Chapitre 1

Théorie des ensembles – notions de base

1.1. Le langage des mathématiques

Les textes mathématiques utilisent une combinaison d'éléments du langage usuel (des noms, des verbes, des adjectifs, etc.) permettant de former des phrases et de rendre le discours compréhensible, et d'éléments spécifiques aux mathématiques, qui en rendent la lecture plus facile, du moins pour un public averti ! L'objectif de cette section est de présenter ces éléments de langage spécifiques aux mathématiques. Nous y reviendrons souvent dans les sections et chapitres suivants, ils sont présentés ici, un peu sèchement, à titre de référence.

1.1.1. Les symboles mathématiques.

En complément au vocabulaire ordinaire et aux termes mathématiques introduits dans des définitions, le texte mathématique utilise de nombreux *symboles mathématiques* qui permettent de raccourcir les énoncés. Voici les symboles les plus courants.

- **Les nombres et les ensembles de nombres.** Les symboles mathématiques les plus célèbres sont bien sûr les chiffres de 0 à 9, par combinaison des quels on représente les nombres usuels. Certains ensembles de nombres bien connus, que nous revisiterons dans la suite de ce cours, sont désignés par une lettre en double-fonte :

$\mathbb{N}$	Les nombres entiers naturels
$\mathbb{Z}$	Les nombres entiers relatifs
$\mathbb{Q}$	Les nombres rationnels
$\mathbb{R}$	Les nombres réels

$\mathbb{C}$	Les nombres complexes
$\mathbb{H}$	Les quaternions
$\mathbb{O}$	Les octonions

- **Les lettres.** On utilise souvent une lettre seule pour désigner un objet mathématique dans un énoncé. Il est bien sûr indispensable de préciser à quoi la lettre fait référence. L'usage du verbe être conjugué "Soit" est très courant. On dira par exemple

"Soit n un nombre entier naturel."

Cette phrase revient à dire : "Dans l'énoncé qui suit, on désignera par la variable n un nombre entier naturel quelconque". Les lettres majuscules désignent souvent des ensembles, et les lettres minuscules des éléments d'un ensemble, mais ce ne n'est pas une règle absolue. Souvent on manque de lettres dans l'alphabet latin, et on fait appel à l'alphabet grec. Les lettres grecques sont aussi parfois réservées à des fonctions précises, comme des *angles*. On donne ci-dessous l'alphabet grec ; certaines minuscules ou majuscules, ainsi que Omicron, sont identiques aux lettres de l'alphabet latin : on ne les utilise pas.

1	Alpha	α	A
2	Bêta	β	B
3	Gamma	γ	Γ
4	Delta	δ	Δ
5	Epsilon	ε	E
6	Zêta	ζ	Z
7	Êta	η	H
8	Thêta	θ	Θ

9	Iota	ι	I
10	Kappa	κ	K
11	Lambda	λ	Λ
12	Mu	μ	M
13	Nu	ν	N
14	Xi	ξ	Ξ
15	Omicron	o	O
16	Pi	π	Π

17	Rhô	ρ	P
18	Sigma	σ	Σ
19	Tau	τ	T
20	Upsilon	υ	Y
21	Phi	φ ou ϕ	Φ
22	Chi	χ	X
23	Psi	ψ	Ψ
24	Omega	ω	Ω

La lettre Aleph $\aleph$ de l'alphabet hébreu est utilisée pour désigner des cardinaux. Certaines lettres ont été attribuées à des nombres remarquables, notons en particulier :

π	$3,1415\cdots \in \mathbb{R}$	L'aire d'un disque de rayon 1
e	$2,71828\cdots \in \mathbb{R}$	Le nombre d'Euler $e = \sum_{n=0}^{\infty} 1/n!$
i	$i \in \mathbb{C}$ avec $i^2 = -1$	Parfois appelé *l'unité imaginaire*

Mentionnons la notation ressemblant à un 8 couché pour désigner l'infini. Ce n'est pas un nombre, mais il est très utile dans divers expressions que nous définirons. Le célèbre S allongé est utilisé pour désigner les intégrales :

∞	L'infini	Utilisé dans des notations : $[1, \infty[\subset \mathbb{R}$, ou encore $\sum_{n=0}^{\infty} 1/n!$, etc.
$\int$	L'intégrale	Par exemple dans l'expression $\int_0^1 t^2 dt$.

Enfin, on peut décorer les lettres de divers signes, comme par exemple f' pour la dérivée d'une fonction f. En voici une liste, avec la prononciation :

a'	a prime
a''	a seconde
a'''	a tierce

$\tilde{a}$	a tilde
$\check{a}$	a check
$\hat{a}$	a chapeau

$\bar{a}$	a barre
a_i	a indice i
a^i	a exposant i

▹ **Les opérations.** Elles permettent de décrire un objet mathématique à partir d'autres objets de même type, comme par exemple les opérations bien connues sur les nombres : somme, le produit, la division. Il y en beaucoup d'autres, qui peuvent porter sur toute sorte d'objets mathématiques, tel les nombres, les ensembles, les applications, etc. Une opération peut avoir comme argument un, deux, ou plusieurs objets. Voici une liste des opérations les plus connues (nous y reviendrons par la suite). Dans la première liste, on indique la notation usuelle pour deux objets dans la colonne 3, pour une famille d'objets indicés par $i \in I$ dans la colonne 4.

La somme	$+$	$a + b$	$\sum_{i \in I} a_i$
Le produit	$\times$ ou $\cdot$	$a \times b$ ou $a \cdot b$ ou ab	$\prod_{i \in I} a_i$
La réunion	$\cup$	$A \cup B$	$\bigcup_{i \in I} A_i$
L'intersection	$\cap$	$A \cap B$	$\bigcap_{i \in I} A_i$

Certaines opérations ne portent que sur deux objets :

La différence (de deux nombres)	$-$	$a - b$
La division, le quotient	: ou /	$a : b$ ou a/b ou $\frac{a}{b}$
La différence (de deux ensembles)	$\smallsetminus$	$A \smallsetminus B$
La composition (d'applications)	$\circ$	$f \circ g$ ou fg

D'autres opérations ne portent que sur un seul objet :

L'opposé (d'un nombre)	$-$	$-a$
L'inverse (d'un nombre)	$(-)^{-1}$ ou $1/(-)$	a^{-1} ou $1/a$ ou $\frac{1}{a}$
Le complémentaire (d'un sous-ensemble A de E)		$C_E A$ ou $E \smallsetminus A$

▹ **Les relations.** Elles décrivent un lien entre deux objets, une propriété partagée ou non, etc. Il y a de nombreux type de relations, les plus communes sont :

L'égalité	$=$	$a = b$	*a est égal à b*
Une relation d'équivalence	$\sim$	$a \sim b$	*a est équivalent à b*
Les relations d'ordre	$\leqslant$	$a \leqslant b$	*a est plus petit ou égal à b*
	$\geqslant$	$a \geqslant b$	*a est plus grand ou égal à b*
L'ordre strict	$<$	$a < b$	*a est strictement plus petit que b*
	$>$	$a > b$	*a est strictement plus grand que b*
L'appartenance	$\in$	$a \in A$	*a appartient à A*
L'inclusion	$\subset$	$A \subset B$	*A est inclus dans B*
L'inclusion stricte	$\subsetneq$	$A \subsetneq B$	*A est un strictement inclus dans B*

On a aussi les relations qui sont la négation de ces relations, que l'on note généralement par le même symbole barré : $a \neq b$, *a n'est pas égal à b*, et ainsi de suite : $\nsim$, $\nleqslant$, $\nless$, $\ngeqslant$, $\ngtr$, $\notin$, et $\not\subset$.

▹ **Les quantificateurs.** Quand on parle d'une propriété qui peut être remplie ou non par certains éléments d'un ensemble E donné, on s'intéresse souvent aux questions :

- Cette propriété est-elle vraie *pour tout* élément de E ?
- *Existe-t-il (au moins) un* élément de E qui vérifie cette propriété ?
- *Existe-t-il un unique* élément de E qui vérifie cette propriété ?

Les expressions *pour tout*, *il existe*, et *il existe un unique* sont appelées *quantificateurs*. On leur a attribué un symbole :

Quantificateurs existentiels	$\exists$	il existe
	$\exists!$	il existe un unique
Quantificateur universel	$\forall$	pour tout

Par exemple, l'expression

$$\forall n \in \mathbb{Z}\ ,\ \exists! m \in \mathbb{Z} \quad \text{avec } m + n = 0$$

se lira

Pour tout nombre entier relatif n, il existe un unique nombre entier relatif m avec $m + n = 0$.

Remarquons que l'usage des symboles $\exists$, $\exists!$, $\forall$ est réservé aux formules où l'on veut gagner de la place, mais ces symboles ne devraient pas être utilisés dans des phrases (si possible, on préfèrera la deuxième formulation dans l'exemple ci-dessus). Le symbole $\exists$ fait référence au E de *existe*, le symbole $\forall$ est un A inversé en référence à *alle*, le mot allemand pour *tout*.

▹ **Les flèches.** Les flèches simples sont utilisées pour désigner *des applications*, et les flèches doubles pour désigner *des connecteurs logiques (implications)*, comme indiqué ci-dessous.

Application	$\to$	$f : A \to B$	*f est une application de A dans B*, et
	$\mapsto$	$a \mapsto b$	*a est envoyé sur b*
Implication	$\Rightarrow$	$P \Rightarrow Q$	*P implique Q*, ou : *Q est nécessaire à P*.
	$\Leftrightarrow$	$P \Leftrightarrow Q$	*P et Q sont équivalents*, ou : *P si et seulement si Q*

Par exemple, on peut définir l'application f de $\mathbb{R}$ dans $\mathbb{R}$ qui envoie un nombre réel x sur le nombre réel x^2 par les notations suivantes :

$$f : \mathbb{R} \to \mathbb{R}\ ,\ \ x \mapsto x^2 \quad \text{ou aussi} \quad f : \mathbb{R} \to \mathbb{R}\ ,\ \ f(x) = x^2\ ,\ \forall x \in \mathbb{R}\ .$$

L'expression

Les nombres m et $n \in \mathbb{Z}$ sont de même parité $\Leftrightarrow$ 2 divise $m - n$.

signifie

Les nombres m et $n \in \mathbb{Z}$ sont de même parité si et seulement si 2 divise $m - n$.

On peut aussi l'exprimer en disant :

Les conditions suivantes sur m et $n \in \mathbb{Z}$ sont équivalentes :

(i) *m et n sont de même parité ;*

(ii) *2 divise $m - n$.*

▹ **Les délimiteurs.** Ce sont les paranthèses, les accolades, les crochets. On les utilise de nombreuses façons. Voici quelques exemples très courants :

$(\ )$	Pour spécifier l'ordre des opérations	$(a + b) \times c$
	Pour évaluer une application en un élément	$f(x)$
	Pour donner des matrices	$\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$
$\{\ \}$	Pour définir des ensembles	$\{a \in \mathbb{N} \,;\, a \geqslant 5\}$
	Pour spécifier des cas	Pour $x \in \mathbb{R}$, soit $\lvert x\rvert = \begin{cases} x & \text{si } x \geqslant 0, \\ -x & \text{si } x < 0. \end{cases}$
$[\ ]$	Pour définir des intervalles	$[a, b] \subset \mathbb{R}$, $]a, b] \subset \mathbb{R}$, etc.

▹ **Les noms abréges.** De nombreuses fonctions sont désignées par des abbréviations faisant référence à leur nom ; notons par example :

cos	Le cosinus
sin	Le sinus
tan	La tangente

arccos	L'arccosinus
arcsin	L' arcsinus
arctan	L'arctangente

exp	l'exponentielle
log	le logarithme (base 10)
ln	le logarithme naturel

La liste de symboles ci-dessus est loin d'être exhaustive, nous en rencontrerons bien d'autres !

1.1.2. Les énoncés mathématiques.

Les mathématiques visent à *définir* de façon rigoureuse certains objets (des nombres, des fonctions, des constructions géométriques, etc.), puis à les *étudier* en énonçant et démontrant leurs propriétés. Les motivations pour la définition et l'étude de ces objets viennent souvent des autres sciences, en particulier de la physique. Un texte mathématique s'articule donc autour d'énoncés de deux types, qui correspondent à ces deux objectifs :

- *Les définitions :* ce sont les énoncés qui permettent définir, de spécifier les objets mathématiques que l'on va étudier, en se basant sur d'autres objets déjà supposés connus.
- *Les propositions mathématiques :* ce sont les affirmations ou les assertions qui énoncent des propriétés des objets mathématiques en question. Par définition, une proposition mathématique doit être soit *vraie*, soit *fausse*. C'est ce qu'on appelle le principe du *tiers-exclu*. On dit souvent *proposition* au lieu de *proposition mathématique*.

