i\pi/8}$.

37. Les n racines n-ièmes de 1 sont $u_k=e^{2ik\pi/n}$ pour $k=0,1,\ldots,n-1$. Pour $n=4$, cette expression devient $u_0=1$, $u_1=e^{i\pi/2}=\cos\pi/2+i\sin\pi/2=i$ et, similairement $u_2=-1$ et $u_3=-i$. Clairement, pour ces quatre racines, on a bien $u_k^4=1$.