Voici quelques exemples. Les énoncés suivants sont des définitions :

- Soient $a, b \in \mathbb{R}$ avec $a \leqslant b$. On note $[a, b]$ l'ensemble des nombres réels x avec $a \leqslant x \leqslant b$, et on l'appelle *l'intervalle fermé de a à b*.
- On dit qu'un nombre entier est *pair* s'il est divisible par 2.

Le premier énoncé donne une définition d'un sous-ensemble de $\mathbb{R}$, qui sera noté $[a, b]$, et lui donne le nom *intervalle fermé de a à b*. Le second énoncé définit sous quelle condition un nombre entier est dit *pair*. Les énoncés suivants sont des propositions mathématiques :

(a) *Le nombre entier* 4 *est pair.*

(b) $3 \in [2, 4]$.

(c) *Le nombre entier* 3 *est pair.*

(d) $5 \in [2, 4]$.

Les propositions mathématiques (a) et (b) sont vraies, alors que (c) et (d) sont fausses ! Pour décider si une assertion est une proposition mathématique, et pour pouvoir décider si elle est vraie ou fausse, il faut bien sûr avoir défini tous les objets et concepts apparaissant dans l'assertion. Par exemple, pour les assertions (a) et (c), il faut que la notion de nombre *pair* ait été définie. De même, les assertions (b) et (d) ont un sens seulement si l'intervalle $[2, 4]$ a été défini.

De nombreuses assertions portent sur plusieurs éléments d'un ensemble à la fois. Pour énoncer l'assertion, il est très utile de nommer une variable et préciser comment celle-ci peut varier. Voici un exemple :

Pour tout nombre naturel pair n, le nombre $n + 2$ *est pair.*

Notons que cette assertion fait appel au quantificateur universel "pour tout", et à la variable n, qui désigne un nombre naturel pair. Cette assertion est une proposition mathématique vraie, car on obtient une assertion vraie lorsque l'on remplace la variable n par chacune de ses valeurs possibles, c'est-à-dire par n'importe quel nombre naturel pair. L'assertion

Pour tout nombre entier n, le nombre $n + 2$ *est pair*

est fausse : par exemple 1 est nombre entier, mais $1 + 2 = 3$ n'est pas pair. Dans d'autres situations, une assertion peut porter sur l'existence d'un objet avec une certaine propriété :

Il existe un nombre réel y *avec* $y^2 = 2$.

Cette assertion est vraie. Ici, on fait appel à une variable $y \in \mathbb{R}$ pour pouvoir spécifier la propriété des nombres recherchés (ceux dont le carré est 2), et l'énoncé affirme qu'il existe au moins un tel nombre. La proposition mathématique

Il existe un unique nombre réel $y > 0$ *avec* $y^2 = 2$.

est aussi vraie : elle nous permet de définir $\sqrt{2}$ comme l'unique nombre réel positif vérifiant $(\sqrt{2})^2 = 2$.

Enfin, de nombreux énoncés font appels à la fois aux quantificateurs universel et existentiel. Par exemple, la proposition

Pour tout $x \in \mathbb{R}$ *avec* $x \geqslant 0$*, il existe un unique* $y \in \mathbb{R}$ *avec* $y \geqslant 0$ *et* $y^2 = x$

est vraie : elle affirme que tout nombre réel non négatif admet une racine non négative, et une seule. Il faut bien sûr faire très attention aux quantificateurs, et à l'ensemble des valeurs des variables. Par exemple, la proposition

Pour tout $x \in \mathbb{R}$, il existe $y \in \mathbb{R}$ avec $y^2 = x$.

est fausse : si le nombre x est négatif, il n'a aucune racine. De même, la proposition

Pour tout $x \in \mathbb{C}$, il existe un unique $y \in \mathbb{C}$ avec $y^2 = x$

est aussi fausse : un nombre complexe x admet effectivement toujours une racine, mais elle n'est pas unique si $x \neq 0$. Par contre, la proposition

Pour tout $x \in \mathbb{C}$, il existe $y \in \mathbb{C}$ avec $y^2 = x$

est vraie.

Ainsi, dans une proposition mathématique qui utilise une variable, il est **indispensable** de toujours bien préciser les quantificateurs et le domaine des valeurs possibles de la variable ; sans cela, ce n'est pas une proposition mathématique. Par exemple, l'assertion

Pour tout x, il existe y avec $y^2 = x$

n'est pas une proposition mathématique : comme on a pas précisé les valeurs possibles de x, y, ni précisé ce qu'est y^2 (est-ce le produit d'un nombre y avec lui-même, ou est-ce un produit dans un autre contexte ?), cet énoncé est trop imprécis pour pouvoir décider s'il est vrai ou faux.

Pour aider le lecteur à repérer le rôle des énoncés, les textes mathématiques sont très structurés : ils sont en général découpés en petits paragraphes introduits par un *intitulé*. L'intitulé précise la fonction du paragraphe, par exemple s'il vise à *définir* un objet ou une propriété d'un objet, à *énoncer* une proposition, à la *démontrer*, etc. Voici une liste des intitulés les plus courants :

- **Définition.** Le paragraphe qui suit introduit un *nouveau* concept mathématique, en n'utilisant que de notions déjà supposées connues, et lui donne un nom ou un qualificatif. Ce nom est en général mis en *italique* pour bien souligner que c'est lui qui est défini ici.
- **Théorème.** L'énoncé qui suit est une affirmation vraie. De plus, le résultat énoncé est considéré comme l'un des résultats majeur du texte.
- **Proposition.** L'énoncé qui suit est une affirmation vraie. Le résultat énoncé est considéré important, mais pas suffisamment pour être appelé "théorème". Ne pas confondre avec la notion de *proposition mathématique* discutée plus haut, qui peut être vraie ou fausse.
- **Corollaire.** L'énoncé qui suit est une affirmation vraie qui se déduit plus ou moins directement du résultat précédent.
- **Lemme.** L'énoncé qui suit est une affirmation vraie qui n'est pas retenue comme résultat majeur, mais qui peut être par exemple de nature technique, ou qui est une étape intermédiaire dans la preuve d'un résultat majeur. Un lemme peut malgré tout avoir une démonstration difficile, ou être célèbre !
- **Démonstration** ou **Preuve.** Annonce que le texte qui suit apporte la démonstration de l'affirmation précédente : l'auteur va s'efforcer de convaincre le lecteur que le résultat énoncé est vrai. Pour le lecteur, comprendre une démonstration nécessitera souvent un travail supplémentaire à la simple lecture du texte. La fin d'une démonstration est souvent marquée par un symbole, comme par exemple □.
- **Conjecture.** S'utilise pour une assertion que l'auteur pense être vraie (par exemple parce qu'il n'a pas trouvé de contre-exemple), mais pour laquelle une démonstration n'est pas connue.
- **Remarque.** Le texte qui suit vise en général à apporter des éclaircissements ou des variantes, à avertir le lecteur sur des pièges à éviter, etc.
- **Exemple.** Le texte qui suit sert à illustrer une définition ou un résultat en présentant ce que l'énoncé signifie dans une situation concrète, explicite.
- **Axiome.** Se dit d'une proposition qui est considérée comme indémontrable mais vraie, et qui sert de point de départ à la théorie que l'on développe.
- **Exercice.** Le texte qui suit soumet un problème à résoudre. En général, tout ce qui est nécessaire à la résolution a été présenté auparavant. Si l'exercice est difficile, l'auteur peut donner une aide ou un "tuyau" au lecteur : ce tuyau est alors précédé de l'intitulé **Indication.**
- **Notation.** Le texte qui suit introduit une façon de noter ou d'écrire un concept mathématique déjà défini.

Remarquons que les phrases énonçant un résultat ou une conjecture sont en général en *italique*, alors que les définitions, les remarques et les exemples ne le sont pas.

Une fois qu'ils ont fait l'objet d'une définition dédiée, les nouveaux concepts peuvent être utilisés dans la suite du texte sans rappels : c'est au lecteur de se souvenir de toutes les définitions introduites plus haut, de connaitre les résultats et les utilisations qui ont en été faites. C'est ainsi que le vocabulaire utilisé s'enrichit progressivement de termes au sens mathématique très précis, dont la définition est supposée connue, comme par exemple une *fonction continue*, un *polynôme irréductible*, etc. Plus on avance dans l'étude des mathématiques, plus le bagage de notions et résultats supposés connus est grand, et plus ceux-ci sont utilisés sans être rappelés.

Terminons par une remarque typographique : on ne commence jamais une phrase par un symbole mathématique, car le résultat est souvent peu lisible. Ainsi, on n'écrira pas

Considérons un nombre entier naturel pair n. $n + 2$ *est pair*

car ce n'est pas très lisible, mais, par exemple,

Considérons un nombre entier naturel pair n. Alors $n + 2$ *est pair.*

1.2. Les ensembles

Dans cette section, nous allons présenter la notion d'un *ensemble* et la notion *d'éléments appartenant à un ensemble*. Ces notions jouent un rôle fondamental : on peut considérer que les ensembles sont les objets à partir des quels toutes les mathématiques sont construites. Cependant, nous n'allons pas donner de définition d'un ensemble : nous considérerons que leur existence et la possibilité de les manipuler comme nous le ferons sont des axiomes à partir des quelles les mathématiques sont construites. La nécessité d'axiomatiser les ensembles, c'est-à-dire de donner une liste précise de postulats et d'axiomes à partir des quels on peut définir les ensembles qui nous intéressent, et formuler et démontrer des résultats à leur sujet, est apparue au 19ème siècle, et à donné naissance à une branche des mathématiques appelée *Théorie des Ensembles*, crée par Georg Cantor. Un ensemble d'axiomes offrant un cadre à la théorie des ensembles a été proposé au début du 20ème siècle par Ernst Zermelo et Adolf A. H. Fraenkel. Au milieu du 20ème siècle, Kurt Gödel a démontré ses célèbres *Théorèmes d'Incomplétude*, qui, ont révolutionné la théorie des ensembles. La théorie des ensembles fait aujourd'hui partie du domaine des mathématiques appelée *Logique*.

Dans ce cours, nous partirons de notre connaissance intuitive de la notion d'ensemble, sans entrer dans les détails de la théorie des ensembles, dont l'étude, très abstraite, est en général reportée à un niveau d'études correspondant au master.

1.2.1. Les ensembles et leurs éléments.

Comme annoncé plus haut, nous ne donnons pas de définition d'un *ensemble*, mais nous basons sur la connaissance intuitive que nous en avons. Disons :

> Un *ensemble* est une collection d'objets, appelés *éléments*, avec la propriété suivante : pour un objet donné, l'assertion que cet objet appartient à la collection est soit vraie, soit fausse.

Dans ce chapitre, nous noterons en général un ensemble par une lettre majuscule, par exemple A, et un élément de A par une lettre minuscule, par exemple a. Remarquons que l'on ne dit rien sur la nature de a, mais juste que c'est *un élément de* A. La seule chose qui importe, pour caractériser un ensemble A, est qu'il n'y a pas d'ambigüité sur ses éléments : si on se donne un objet a, on a soit que a appartient à A, soit il n'y appartient pas.

Notation 1.1. Pour noter l'appartenance d'un élément à un ensemble, on utilise le symbole "$\in$". Ainsi, la notation

$$a \in A$$

signifie *a appartient à* A, ou, de façon équivalente, *a est un élément de l'ensemble* A. Pour dire qu'on objet b n'appartient pas à un ensemble A, on utilise la notation $b \notin A$.

Exemples 1.2. **(a)** Un exemple très intuitif d'ensemble est celui d'un sac de billes A, dont les éléments sont les billes qu'il contient. On sera tous d'accord que si l'on pointe sur un objet quelconque, on pourra dire s'il s'agit d'une bille de ce sac, donc d'un élément de A, ou non.

(b) Un exemple fondamental est celui d'*ensemble vide* : c'est un ensemble qui ne contient aucun élément. On

peut y penser, en terme de l'exemple (a), comme d'un sac de billes vide. Remarquons que l'existence d'un ensemble vide est essentiellement un axiome de la théorie des ensembles.

Notation 1.3. Un ensemble peut être donné *en extension*, c'est-à-dire en donnant la liste de tous ses éléments. On dit aussi *énumérer* l'ensemble. La liste des éléments s'écrit alors entre accolades : par exemple, on peut définir l'ensemble A contenant comme éléments les nombres 1, 2, 3 et 4, et on utilise pour cela la notation

$$A = \{1, 2, 3, 4\} .$$

On peut aussi se représenter A sous la forme d'un sac de billes, contenant les quatres "billes" ou "points" appelés 1, 2, 3 et 4 ; les parenthèses $\{ \dots \}$ représentent alors le "sac" ou le conteneur.

Définition 1.4. Un ensemble qui contient un élément et un seul est appelé un *singleton*. Si a est l'unique élément d'un singleton A, on notera l'ensemble A en extension : $A = \{a\}$.

Attention, dans le cas d'un singleton $\{a\}$, il ne faut pas confondre a, ici un élément, et $\{a\}$, qui est l'ensemble contenant l'unique élément a. On a par contre $a \in \{a\}$.

Définition 1.5. Supposons donnés deux ensembles A et B.
(a) On dit que A est *inclu* dans B si tous les éléments de A sont aussi des éléments de B. On notera

$$A \subset B$$

l'assertion que A est inclu dans B. On dira aussi qu'

$$\textit{il y a une inclusion de } A \textit{ dans } B \textit{ ,}$$

ou, de façon équivalente, que

$$A \textit{ est un sous-ensemble de } B \textit{ .}$$

Si A contient au moins un élément qui n'appartient pas à B, alors A n'est pas inclu dans B, ce que l'on note

$$A \not\subset B .$$

(b) On dit que A et B sont *égaux* si on a une double inclusion $A \subset B$ et $B \subset A$. On notera

$$A = B$$

l'égalité de A et B. En d'autres termes, A et B sont égaux s'ils sont formés des mêmes éléments.

Notation 1.6. Si on veut préciser que A est un sous-ensemble de B qui n'est *pas égal* à B, on dit que l'on a une *inclusion stricte* de A dans B, et on le note $A \subsetneq B$.

Si B est un ensemble quelconque et si A est un ensemble vide, on a forcément $A \subset B$. En particulier, si A et B sont des ensembles vides, alors $A = B$. Ainsi, il existe un et un seul ensemble vide. Cela justifie la définition suivante.

Définition 1.7. On appelle *ensemble vide* l'unique ensemble ne contenant aucun élément, et on le note $\emptyset$.

Remarque 1.8. Soit A un ensemble, et B un sous-ensemble. On remarque que dans l'écriture en extension d'un ensemble, l'ordre dans le quel on écrit la liste les éléments n'a pas d'importance. Par exemple,

$$\{1, 2, 3, 4\} = \{2, 4, 1, 3\},$$

car ces deux ensembles ont les mêmes éléments, qui sont les nombres 1, 2, 3 et 4.

Exemples 1.9. (a) Si A est un ensemble quelconque, on a bien sûr $A \subset A$ et $A = A$.

Proposition 1.10. *Si A, B et C sont des ensembles avec $A \subset B$ et $B \subset C$, alors on a aussi $A \subset C$.*

Démonstration. Soit $x \in A$. Comme $A \subset B$, on en déduit $x \in B$. Comme $B \subset C$, on en déduit $x \in C$. Ainsi, pour tout $x \in A$, on a $x \in C$, donc $A \subset C$. □

Définition 1.11. Soit E un ensemble. L'ensemble de tous les sous-ensembles de E est un ensemble appelé *l'ensemble des parties de E*, et est noté $P(E)$.

Exemples 1.12.

Remarque 1.13. Par définition même de $P(E)$, dire que A est un sous-ensemble de E est équivalent à dire que A est un élément de $P(E)$. Les éléments de $P(E)$ sont donc eux-mêmes des ensembles. Attention donc aux notations :

- Pour A un sous-ensemble de E, on utilise les notations $A \subseteq E$ et $A \in P(E)$.
- Pour x un élément de E, on note $x \in E$ pour l'élément, et $\{x\} \subset E$ ou $\{x\} \in P(E)$ pour le sous-ensemble de E ne contenant que l'élément x.

Souvent, les éléments d'un ensemble E que l'on choisit pour former un sous-ensemble A de E sont nombreux, voire sont en nombre infinis ; c'est par exemple le cas si on veut parler du sous-ensemble de $\mathbb{N}$ contenant tous les entiers naturels pairs. Dans ce cas, il est alors impossible de donner l'ensemble A en extension (donc de

dresser la liste complète de ses éléments). On recourt alors à la notion de *propriété* d'un élément de E, et on dit que A est le sous-ensemble formé des éléments de E ayant cette propriété.

Définition 1.14. Soit E un ensemble, et soit $\mathcal{P}$ une assertion dépendant d'un paramètre $x \in E$. Notons $\mathcal{P}(x)$ cette assertion évaluée en x. On dira que $\mathcal{P}$ est *une propriété sur les éléments de* E si, pour chaque $x \in E$, l'assertion $\mathcal{P}(x)$ est une proposition au sens mathématique, donc est soit vraie, soit fausse (tiers-exclu). Dans ce cas, on dénotera par

$$\{x \in E \ ; \ \mathcal{P}(x)\}$$

le sous-ensemble de E formé des éléments $x \in E$ pour les quels $\mathcal{P}(x)$ est *vraie*.

Remarque 1.15. On remarque que la condition de tiers-exclu sur $\mathcal{P}$ nous garantit que le sous-ensemble

$$A = \{x \in E \ ; \ \mathcal{P}(x)\}$$

est bien-défini, c'est-à-dire que ses éléments ont été bien caractérisés : si $x \in E$, alors $x \in A$ si $\mathcal{P}(x)$ est vraie, et $x \notin A$ si $\mathcal{P}(x)$ est fausse. On ne donne pas la liste des éléments de A, mais une propriété qui caractérise ses éléments : on dit que A est donné *en compréhension* (par opposition à un ensemble donné *en extension*). Par exemple,

$$\{1, 2, 3, 4\} \quad \text{et} \quad \{n \in \mathbb{N} \ ; \ 1 \leqslant n \leqslant 4\}$$

sont deux notations pour le même sous-ensemble de $\mathbb{N}$: la première est *en extension*, la deuxième *en compréhension*.

Exemples 1.16. (a) Supposons donné un ensemble E et un sous-ensemble A. On considère la propriété $\mathcal{P}$ donnée, pour $x \in E$, par

$$\mathcal{P}(x) \ \text{ est l'assertion : } \ x \in A,$$

ce que l'on notera $\mathcal{P}(x) : (x \in A)$. Alors $\mathcal{P}$ est bien une propriété portant sur les éléments de E : pour $x \in E$, l'assertion $x \in A$ est soit vraie, soit fausse. On a bien sûr $A = \{x \in E \ ; \ \mathcal{P}(x)\}$. Évidemment, cette notation n'est pas très utile ici, il est plus simple d'écrire A que $\{x \in E \ ; \ x \in A\}$.

Remarque 1.17. Le paradoxe de Russel (1903).

Définition 1.18. Supposons donnés un ensemble E et deux propriétés $\mathcal{P}$ et $\mathcal{Q}$ portant sur les éléments de E.

(a) On dit que $\mathcal{P}$ *implique* $\mathcal{Q}$, ce que l'on note $\mathcal{P} \Rightarrow \mathcal{Q}$, si, pour tout $x \in E$ pour le quel $\mathcal{P}(x)$ est vraie, alors $\mathcal{Q}(x)$ est aussi vraie.

(b) On dit que $\mathcal{P}$ *est équivalente à* $\mathcal{Q}$, ce que l'on note $\mathcal{P} \Leftrightarrow \mathcal{Q}$, si d'une part $\mathcal{P}$ implique $\mathcal{Q}$ et d'autre part $\mathcal{Q}$ implique $\mathcal{P}$.

Remarque 1.19. Supposons donnés un ensemble E et deux propriétés $\mathcal{P}$ et $\mathcal{Q}$ portant sur les éléments de E. Alors $\mathcal{P} \Leftrightarrow \mathcal{Q}$ revient à dire que pour $x \in E$,

$$\textit{si } \mathcal{P}(x) \textit{ est vraie alors } \mathcal{Q}(x) \textit{ est vraie, et si } \mathcal{Q}(x) \textit{ est vraie alors } \mathcal{P}(x) \textit{ est vraie}$$

ce que l'on dit plus simplement de la façon suivante :

$$\mathcal{P}(x) \textit{ est vraie si et seulement si } \mathcal{Q}(x) \textit{ est vraie.}$$

La proposition suivante est simplement une reformulation de la Définition 1.18.

Proposition 1.20. *Supposons donnés un ensemble E et deux propriétés $\mathcal{P}$ et $\mathcal{Q}$ portant sur les éléments de E. Alors les conditions suivantes sur $\mathcal{P}$ et $\mathcal{Q}$ sont équivalentes :*

(a) *$\mathcal{P}$ implique $\mathcal{Q}$;*

(b) *On a une inclusion $\{x \in E \ ; \ \mathcal{P}(x)\} \subset \{x \in E \ ; \ \mathcal{Q}(x)\}$.*

Corollaire 1.21. *Supposons donnés un ensemble E et deux propriétés $\mathcal{P}$ et $\mathcal{Q}$ portant sur les éléments de E. Alors les conditions suivantes sur $\mathcal{P}$ et $\mathcal{Q}$ sont équivalentes :*

(a) *$\mathcal{P}$ est équivalente à $\mathcal{Q}$;*

(b) *On a une égalité $\{x \in E \ ; \ \mathcal{P}(x)\} = \{x \in E \ ; \ \mathcal{Q}(x)\}$.*

Démonstration. Cela suit de la Proposition 1.20, car l'égalité des ensembles correspond à la double inclusion, et l'équivalence de $\mathcal{P}$ et $\mathcal{Q}$ à la double implication $\mathcal{P} \Rightarrow \mathcal{Q}$ et $\mathcal{Q} \Rightarrow \mathcal{P}$. □

Exemples 1.22. **(a)** Sur les nombres réels, considérons les propriétés portant sur $x \in \mathbb{R}$ données par $\mathcal{P}(x)$: $(x \geqslant 1)$ et $\mathcal{Q}(x)$: $(x^2 \geqslant 1)$. Alors $\mathcal{P} \Rightarrow \mathcal{Q}$, ce qui correspond à l'inclusion

$$\{x \in \mathbb{R} \ ; \ x \geqslant 1\} \subset \{x \in \mathbb{R} \ ; \ x^2 \geqslant 1\} \, .$$

1.2.2. Opérations sur les ensembles.

Dans cette section, nous ne considérerons dans un premier temps que des opérations définies sur les sous-ensembles d'un ensemble donné E. Nous mentionnerons plus tard le cas général.

Définition 1.23. Soit E un ensemble, et soient A et B deux sous-ensembles de E.

(a) *La réunion de A et de B* est le sous-ensemble de E composé des éléments qui sont dans A **ou** dans B. La réunion de A et B est notée $A \cup B$, et se lit "A union B". Ainsi, on a

$$A \cup B = \{x \in E \ ; \ x \in A \ \textbf{ ou } \ x \in B\} .$$

(b) *L'intersection de A et de B* est le sous-ensemble de E composé des éléments qui sont dans A **et** dans B. L'intersection de A et B est notée $A \cap B$, et se lit "A inter B". Ainsi, on a

$$A \cap B = \{x \in E \ ; \ x \in A \ \textbf{ et } \ x \in B\} .$$

(c) *La différence de A et B* est le sous-ensemble de E composé des éléments qui sont dans A **et** qui ne sont **pas** dans B. La différence de A et B est notée $A \smallsetminus B$. Ainsi, on a

$$A \smallsetminus B = \{x \in E \ ; \ x \in A \ \textbf{ et } \ x \notin B\} .$$

(d) *Le complémentaire de A dans E* est l'ensemble des éléments de E qui ne sont pas dans A. On le notera souvent $C_E A$ ou $E \smallsetminus A$. Ainsi, on a

$$C_E A = E \smallsetminus A = \{x \in E \ ; \ x \notin A\} .$$

Remarque 1.24. Dans la définition ci-dessus, le rôle des mots **et / ou** en gras est essentiel. De plus, dans la définition de la réunion de A et de B, il faut bien prendre garde que le **ou** est *inclusif* (on dit aussi *non-exclusif*). Cela signifie que l'on accepte dans $A \cup B$ les éléments qui sont à la fois dans A et dans B. Autrement dit, on aura toujours l'inclusion

$$A \cap B \subset A \cup B .$$

Exemples 1.25.

Remarque 1.26. Dans la définition de la réunion et de l'intersection de A et B, l'ordre dans lequel A et B interviennent n'a pas d'importance. C'est-à-dire que $A \cup B = B \cup A$ et $A \cap B = B \cap A$. Il faut bien prendre

garde que, en revanche, pour la différence de A et B l'ordre est essentiel. En d'autres termes, $A \smallsetminus B$ et $B \smallsetminus A$ ne sont pas égaux en général, comme on l'a vu dans l'exemple 1.25.(a) ci-dessus. On le visualise bien à l'aide des diagrammes de Venn.

Remarque 1.27. Les diagrammes de Venn permettent de décrire par un schéma les relations entre les opérations d'une famille finie de sous-ensembles d'un ensemble E.

Proposition 1.28. *Soit E un ensemble. Alors, quelque soient les sous-ensembles A, B et C de E, on a les égalités suivantes :*

$A \cup (B \cup C) = (A \cup B) \cup C$	*la réunion est associative*
$A \cup B = B \cup A$	*la réunion est commutative*
$A \cup \emptyset = A$	*l'ensemble vide est neutre pour la réunion*
$A \cap (B \cap C) = (A \cap B) \cap C$	*l'intersection est associative*
$A \cap B = B \cap A$	*l'intersection est commutative*
$A \cap E = A$	*l'ensemble E est neutre pour l'intersection*
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	*distributivité*
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	
$E \smallsetminus (E \smallsetminus A) = A$	*règles pour le complémentaire*
$E \smallsetminus (A \cap B) = (E \smallsetminus A) \cup (E \smallsetminus B)$	
$E \smallsetminus (A \cup B) = (E \smallsetminus A) \cap (E \smallsetminus B)$	

Démonstration. La démonstration sera discutée en TD : c'est essentiellement les relations correspondantes entre les *connecteurs logiques* **et / ou**. Voir aussi la remarque suivante. □

Remarque 1.29. On peut visualiser très facilement les "règles de calcul" données par la Proposition 1.28 à l'aide d'un diagramme de Venn pour les trois sous-ensembles A, B et C de E :

Remarque 1.30. Remarquons que l'associativité de la réunion nous permet d'écrire $A \cup B \cup C$ sans que cela soit ambigu. Cette remarque vaut aussi pour l'intersection.

Lorsque E est un ensemble, et que A et B sont des sous-ensembles donnés par des propriétés $\mathcal{P}$ et $\mathcal{Q}$ portant sur les éléments de E, on peut former de nouvelles propriétés, qui correspondront aux sous-ensembles $A \cup B$, $A \cap B$ et $E \setminus A$.

Définition 1.31. Soit E un ensemble, et soient $\mathcal{P}$ et $\mathcal{Q}$ deux propriétés portant sur les éléments de E. On définit les propriétés suivantes, portant aussi sur les éléments de E.

(a) La propriété ($\mathcal{P}$ ou $\mathcal{Q}$), notée aussi $\mathcal{P} \vee \mathcal{Q}$:

pour $x \in E$, ($\mathcal{P}$ ou $\mathcal{Q}$)(x) est *vraie* si $\mathcal{P}(x)$ est vraie **ou** si $\mathcal{Q}(x)$ est vraie, et est fausse sinon.

(b) La propriété ($\mathcal{P}$ et $\mathcal{Q}$), notée aussi $\mathcal{P} \wedge \mathcal{Q}$:

pour $x \in E$, ($\mathcal{P}$ et $\mathcal{Q}$)(x) est *vraie* si $\mathcal{P}(x)$ est vraie **et** si $\mathcal{Q}(x)$ est vraie, et est fausse sinon.

(c) La propriété (non $\mathcal{P}$), notée aussi $\neg\mathcal{P}$:

pour $x \in E$, (non $\mathcal{P}$)(x) est *vraie* si $\mathcal{P}(x)$ est fausse, et est fausse si $\mathcal{P}(x)$ est vraie.

Remarque 1.32. Si E est un ensemble, et si $\mathcal{P}$ et $\mathcal{Q}$ sont deux propriétés portant sur les éléments de E, alors les définitions de ($\mathcal{P}$ ou $\mathcal{Q}$), ($\mathcal{P}$ et $\mathcal{Q}$) et (non $\mathcal{P}$) peuvent être exprimées de façon synthétique par les tableaux suivants, appelés *tables de vérité* :

Définition 1.33. Les termes – **ou**, **et**, **non** – (en symbole $\vee$, $\wedge$, $\neg$) qui permettent d'assembler des propriétés portant sur les éléments d'un ensemble pour en former de nouvelles, sont appelés *connecteurs* ou *connecteurs logiques*.

Remarque 1.34. On utilise aussi les connecteurs pour combiner des *propositions mathématiques* afin d'obtenir une nouvelle proposition, voir la Défininiton 1.39. L'implication $\Rightarrow$ et l'équivalence $\Leftrightarrow$ sont aussi des connecteurs logiques, qui peuvent s'exprimer en terme des connecteurs $\vee$, $\wedge$ et $\neg$, voir la Remarque 1.40.

La proposition suivante est une conséquence directe des définitions.

Proposition 1.35. *Soit E un ensemble, et soient $\mathcal{P}$ et $\mathcal{Q}$ deux propriétés portant sur les éléments de E. Alors on a les égalités suivantes entre sous-ensembles de E :*

$$\{x \in E \,;\, \mathcal{P}(x)\} \cup \{x \in E \,;\, \mathcal{Q}(x)\} = \{x \in E \,;\, (\mathcal{P} \text{ ou } \mathcal{Q})(x)\}$$
$$\{x \in E \,;\, \mathcal{P}(x)\} \cap \{x \in E \,;\, \mathcal{Q}(x)\} = \{x \in E \,;\, (\mathcal{P} \text{ et } \mathcal{Q})(x)\}$$
$$E \smallsetminus \{x \in E \,;\, \mathcal{P}(x)\} = \{x \in E \,;\, (\text{non } \mathcal{P})(x)\}\,.$$

Exemples 1.36. **(a)** On a l'égalité suivante entre sous-ensembles de $\mathbb{R}$:

$$\{x \in \mathbb{R} \,;\, x \leqslant -1\} \cup \{x \in \mathbb{R} \,;\, 1 \leqslant x\} = \{x \in \mathbb{R} \,;\, x \leqslant -1 \text{ ou } 1 \leqslant x\}\,.$$

On rappelle que le mot "ou" est non-exclusif : on admet aussi dans $\{x \in E \,;\, (\mathcal{P} \text{ ou } \mathcal{Q})(x)\}$ les éléments $x \in E$ pour les quels les propriétés $\mathcal{P}(x)$ et $\mathcal{Q}(x)$ sont toutes deux vraies. Par exemple,

$$\{x \in \mathbb{R} \,;\, x \leqslant 1\} \cup \{x \in \mathbb{R} \,;\, -1 \leqslant x\} = \{x \in \mathbb{R} \,;\, x \leqslant 1 \text{ ou } -1 \leqslant x\} = \mathbb{R}\,.$$

(b) On a l'égalité suivante entre sous-ensembles de $\mathbb{R}$:

$$\{x \in \mathbb{R} \,;\, -1 \leqslant x\} \cap \{x \in \mathbb{R} \,;\, x \leqslant 1\} = \{x \in \mathbb{R} \,;\, -1 \leqslant x \text{ et } x \leqslant 1\}$$

Remarquons que si l'on pose $\mathcal{P}(x) : (-1 \leqslant x)$ et $\mathcal{Q}(x) : (x \leqslant 1)$, la condition $(\mathcal{P} \text{ et } \mathcal{Q})$ est donnée par

$$(\mathcal{P} \text{ et } \mathcal{Q})(x) : (-1 \leqslant x \text{ et } x \leqslant 1)$$

que l'on peut écrire aussi $(-1 \leqslant x \leqslant 1)$. Dans cette propriété, "et" a disparu ; mais bien sûr, l'écriture $(-1 \leqslant x \leqslant 1)$ résume deux conditions devant être remplies, $(-1 \leqslant x)$ **et** $(x \leqslant 1)$. On peut donc écrire plus simplement, si l'on veut,

$$\{x \in \mathbb{R} \,;\, -1 \leqslant x\} \cap \{x \in \mathbb{R} \,;\, x \leqslant -1\} = \{x \in \mathbb{R} \,;\, -1 \leqslant x \leqslant 1\}\,.$$

(c) On a l'égalité suivante entre sous-ensembles de $\mathbb{R}$:

$$\mathbb{R} \smallsetminus \{x \in \mathbb{R} \,;\, x \leqslant 1\} = \{x \in \mathbb{R} \,;\, x \nleqslant 1\}\,.$$

Dans cet exemple, la propriété est $\mathcal{P}(x) : (x \leqslant 1)$, et donc $(\text{non } \mathcal{P})$ est donnée par $(\text{non } \mathcal{P})(x) : (x \nleqslant 1)$. On a aussi une autre notation pour exprimer $(x \nleqslant 1)$, à savoir $(x > 1)$, où la négation n'est plus apparente. Néanmoins, on peut écrire

$$\mathbb{R} \smallsetminus \{x \in \mathbb{R} \,;\, x \leqslant 1\} = \{x \in \mathbb{R} \,;\, x > 1\}\,.$$

Nous avons donc vu que pour les sous-ensembles d'un ensemble E donnés en compréhension, la réunion, l'intersection, et le complémentaire correspondent aux connecteurs – **ou**, **et**, **non** – respectivement. La proposition suivante est simplement une autre formulation de la Proposition 1.28. Ces règles sont très utiles pour manipuler les propriétés ; les deux dernières du tableau sont appelées *Lois de Morgan*.

Proposition 1.37. *Soit E un ensemble, et soient $\mathcal{P}$, $\mathcal{Q}$ et $\mathcal{R}$ trois propriétés portant sur les éléments de E. Alors on a les équivalences suivantes entre propriétés portant sur les éléments de E :*

$\mathcal{P}$ ou $(\mathcal{Q}$ ou $\mathcal{R}) \Leftrightarrow (\mathcal{P}$ ou $\mathcal{Q})$ ou $\mathcal{R}$	*associativité de* **ou**
$\mathcal{P}$ ou $\mathcal{Q} \Leftrightarrow \mathcal{Q}$ ou $\mathcal{P}$	*commutativité de* **ou**
$\mathcal{P}$ et $(\mathcal{Q}$ et $\mathcal{R}) \Leftrightarrow (\mathcal{P}$ et $\mathcal{Q})$ et $\mathcal{R}$	*associativité de* **et**
$\mathcal{P}$ et $\mathcal{Q} \Leftrightarrow \mathcal{Q}$ et $\mathcal{P}$	*commutativité de* **et**
$\mathcal{P}$ et $(\mathcal{Q}$ ou $\mathcal{R}) \Leftrightarrow (\mathcal{P}$ et $\mathcal{Q})$ ou $(\mathcal{P}$ et $\mathcal{R})$	*distributivité*
$\mathcal{P}$ ou $(\mathcal{Q}$ et $\mathcal{R}) \Leftrightarrow (\mathcal{P}$ ou $\mathcal{Q})$ et $(\mathcal{P}$ ou $\mathcal{R})$	
non $($non $\mathcal{P}) \Leftrightarrow \mathcal{P}$	*règles pour la négation*
non $(\mathcal{P}$ et $\mathcal{Q}) \Leftrightarrow ($non $\mathcal{P})$ ou $($non $\mathcal{Q})$	
non $(\mathcal{P}$ ou $\mathcal{Q}) =$ (non $\mathcal{P}$) et (non $\mathcal{Q}$)	

Démonstration. On peut démontrer ces équivalences en montrant que les deux propriétés dont on affirme l'équivalence ont les mêmes tables de vérité. Nous laissons ces vérifications comme exercice, ne faisant ici que le cas de la première règle de distributivité :

□

Exemples 1.38. **(a)** Les règles énoncées dans la Proposition 1.37 correspondent tout-à-fait au règles usuelles de logique du langage commun, sauf qu'ici, on est plus rigoureux et on place des parenthèses, qui indiquent l'ordre dans le quel assembler deux propositions en une seule. En français, elles sont remplacées par l'usage d'une virgule : être *rouge, et rond ou carré*, c'est pareil qu'être *rouge et rond, ou rouge et carré*.

(b) Considérons les propriétés suivantes portant sur $n \in \mathbb{N}$:

$$\mathcal{P}(n) : (n \leqslant 10), \qquad \mathcal{Q}(n) : (2|n), \qquad \mathcal{R}(n) : (3|n).$$

On verifie facilement que la propriété $\big(\mathcal{P}$ et $(\mathcal{Q}$ ou $\mathcal{R})\big)$ est équivalente à la propriété $\big((\mathcal{P}$ et $\mathcal{Q})$ ou $(\mathcal{P}$ et $\mathcal{R})\big)$: elles définissent toutes deux les sous-ensemble suivant de $\mathbb{N}$:

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

Nous avons defini plus haut les connecteurs logiques – **et**, **ou**, **non** – qui permettent de formuler les nouvelles propriétés $(\mathcal{P}$ et $\mathcal{Q})$, $(\mathcal{P}$ ou $\mathcal{Q})$ et (non $\mathcal{P}$) à partir de propriétés $\mathcal{P}$ et $\mathcal{Q}$ portant sur les éléments d'un ensemble E. Nous pouvons aussi définir ces mêmes connecteurs pour les *propositions mathématiques*, c'est-à-dire en reprenant simplement les mêmes valeurs de vérité, comme données dans les tables de vérités

de la Remarque 1.32. L'implication est aussi un connecteur logique entre propositions mathématiques : on la note $(\mathcal{P} \Rightarrow \mathcal{Q})$, que l'on lit $\mathcal{P}$ implique $\mathcal{Q}$. On fera le lien avec la Définition 1.18 après avoir introduit les quantificateurs, voir la Remarque 1.46.

Définition 1.39. Si $\mathcal{P}$ et $\mathcal{Q}$ sont des propositions mathématiques, on définit les propositions mathématiques $(\mathcal{P}$ ou $\mathcal{Q})$, $(\mathcal{P}$ et $\mathcal{Q})$, (non $\mathcal{P}$) et $(\mathcal{P} \Rightarrow \mathcal{Q})$ par les tables de vérité suivantes.

$\mathcal{P}$	$\mathcal{Q}$	$(\mathcal{P}$ ou $\mathcal{Q})$
V	V	V
V	F	V
F	V	V
F	F	F

$\mathcal{P}$	$\mathcal{Q}$	$(\mathcal{P}$ et $\mathcal{Q})$
V	V	V
V	F	F
F	V	F
F	F	F

$\mathcal{P}$	(non $\mathcal{P}$)
V	F
F	V

$\mathcal{P}$	$\mathcal{Q}$	$(\mathcal{P} \Rightarrow \mathcal{Q})$
V	V	V
V	F	F
F	V	V
F	F	V

On définit aussi *l'équivalence de $\mathcal{P}$ et $\mathcal{Q}$* comme la double implication

$$\big((\mathcal{P} \Rightarrow \mathcal{Q}) \text{ et } (\mathcal{Q} \Rightarrow \mathcal{P})\big), \quad \text{que l'on note } (\mathcal{P} \Leftrightarrow \mathcal{Q}).$$

Remarque 1.40. On constate que la proposition $(\mathcal{P} \Rightarrow \mathcal{Q})$ et la proposition $\big((\text{non}\,\mathcal{P})\,\text{ou}\,\mathcal{Q}\big)$ ont les mêmes tables de vérité. On peut donc remplacer l'une par l'autre.

Exemples 1.41. La table de vérité de $(\mathcal{P} \Leftrightarrow \mathcal{Q})$:

Exemples 1.42.

Puisque les connecteurs ont été définis pour les propriétés et les propositions par les mêmes tables de vérité, la proposition suivante suit immédiatement de la Proposition 1.37.

Proposition 1.43. *Soient $\mathcal{P}$, $\mathcal{Q}$ et $\mathcal{R}$ des* propositions mathématiques. *Alors toutes les équivalences données dans la Proposition 1.37 sont vraies.*

Nous définissons maintenant les quantificateurs universel et existentiel, déjà rencontré dans la Section 1.1 ci-dessus et en TD. Si E est un ensemble et $\mathcal{P}$ est une propriété portant sur les éléments $x \in E$, les quantificateurs transforment cette propriété en une *proposition mathématique* donc une assertion mathématique *soit vraie, soit fausse* : sa valeur de vérité ne dépend plus de la variable $x \in E$.

Définition 1.44. Soit E un ensemble, et $\mathcal{P}$ une propriété portant sur les éléments de E.

(a) La proposition

$$\textit{Pour tout } x \in E\textit{, l'assertion } \mathcal{P}(x) \textit{ est vraie}$$

est notée $\big(\forall x \in E\,,\ \mathcal{P}(x)\big)$ en symboles mathématiques. Cette proposition est vraie si $E = \{x \in E\ ;\ \mathcal{P}(x)\}$, et est fausse si $E \neq \{x \in E\ ;\ \mathcal{P}(x)\}$. Le terme *pour tout*, correspondant au symbole $\forall$, est appelé *quantificateur universel*.

(b) La proposition

$$\textit{Il existe } x \in E \textit{ pour lequel l'assertion } \mathcal{P}(x) \textit{ est vraie}$$

est notée $\big(\exists x \in E\,,\ \mathcal{P}(x)\big)$ en symboles mathématiques. Cette proposition est vraie si $\{x \in E\ ;\ \mathcal{P}(x)\} \neq \emptyset$, et est fausse si $\{x \in E\ ;\ \mathcal{P}(x)\} = \emptyset$. Le terme *il existe*, correspondant au symbole $\exists$, est appelé *quantificateur existentiel*.

Exemples 1.45.

Remarque 1.46. Soit E un ensemble, et $\mathcal{P}$ et $\mathcal{Q}$ des propriétés portant sur les éléments de E. La définition de $\mathcal{P} \Rightarrow \mathcal{Q}$ a été donnée en 1.18 : en terme des notations introduites ci-dessus, c'est la proposition

$$\Big(\forall x \in E\,,\ \big(\mathcal{P}(x) \Rightarrow \mathcal{Q}(x)\big)\Big)\,.$$

On remarque que $\mathcal{P} \Rightarrow \mathcal{Q}$ n'est plus une propriété portant sur les éléments de E, mais bien une proposition mathématique, en raison du quantificateur. Avec l'aide de la Remarque 1.40, on peut aussi la formuler

$$\Big(\forall x \in E\,,\ \big((\text{non } P) \text{ ou } \mathcal{Q}\big)(x)\Big)\,. \tag{1.47}$$

Posons $A = \{x \in E\ ;\ \mathcal{P}(x)\}$ et $B = \{x \in E\ ;\ \mathcal{Q}(x)\}$. Comme la propriété $\big((\text{non } P) \text{ ou } \mathcal{Q}\big)$ décrit les éléments de $(E \smallsetminus A) \cup B$, l'expression (1.47) signifie simplement

$$E \subset (E \smallsetminus A) \cup B\,.$$

ou, puisque $E \supset (E \smallsetminus A) \cup B$ est forcément vrai,

$$E = (E \smallsetminus A) \cup B\,.$$

On se souvient (voir 1.20) que la proposition $\mathcal{P} \Rightarrow \mathcal{Q}$ correspond précisément à $A \subset B$. En résumé, pour les propriétés $\mathcal{P}$ et $\mathcal{Q}$, l'équivalence entre les propositions $\mathcal{P} \Rightarrow \mathcal{Q}$ et $\Big(\forall x \in E\,,\ \big((\text{non } P) \text{ ou } \mathcal{Q}\big)(x)\Big)$ correspond à l'équivalence

$$A \subset B \quad \Leftrightarrow \quad E = (E \smallsetminus A) \cup B\,.$$

Remarque 1.48. Attention, lorsque l'on utilise les quantificateurs pour une variable x, il faut *toujours* précisez l'ensemble dans lequel x varie. Par exemple, l'assertion

$$\textit{Pour tout } x\textit{, il existe } y \textit{ avec } xy = 1$$

n'est pas une proposition mathématique ; l'assertion

$$\textit{Pour tout } x \in \mathbb{Q} \smallsetminus \{0\}\textit{, il existe } y \in \mathbb{Q} \textit{ avec } xy = 1$$

en est une.

Il est *très important* de savoir manipuler correctement les quantificateurs, et de comprendre la façon dont ils interagissent avec les connecteurs. Commençons par la négation.

Proposition 1.49. *Soit E un ensemble, et $\mathcal{P}$ une propriété portant sur les éléments de E. Alors on a les équivalences suivantes entre propositions :*

(a) *La négation de la proposition*

$$\text{Pour tout } x \in E, \mathcal{P}(x) \text{ est vraie}$$

est équivalente à la proposition

$$\text{Il existe } x \in E \text{ pour lequel } \mathcal{P}(x) \text{ est fausse.}$$

(b) *La négation de la proposition*

$$\text{Il existe } x \in E \text{ pour lequel } \mathcal{P}(x) \text{ est vraie}$$

est équivalente à la proposition

$$\text{Pour tout } x \in E, \mathcal{P}(x) \text{ est fausse.}$$

On peut résumer ces règles à l'aide des formules suivantes :

$$\boxed{\text{non}\left(\forall x \in E\,,\ \mathcal{P}(x)\right) \quad \Leftrightarrow \quad \left(\exists x \in E\,,\ \text{non}\,\mathcal{P}(x)\right)}$$

$$\boxed{\text{non}\left(\exists x \in E\,,\ \mathcal{P}(x)\right) \quad \Leftrightarrow \quad \left(\forall x \in E\,,\ \text{non}\,\mathcal{P}(x)\right)}$$

Démonstration. Commençons par (a), et posons $A = \{x \in E\ ;\ \mathcal{P}(x)\}$. Rappelons que les propositions

$$\left(\forall x \in E\,,\ \mathcal{P}(x)\right) \quad \text{et} \quad E = A$$

sont équivalentes par définition, donc leur négations

$$\text{non}\left(\forall x \in E\,,\ \mathcal{P}(x)\right) \quad \text{et} \quad E \neq A$$

sont aussi équivalentes. Or $A \subset E$, donc $E \neq A$ est équivalent à $E \smallsetminus A \neq \emptyset$. D'autre part, on a

$$E \smallsetminus A = \{x \in E\,,\ \text{non}\,\mathcal{P}(x)\}\,.$$

Donc $E \smallsetminus A \neq \emptyset$ peut s'écrire aussi $\{x \in E\ ;\ \text{non}\,\mathcal{P}(x)\} \neq \emptyset$. Cette dernière proposition est équivalente à la proposition $\left(\exists x \in E\,,\ \text{non}\,\mathcal{P}(x)\right)$. Ceci démontre (a).
La preuve de (b) est similaire :

□

Exemples 1.50. **(a)** Les règles données par la Proposition 1.49 sont très intuitives. Par exemple, la négation de

Toutes *les billes de ce sac sont* **rouges**

s'exprime par

Au moins une des billes de ce sac n'est pas rouge,

ce que nous dirons, en jargon mathématique :

Il existe *une bille de ce sac qui n'est* **pas rouge**.

Remarque 1.51. De nombreuses propositions contiennent plusieurs variables et quantificateurs : l'ordre dans le quel ils apparaissent est alors important, car la valeur de vérité de la proposition en dépend ! Pour ne pas s'embrouiller, on peut commencer par bien identifier chaque variable et la propriété dont la valeur dépend de cette variable, et placer des parenthèses correctement. Prenons un exemple :

$$\textit{Pour tout } x \in \mathbb{R}\textit{, il existe } y \in \mathbb{R} \textit{ avec } y > x. \tag{1.52}$$

Définissons une propriété $\mathcal{P}$ portant sur les éléments $x \in \mathbb{R}$ par

$$\mathcal{P}(x) : (\exists y \in \mathbb{R}\ ,\ y > x)\,.$$

On remarque que la variable y est utilisée pour définir $\mathcal{P}(x)$. On peut aussi définir un propriété $\mathcal{Q}_x$ portant sur les éléments $y \in \mathbb{R}$, et dépendant d'un $x \in \mathbb{R}$, par $\mathcal{Q}_x(y) : (y > x)$. On peut donc exprimer $\mathcal{P}(x)$ par

$$\mathcal{P}(x) : \big(\exists y \in \mathbb{R}\ ,\ \mathcal{Q}_x(y)\big)\,.$$

La proposition donnée en (1.52) s'écrit en formule $\big(\forall x \in \mathbb{R}\ ,\ \mathcal{P}(x)\big)$, ou ainsi, si on remplace $\mathcal{P}(x)$ par sa formule :

$$\Big(\forall x \in \mathbb{R}\ ,\ \big(\exists y \in \mathbb{R}\ ,\ \mathcal{Q}_x(y)\big)\Big)\,. \tag{1.53}$$

Cette proposition est vraie (il suffit de trouver pour chaque x un tel y, et on peut prendre $y = x + 1$). Si on inverse l'ordre des variables et quantificateurs, on obtient :

$$\textit{Il existe } y \in \mathbb{R}\textit{, tel que pour tout } x \in \mathbb{R}\textit{, on a } y > x.$$

Cette proposition est fausse : elle affirme qu'il existe un nombre réel y plus grand que tous les autres réels. Elle est donc clairement non-équivalente à (1.52).

Remarque 1.54. Dans la remarque précédente, on a vu l'importance de l'ordre des variables et de leurs quantificateurs. Pour éviter toute confusion, il est utile d'écrire une proposition du type (1.52) sous la forme (1.53), en identifiant clairement les *propriétés* et en plaçant correctement les *parenthèses*. Par exemple, essayons de formuler la négation de la proposition (1.52). Écrivons-la en formule comme en (1.53), puis appliquons deux fois la Proposition 1.49 pour former la négation en présence de quantificateurs : une première fois pour

reformuler non $\big(\forall x \in \mathbb{R}\,,\ \mathcal{P}(x)\big)$, une seconde fois pour reformuler non $\big(\exists y \in \mathbb{R}\,,\ Q_x(y)\big)$. Notez bien le rôle des parenthèses :

$$\begin{aligned}
&\text{non}\Big(\forall x \in \mathbb{R}\,,\ \big(\exists y \in \mathbb{R}\,,\ Q_x(y)\big)\Big)\\
&\Leftrightarrow \Big(\exists x \in \mathbb{R}\,,\ \text{non}\,\big(\exists y \in \mathbb{R}\,,\ Q_x(y)\big)\Big)\\
&\Leftrightarrow \Big(\exists x \in \mathbb{R}\,,\ \big(\forall y \in \mathbb{R}\,,\ \text{non}\,Q_x(y)\big)\Big)\\
&\Leftrightarrow \Big(\exists x \in \mathbb{R}\,,\ \big(\forall y \in \mathbb{R}\,,\ y \leqslant x\big)\Big).
\end{aligned}$$

Dans la dernière équivalence, on a simplement utilisé que la négation de $y > x$ est $y \leqslant x$. En traduisant la dernière formule en français, on trouve que la négation de (1.52) est

Il existe $x \in \mathbb{R}$, tel que pour tout $y \in \mathbb{R}$, on a $y \leqslant x$.

Notons que puisque (1.52) était vraie, sa négation est fausse.

Exemples 1.55.

La proposition suivante énonce les relations existant entre les quantificateurs et les connecteurs **ou**, **et**.

Proposition 1.56. *Soit E un ensemble, et soient $\mathcal{P}$ et Q des propriétés portant sur les éléments $x \in E$. Alors on a les implications et équivalences suivantes :*

$\big(\exists x \in E\,,\ (\mathcal{P}\ \text{ou}\ Q)(x)\big)$	$\Leftrightarrow$	$\big(\exists x \in E\,,\ \mathcal{P}(x)\big)\ \text{ou}\ \big(\exists x \in E\,,\ Q(x)\big)$
$\big(\forall x \in E\,,\ (\mathcal{P}\ \text{ou}\ Q)(x)\big)$	$\Leftarrow$	$\big(\forall x \in E\,,\ \mathcal{P}(x)\big)\ \text{ou}\ \big(\forall x \in E\,,\ Q(x)\big)$
$\big(\forall x \in E\,,\ (\mathcal{P}\ \text{et}\ Q)(x)\big)$	$\Leftrightarrow$	$\big(\forall x \in E\,,\ \mathcal{P}(x)\big)\ \text{et}\ \big(\forall x \in E\,,\ Q(x)\big)$
$\big(\exists x \in E\,,\ (\mathcal{P}\ \text{et}\ Q)(x)\big)$	$\Rightarrow$	$\big(\exists x \in E\,,\ \mathcal{P}(x)\big)\ \text{et}\ \big(\exists x \in E\,,\ Q(x)\big)$

Démonstration. On se convainc facilement de ces équivalences on considérant les sous-ensembles définis par ces propriétés. Posons $A = \{x\ ;\ \mathcal{P}(x)\}$ et $B = \{x\ ;\ Q(x)\}$. Alors, en reprenant les définitions données en 1.44, on constate que la première équivalence donnée ci-dessus correspond à

$$\big(A \cup B \neq \emptyset\big) \Leftrightarrow \big((A \neq \emptyset)\,\text{ou}\,(B \neq \emptyset)\big)$$

qui est évident. Il en va de même des autres implications. □

Remarque 1.57. Attention, dans le tableau ci-dessus, si l'on a indiqué seulement $\Leftarrow$, c'est que l'implication $\Rightarrow$ est fausse en général, et vice-versa. On note en particulier les deux équivalences, que l'on peut formuler ainsi : on peut "distribuer" $\exists$ sur **ou**, et on peut "distribuer" $\forall$ sur **et**.

Exemples 1.58. Remarquons que les règles de la Propositions 1.56 sont intuitives : prenons un exemple. Soit E un sac de billes, et pour $x \in E$, considérons les propriétés

$$\mathcal{P}(x) : (x \text{ est rouge})$$
$$\mathcal{Q}(x) : (x \text{ est en bois}).$$

Alors $\big((\forall x \in E,\ \mathcal{P}(x) \text{ ou } (\forall x \in E,\ \mathcal{Q}(x)\big)$ signifie

Toutes les billes du sac sont rouges, ou toutes les billes du sac sont en bois

et implique bien que $\big(\forall x \in E,\ \mathcal{P}(x) \text{ ou } \mathcal{Q}(x)\big)$, qui signifie

Toutes les billes du sac sont soit rouges, soit en bois (ou les deux).

1.2.3. Types de démonstrations.

Les valeurs de vérités des propositions composées des connecteurs "**non**" et "$\Rightarrow$", comme données dans la Définition 1.39, justifient différents *types de raisonnement* ou *types de démonstration*, sur lesquels nous reviendrons souvent dans ce cours, et qui sont utilisés très fréquemment en mathématiques. Voici ces principaux types de démonstrations :

- **La déduction.** Ce type de raisonnement se base sur le résultat suivant : supposons données deux propositions mathématiques $\mathcal{P}$ et $\mathcal{Q}$. L'affirmation suivante est vraie :

  Si $\mathcal{P}$ est vraie **et** *si $(\mathcal{P} \Rightarrow \mathcal{Q})$ est vraie, alors $\mathcal{Q}$ est vraie.*

  Cela suit directement de la table de vérité de $(\mathcal{P} \Rightarrow \mathcal{Q})$. Remarquons qu'on itère souvent la déduction : si $\mathcal{P}$ est vraie, et si $(\mathcal{P} \Rightarrow \mathcal{Q})$ et $(\mathcal{Q} \Rightarrow \mathcal{R})$ sont vraies, alors $\mathcal{R}$ est vraie, etc.

- **La démonstration par contraposée.** Ce type de raisonnement se base sur le résultat suivant : supposons données deux propositions mathématiques $\mathcal{P}$ et $\mathcal{Q}$. L'affirmation suivante est vraie :

  La proposition $(\mathcal{P} \Rightarrow \mathcal{Q})$ et la proposition $\big((\text{non}\,\mathcal{Q}) \Rightarrow (\text{non}\,\mathcal{P})\big)$ sont équivalentes.

  On la vérifie facilement avec la table de vérité des propositions $(\mathcal{P} \Rightarrow \mathcal{Q})$ et $\big((\text{non}\,\mathcal{Q}) \Rightarrow (\text{non}\,\mathcal{P})\big)$.

▹ **La démonstration par l'absurde.** Ce type de raisonnement se base sur le résultat suivant : supposons données deux propositions mathématiques $\mathcal{P}$ et $\mathcal{Q}$. L'affirmation suivante est vraie :

$$\textit{Si } \big((\text{non}\,\mathcal{P}) \Rightarrow \mathcal{Q}\big) \textit{ est vraie } \textbf{et } \textit{si } \mathcal{Q} \textit{ est fausse, alors } \mathcal{P} \textit{ est vraie.}$$

On la vérifie facilement avec la table de vérité de la proposition $\big((\text{non}\,\mathcal{P}) \Rightarrow \mathcal{Q}\big)$.

▹ **La démonstration par cas (ou disjonction).** Soit E un ensemble, et $\mathcal{P}$ une propriété portant sur les éléments de E. Supposons que A et B sont des sous-ensemles de E avec $E = A \cup B$. Montrer que $\mathcal{P}(x)$ est vraie pour tous les $x \in E$ est équivalent à montrer que $\mathcal{P}(x)$ est vraie pour tous les $x \in A$ et que $\mathcal{P}(x)$ est vraie pour tous les $x \in B$: on distingue les cas $x \in A$ et $x \in B$. On prend souvent $B = E \setminus A$, mais pas nécessairement. En formule, cela donne

$$\big(\forall x \in A \cup B,\ \mathcal{P}(x)\big) \quad \Leftrightarrow \quad \Big(\big(\forall x \in A,\ \mathcal{P}(x)\big) \text{ et } \big(\forall x \in B,\ \mathcal{P}(x)\big)\Big).$$

- **La démonstration par un exemple.** Soit E un ensemble, et $\mathcal{P}$ une propriété portant sur les éléments de E. Si on veut démontrer la proposition $\big(\exists x \in E,\ \mathcal{P}(x)\big)$, il suffit de trouver un élément $a \in E$ pour lequel $\mathcal{P}(a)$ est vraie. Un tel a est un *exemple* d'élément de E satisfaisant à $a \in \{x \in E\,;\, \mathcal{P}(x)\}$; en particulier, $\{x \in E\,;\, \mathcal{P}(x)\} \neq \emptyset$, qui est équivalent à $\big(\exists x \in E,\ \mathcal{P}(x)\big)$.

- **La démonstration par un contre-exemple.** Soit E un ensemble, et $\mathcal{P}$ une propriété portant sur les éléments de E. Si on veut démontrer que la proposition $\big(\forall x \in E,\ \mathcal{P}(x)\big)$ est fausse, il suffit de trouver un élément $a \in E$ pour lequel $\mathcal{P}(a)$ est fausse. On dit souvent qu'un tel a est un *contre-exemple* de la proposition $\big(\forall x \in E,\ \mathcal{P}(x)\big)$. On en déduit que $a \notin \{x \in E\,;\, \mathcal{P}(x)\}$, donc $E \neq \{x \in E\,;\, \mathcal{P}(x)\}$. Ainsi, $\big(\forall x \in E,\ \mathcal{P}(x)\big)$ est fausse.

Remarque 1.59. Résumons quelques points importants à retenir pour éviter des erreurs :

(a) Ne pas confondre
- une *propriété portant sur des éléments* d'un ensemble E, que l'on formule à l'aide d'une *variable* désignant un élément quelconque de E, par exemple $x \in E$;
- une *proposition* : chacune des variables qui apparait dans une proposition doit être accompagnée d'un *quantificateur*.

(b) Une égalité entre deux ensembles est une double-inclusion, et de même, une équivalence entre propriétés ou propositions est une double-implication.

(c) Si une proposition contient plusieurs variables quantifiées, l'ordre dans lesquels ont les écrit est important ! Voir Remarque 1.51.

1.3. Applications

Dans cette section, nous allons étudier les applications et leurs principales propriétés. L'exemple le plus rencontré au lycée est celui des fonctions réelles d'une variable réelle. Nous allons voir qu'une application peut-être définie par son graphe.

Remarque 1.60. Nous avons défini plus haut les opérations sur les sous-ensembles d'un ensemble E (voir Définition 1.23). Ces opérations de réunion, d'intersection et de différence existent aussi pour des ensembles quelconques. Si A et B sont des ensembles, on peut définir en compréhension
- $A \cap B = \{a \in A\,;\, a \in B\} = \{a \in B\,;\, a \in A\}$,
- $A \smallsetminus B = \{a \in A\,;\, a \notin B\}$.

Par contre, on ne peut pas définir $A \cup B$ en compréhension si on ne sait pas *à priori* qu'il existe un ensemble E qui contient A et B comme sous-ensembles. L'existence d'un ensemble $A \cup B$ formé de tous les éléments qui sont dans A ou dans B est un axiome de la Théorie des Ensembles de Zermelo-Fraenkel.

Axiome 1.61. Soient E et F deux ensembles. Il existe un ensemble noté $E \times F$, dont les éléments sont les *paires ordonnées* (x, y) avec $x \in E$ et $y \in F$. On appelle $E \times F$ le *produit cartésien de E et F*. Le symbole $E \times F$ se lit parfois E *croix* F.

Remarque 1.62. On souhaiterait définir simplement

$$E \times F = \{(x, y)\,;\ x \in E \text{ et } y \in F\},$$

mais nous avons vu qu'il n'est possible de définir un ensemble en compréhension que comme sous-ensemble d'un autre ensemble : la formule ci-dessus ne défini pas un ensemble $E \times F$ car nous ne précisons pas à quel ensemble déjà défini (x, y) appartient. C'est pourquoi nous l'avons donné en 1.61 sous forme d'axiome. Cependant, il est possible de construire $E \times F$ en compréhension, à partir de E et F, en utilisant les axiomes qui garantissent l'existence de la réunion et de l'ensemble des parties. Nous l'indiquons ici pour les étudiants curieux, mais nous nous contenterons de l'approche axiomatique. La paire ordonnée (x, y) peut être définie comme un sous-ensemble de $P(E \cup F)$, donc comme un élément de $P\big(P(E \cup F)\big)$:

$$(x, y) := \{\{x\}, \{x, y\}\} \in P\big(P(E \cup F)\big)\,.$$

Notez que $\{x, y\} = \{y, x\}$, puisque dans les ensembles donnés en extension, l'ordre des éléments ne compte pas ; le rôle du singleton $\{x\}$ est de préciser que x est le premier terme de la paire (x, y) (et donc y est le deuxième terme de la paire). Remarquons que si $x \neq y$, alors $(x, y) = \{\{x\}, \{x, y\}\} \neq \{\{y\}, \{y, x\}\} = (y, x)$ (cela justifie la Remarque 1.63 ci-dessous). Avec cette définition de (x, y), le produit cartésien de E et F peut alors être défini en compréhension par

$$E \times F = \{(x, y) \in P\big(P(E \cup F)\big)\,;\ x \in E \text{ et } y \in F\}\,.$$

Remarque 1.63. Si E et F sont des ensembles avec $E \neq F$, alors $E \times F \neq F \times E$. Par ailleurs, dans une paire ordonnée $(x, y) \in E \times F$, on tient compte de l'ordre d'écriture des éléments (c'est le sens du mot *ordonnée* utilisé) : si $x \neq y$ alors $(x, y) \neq (y, x)$.

Notation 1.64. Dans le cas où $E = F$, on note souvent le produit cartésien de E avec lui-même par

$$E^2 := E \times E\,.$$

Exemples 1.65. **(a)** Si E est un ensemble, alors $\emptyset \times E = \emptyset$: comme $\emptyset$ ne contient aucun élément, on ne peut former aucune paire dont le premier élément est dans $\emptyset$, et le second dans E. De même, $E \times \emptyset = \emptyset$.

(b) On se représente en général $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ sous la forme d'un plan avec un système de coordonnées, la paire $(x, y) \in \mathbb{R}^2$ correspondant alors au point d'abscisse x et d'ordonnée y.

(c) Si E et F sont donnés en extension, on peut donner facilement $E \times F$ en extension. Par exemple, si $E = \{a, b, c\}$ et $F = \{0, 1\}$, alors

$$E \times F = \{(a, 0), (a, 1), (b, 0), (b, 1), (c, 0), (c, 1)\}$$
$$F \times E = \{(0, a), (0, b), (0, c), (1, a), (1, b), (1, c)\}\,.$$

On peut se représenter les éléments de $E \times F$ dans un tableau dont les colonnes sont indicées par E et les lignes par F (par analogie avec la représentation de $\mathbb{R}^2$ ci-dessus) :

(d) Si $A \subset E$ et $B \subset F$, alors on a une inclusion $A \times B \subset E \times F$. De plus, si A et B sont des ensembles donnés en compréhension par

$$A = \{x \in E \,;\, \mathcal{P}(x)\} \quad \text{et} \quad B = \{y \in F \,;\, \mathcal{Q}(y)\},$$

alors on peut donner $A \times F$, $E \times B$ et $A \times B$ en compréhension (comme sous-ensembles de $E \times F$) par

$$A \times F = \{(x, y) \in E \times F \,;\, \mathcal{P}(x)\}$$
$$E \times B = \{(x, y) \in E \times F \,;\, \mathcal{Q}(y)\}$$
$$A \times B = (A \times F) \cap (E \times B) = \{(x, y) \in E \times F \,;\, \mathcal{P}(x) \text{ et } \mathcal{Q}(y)\}.$$

Remarque 1.66. Dans certaines propositions, le produit cartésien nous permet de remplacer deux variables $x \in E$, $y \in F$ par une seule variable $(x, y) \in E \times F$, lorsque ces variables se suivent avec le *même* quantificateur : par exemple, la proposition

$$\big(\forall m \in \mathbb{N}, \forall n \in \mathbb{N}, \exists k \in \mathbb{N}, k > mn\big)$$

est équivalente à la proposition

$$\big(\forall (m, n) \in \mathbb{N} \times \mathbb{N}, \exists k \in \mathbb{N}, k > mn\big).$$

Donnons maintenant une définition intuitive de la notion d'application :

Définition 1.67 (Définition informelle d'une application)**.** Soient E et F deux ensembles. Une *application f de E dans F* associe à chaque élément $x \in E$ un unique élément $y \in F$, que l'on note $f(x)$. On la note

$$f \colon E \to F$$
$$x \mapsto f(x)$$

ou simplement $f \colon E \to F$. On dit que

- E est *l'ensemble de définition* (ou *l'ensemble de départ*, ou encore *la source*) de f ;
- F est *l'ensemble d'arrivée* (ou *le but*) de f ;
- $f(x) \in F$ est *l'image* de $x \in E$ par f.

Cette définition n'est pas très précise, car le sens de "associer à chaque élément $x \in E$ un unique élément $y \in F$" n'a pas été donné, même s'il est intuitif. En fait, on peut définir rigoureusement une application à l'aide d'un graphe.

Définition 1.68. Soient E et F deux ensembles. Un graphe dans $E \times F$ est un sous-ensemble $\Gamma \subset E \times F$ possédant la propriété suivante : pour tout $x \in E$, il existe un *unique* $y \in F$ tel que $(x, y) \in \Gamma$.

Une application peut être définie comme un graphe :

Définition 1.69. Soient E et F deux ensembles. Une application $f \colon E \to F$ est un graphe $\Gamma_f \subset E \times F$. Un élément $(x, y) \in \Gamma_f$ est alors noté $\big(x, f(x)\big)$. On dit que Γ_f est *le graphe de l'application f*.

Ainsi, une application est elle-même un ensemble ! Faisons le lien avec la Définition 1.67 : étant donné un graphe $\Gamma_f \subset E \times F$, la définition d'un graphe garantit que pour tout $x \in E$, il existe une unique paire $\big(x, f(x)\big) \in \Gamma_f$. On dit alors que l'application associe à $x \in E$ l'unique élément $f(x) \in F$.

Exemple 1.70.

Définition 1.71. Deux applications $f\colon E \to F$ et $g\colon G \to H$ sont dites *égales* si $E = G$, $F = H$, et $\Gamma_f = \Gamma_g$. On le note $f = g$. Ainsi, $f, g\colon E \to F$ sont égales si pour tout $x \in E$, on a $f(x) = g(x)$.

Exemples 1.72. (a) Soit E un ensemble. Dans ce cours, on dira qu'une *fonction* ou *fonction numérique* est une application de E dans un ensemble de nombres, par exemple $\mathbb{R}$ ou l'un de ses sous-ensembles.

(b) On peut souvent définir une fonction f à l'aide d'une formule pour $f(x)$, tout en précisant les ensembles de définition et d'arrivée, par exemple

$$f\colon \mathbb{R} \to \mathbb{R},\ \ x \mapsto x^2 - 2x + 1\,.$$

Cette notation signifie donc, pour $x \in \mathbb{R}$, que $f(x) = x^2 - 2x + 1$. Le graphe de cette fonction f est

$$\Gamma_f = \{(x, y) \in \mathbb{R} \times \mathbb{R}\ ;\ y = x^2 - 2x + 1\}\,.$$

Attention à ne pas confondre la fonction f avec la formule pour $f(x)$! Une fonction est une application, il faut donc bien préciser son ensemble de définition et son ensemble d'arrivée. Par exemple, avec cette même formule on peut définir des fonctions *différentes* :

$$\begin{aligned} f&\colon \mathbb{R} \to \mathbb{R},\ \ x \mapsto x^2 - 2x + 1\\ g&\colon [0,1] \to \mathbb{R},\ \ x \mapsto x^2 - 2x + 1\\ h&\colon [0,1] \to [0,1],\ \ x \mapsto x^2 - 2x + 1\\ k&\colon \mathbb{N} \to \mathbb{N},\ \ x \mapsto x^2 - 2x + 1 \end{aligned}$$

Bien sûr, quand on donne une application $f\colon E \to F$ à l'aide d'une formule pour $f(x)$, pour que cela ait un sens, il faut s'assurer que

- la formule $f(x)$ est bien définie pour *tout* $x \in E$;
- pour tout $x \in E$, la valeur $f(x)$ est unique et appartient à F.

Par exemple, l'écriture

$$f\colon \mathbb{R} \to \mathbb{R},\ \ x \mapsto \sqrt{x}$$

ne définit pas une fonction, car $\sqrt{x}$ n'est pas défini si $x < 0$. Par contre,

$$f\colon [0, \infty[\to \mathbb{R},\ \ x \mapsto \sqrt{x}$$

définit bien une fonction.

Définition 1.73. Soit E un ensemble. On définit *l'application identité de E* ou simplement *l'identité de E* par

$$\mathrm{id}_E\colon E \to E,\ \ x \mapsto x\,.$$

Son graphe est donné par $\Gamma_{\mathrm{id}_E} = \{(x, y) \in E \times E\ ;\ y = x\}$.

Définition 1.74. Soit $f : E \to F$ une application, et $A \subset E$ un sous-ensemble. On définit *la restriction de f à A* par

$$f|_A : A \to F, \quad x \mapsto f(x)\,.$$

Son graphe est donné par $\Gamma_{f|_A} = \{(x, y) \in A \times F\ ;\ (x, y) \in \Gamma_f\}$.

Définition 1.75. Soit E un ensemble et $A \subset E$ un sous-ensemble. Alors la restriction de id_E à A est appelée *l'inclusion* :

$$i : A \to E, \quad a \mapsto a\,.$$

Son graphe est donné par $\Gamma_i = \{(x, y) \in A \times E\ ;\ y = x\}$.

Exemples 1.76.

Définition 1.77. Soient E, F des ensembles et $f : E \to F$ une application de E dans F. On dit que f est

- *injective* si pour tous $x, z \in E$, l'égalité $f(x) = f(z)$ implique l'égalité $x = z$:

$$\Big(\forall x \in E, \forall z \in E\,,\ \big((f(x) = f(z)) \Rightarrow (x = z)\big)\Big) \text{ est vraie.}$$

- *surjective* si pour tout $y \in F$, il existe $x \in E$ avec $f(x) = y$:

$$\Big(\forall y \in F, \exists x \in E\,,\ \big(f(x) = y\big)\Big) \text{ est vraie.}$$

- *bijective* si elle est injective et surjective :

$$\Big(\forall y \in F, \exists! x \in E\,,\ \big(f(x) = y\big)\Big) \text{ est vraie.}$$

Exemples 1.78. Les exemples suivants permettent de "visualiser" ces notions :

Définition 1.79. Soient E et F des ensembles.

(a) *Une injection de E dans F* est une application injective $f : E \to F$.

(b) *Une surjection de E sur F* est une application surjective $f : E \to F$.

(c) *Une bijection de E dans F* est une application bijective $f : E \to F$.

Définition 1.80. Soit $f : E \to F$ une application.

(a) On appelle *image de f* le sous-ensemble formé des éléments de F qui sont l'image d'un élément de E, et on le note $\mathrm{Im}(f) \subset F$. Donc

$$\mathrm{Im}(f) = \{y \in F \,;\, \exists x \in E \text{ avec } f(x) = y\}\,.$$

(b) Si $A \subset E$, on appelle *image de A par f* (ou *image directe de A par f*) le sous-ensemble formé des éléments de F qui sont l'image d'un élément de A, et on le note $f(A) \subset F$. Donc

$$f(A) = \{y \in F \,;\, \exists x \in A \text{ avec } f(x) = y\}\,.$$

(c) Si $y \in F$, on appelle *antécédent de y* tout élément $x \in E$ avec $f(x) = y$.

(d) Si $B \subset F$, on appelle *préimage de B* (ou *image réciproque de B*) le sous-ensemble de E formé des éléments dont l'image est dans B, et on le note $f^{-1}(B) \subset E$. Donc

$$f^{-1}(B) = \{x \in E \,;\, f(x) \in B\}\,.$$

Remarque 1.81. Soit $f : E \to F$ une application. Il suit des définitions que l'on a les égalités suivantes :

- $\mathrm{Im}(f) = f(E)$.
- Soit $A \subset E$, et soit $f|_A : A \to E$ la restriction de f à A. Alors $f(A) = \mathrm{Im}(f|_A)$.
- Si $y \in F$, alors $f^{-1}(\{y\})$ est l'ensemble des antécédents de y.
- Si $B \subset F$, alors

$$f^{-1}(B) = \{x \in E \,;\, \exists y \in B \text{ tel que } x \text{ soit un antécédent de } y\}\,.$$

Exemples 1.82. **(a)** Considérons la fonction $f : \mathbb{R} \to \mathbb{R}$ avec $f(x) = x^2$.

- L'image de f est $\mathrm{Im}(f) = \mathbb{R}^+$, de même $f(\mathbb{R}) = \mathbb{R}^+$.
- L'image de $[1, 3]$ par f est $f([1, 3]) = [1, 9]$.
- L'image de $[-1, 2]$ par f est $f([-1, 2]) = [0, 4]$.
- Les antécédents de 1 sont 1 et -1.
- L'élément -1 n'a pas d'antécédent.
- La préimage de $[0, 1]$ est $f^{-1}([0, 1]) = [-1, 1]$. D'autres exemples sont $f^{-1}(]-\infty, 1]) = [-1, 1]$, $f^{-1}([-2, -1]) = \emptyset$, et $f^{-1}(\{9\}) = \{-3, 3\}$.

La proposition suivante est traitée en TD :

Proposition 1.83. *Soit $f : E \to F$ une application. Alors*

(a) *f est surjective si et seulement si* $\mathrm{Im}(f) = F$.

(b) *f est injective si et seulement si tout $y \in F$ admet* au plus *un antécédent.*

(c) *f est bijective si et seulement si tout $y \in F$ admet un* unique *antécédent.*

Définition 1.84. Soient E et F deux ensembles. On dénote par $\mathcal{F}(E,F)$ l'ensemble de toutes les applications de E dans F.

Remarque 1.85. Notons que $\mathcal{F}(E,F)$ est bien un ensemble, puisqu'il peut être donné en compréhension de la façon suivante (en se souvenant qu'une application $f\colon E \to F$ est un graphe $\Gamma_f \subset E \times F$) :

$$\mathcal{F}(E,F) = \{\Gamma \in P(E\times F)\,;\ \Gamma \text{ est un graphe}\}\,.$$

Exemples 1.86.

Définition 1.87. Soient E, F et G des ensembles, et $f\colon E \to F$, $g\colon F \to G$ des applications. On appelle *composition de f et g*, et on note $g \circ f$, l'application

$$g\circ f\colon E \to G,\quad x \mapsto g\circ f(x) := g\big(f(x)\big)\,.$$

Ainsi, la composition définit une application

$$\mathcal{F}(F,G)\times\mathcal{F}(E,F) \to \mathcal{F}(E,G),\quad (g,f)\mapsto g\circ f\,.$$

Remarque 1.88. Il faut prendre garde au fait suivant : si f et g sont des applications, alors la composition $g \circ f$ est définie par 1.87 seulement si l'ensemble d'arrivée de f est égal à l'ensemble de définition de g, par exemple $f\colon E \to F$ et $g\colon F \to G$ dans la définition ci-dessus. On visualise souvent cette situation de la façon suivante :

$$E \xrightarrow{f} F \xrightarrow{g} G\,.$$
$$\qquad\qquad\ \ \underset{g\circ f}{\frown}$$

Attention aussi à l'ordre d'écriture de f et g dans $g \circ f$!

Remarque 1.89. Dans la situation de la définition 1.87, considérons les graphes $\Gamma_f \subset E \times F$ et $\Gamma_g \subset F \times G$. On pose

$$\Gamma_{g\circ f} = \{(x,z)\in E\times G\,;\exists y\in F \text{ avec } (x,y)\in\Gamma_f \text{ et } (y,z)\in\Gamma_g\}\,.$$

Alors $\Gamma_{g\circ f}$ est bien un graphe, et c'est bien le graphe de $g \circ f$. En effet, soit $x \in E$. Alors il existe un unique $y \in F$ avec $(x,y) \in \Gamma_f$ (c'est $y = f(x)$), et un unique $z \in G$ avec $(y,z) \in \Gamma_g$ (c'est $z = g(y) = g\big(f(x)\big)$).

Exemples 1.90.

Proposition 1.91. *Soient E, F, G et H des ensembles, et supposons données des applications*

$$f\colon E \to F,\quad g\colon F \to G,\ \text{et}\ \ h\colon G \to H\,.$$

(a) *La composition est associative :*

$$h \circ (g \circ f) = (h \circ g) \circ f\,.$$

(b) *L'application identité est neutre pour la composition :*

$$f \circ \mathrm{id}_E = f = \mathrm{id}_F \circ f\,.$$

(c) *Si $A \subset E$ et si $i\colon A \to E$ est l'inclusion, alors $f \circ i = f|_A$.*

Démonstration.

□

Exemples 1.92. **(a)** On considère les applications $f, g, h\colon \mathbb{N} \to \mathbb{N}$ données par

$$f(n) = n + 1,\quad g(n) = n^2,\quad h(n) = 2n\ \text{ pour tout } n \in \mathbb{N}\,.$$

Alors on a par exemple les compositions suivantes :

Remarque 1.93. Lorsque l'on a deux applications $f\colon E \to E$ et $g\colon E \to E$, alors les compositions $g \circ f\colon E \to E$ et $f \circ g\colon E \to E$ sont toutes les deux définies. Attention, comme remarqué dans l'exemple ci-dessus, en général $g \circ f \neq f \circ g$.

Proposition 1.94. *Soit $f\colon E \to F$ une application. Alors les conditions suivantes sur f sont équivalentes.*

(a) *L'application f est bijective.*

(b) *Il existe une application $g\colon F \to E$ avec $g \circ f = \mathrm{id}_E$ et $f \circ g = \mathrm{id}_F$*

De plus, lorsque ces conditions sont satisfaites, une telle application g est unique.

Démonstration. Montrons que (a) implique (b). Puisque f est bijective, tout élément $y \in F$ admet un *unique* antécédent x. Notons $g\colon F \to E$ l'application qui associe à tout $y \in F$ son antécédent. Si $x \in E$, alors x est un antécédent de $f(x)$, et on en déduit $g\big(f(x)\big) = x$. Donc $g \circ f = \mathrm{id}_E$. De même, si $y \in F$, alors $g(y)$ est un antécédent de y, donc $f\big(g(y)\big) = y$, d'où $f \circ g = \mathrm{id}_F$.

Montrons que (b) implique (a). Il suffit de montrer que f est surjective et injective. Si $y \in F$, alors $f\big(g(y)\big) = g \circ f(y) = \mathrm{id}_F(y) = y$. Donc tout $y \in F$ est dans l'image de f, et f est surjective. Supposons $x, x' \in E$ donnés avec $f(x) = f(x')$. Alors

$$x = \mathrm{id}_E(x) = g \circ f(x) = g\big(f(x)\big) = g\big(f(x')\big) = f \circ g(x') = \mathrm{id}_E(x') = x' .$$

Ceci démontre que f est injective. Donc, étant surjective et injective, f est bijective.

Finalement, montrons que si une telle application g existe, elle est unique. Soit $g' \colon F \to E$ une deuxième application avec $g' \circ f = \mathrm{id}_E$ et $f \circ g' = \mathrm{id}_F$. Alors

$$g' = g' \circ \mathrm{id}_F = g' \circ (f \circ g) = (g' \circ f) \circ g = \mathrm{id}_E \circ g = g .$$

□

Définition 1.95. Soit $f \colon E \to F$ une application bijective. On appelle l'unique application $g \colon F \to E$ avec $g \circ f = \mathrm{id}_E$ et $f \circ g = \mathrm{id}_F$ *l'application réciproque de* f (ou simplement *la réciproque de* f), et on la note $f^{-1} \colon F \to E$.

Remarque 1.96. Si $F \colon E \to F$ est bijective et si f^{-1} est sa réciproque, alors on a

$$\Gamma_{f^{-1}} = \{(y, x) \in F \times E \,;\, (x, y) \in \Gamma_f\}$$

On remarque que la condition que f est bijective (donc que tout élément $y \in F$ admet un unique antécédent par f) est équivalente à la condition que $\Gamma_{f^{-1}}$ est un graphe.

Corollaire 1.97. *Si $f \colon E \to F$ et $g \colon F \to G$ sont bijectives, alors $g \circ f \colon E \to G$ est bijective, et l'on a $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.*

Démonstration.

□

Exemples 1.98.

Remarque 1.99. Attention à ne pas confondre les notations données aux Définitions 1.80 et 1.95 :

(a) Si $f \colon E \to F$ est une application et $B \subset F$, la préimage $f^{-1}(B)$ est définie même si f n'est pas bijective (et donc même si l'application réciproque $f^{-1} \colon F \to E$ n'existe pas). Ainsi, il ne faut pas déduire faussement de la notation $f^{-1}(B)$ que l'application réciproque de f existe.

(b) Si $f \colon E \to F$ est une bijection, sa réciproque $f^{-1} \colon F \to E$ existe. En particulier, si $B \subset F$, l'image directe $f^{-1}(B)$ de B par f^{-1} est définie.

Lorsque f est bijective de réciproque f^{-1}, il n'y a pas de confusion possible sur ce qu'est le sous-ensemble $f^{-1}(B) \subset E$: il est identique qu'on prenne la définition de (a) ou de (b) ci-dessus !

Chapitre 2

Les nombres entiers, rationnels, et réels

Dans ce chapitre, nous revisitons les ensembles de nombres bien connus suivants, et définissons les structures dont ils sont munis :

- $\mathbb{N}$, l'ensemble des entiers naturels ;
- $\mathbb{Z}$, l'anneau des nombres entiers relatifs ;
- $\mathbb{Q}$, le corps des nombres rationnels ;
- $\mathbb{R}$, le corps de nombres réels.

Notre objectif est de définir ces structures et d'énoncer certains résultats fondamentaux, tout en nous appuyant sur les connaissances intuitive et pratique que nous en avons. Certains résultats intuitifs dont la preuve est assez technique seront énoncés sans démonstration ; le cours *Arithmétique* de deuxième année de licence mathématique reprend certaines de ces notions plus en détails, en particulier sur l'anneau des entiers $\mathbb{Z}$. Le corps $\mathbb{R}$ des nombres réels et ses propriétés seront essentiellement étudiés dans les cours d'analyse.

2.1. Les nombres entiers naturels

2.1.1. Approche axiomatique

Dans la théorie des ensembles de Zermelo-Fraenkel, on peut démontrer l'existence d'un ensemble infini correspondant à l'ensemble des entiers naturels : c'est le résultat que nous énonçons ci-dessous sous la forme des *Axiomes de Peano*. Sa démonstration découle directement d'un axiome, appelé *axiome de l'infini* dans la théorie de Zermelo-Fraenkel.

Axiome 2.1 (Axiomes de Peano)**.** Il existe un triplet $(\mathbb{N}, 0, s)$, où $\mathbb{N}$ est un ensemble, $0 \in \mathbb{N}$ est un élément de $\mathbb{N}$ et $s : \mathbb{N} \to \mathbb{N}$ est une application, satisfaisant aux propriétés suivantes :

(P1) L'image de s est $\mathrm{Im}(s) = \mathbb{N} \smallsetminus \{0\}$;

(P2) L'application s est injective ;

(P3) Si A est un sous-ensemble de $\mathbb{N}$ avec $0 \in A$ et $s(a) \in A$ pour tout $a \in A$, alors $A = \mathbb{N}$.

L'ensemble $\mathbb{N}$ est appelé *l'ensemble des nombres entiers naturels*. Si $n \in \mathbb{N}$, l'élément $s(n) \in \mathbb{N}$ est appelé *le successeur de n*. Les propriétés (P1), (P2) et (P3) sont appelées *axiomes de Peano* des entiers naturels.

Remarques 2.2. (a) Le triplet $(\mathbb{N}, 0, s)$ est unique au sens suivant : si $(\mathbb{N}', 0', s')$ est un autre tel triplet satisfaisant aux Axiomes de Peano, alors il existe une unique bijection $f : \mathbb{N} \to \mathbb{N}'$ satisfaisant à

$$f(0) = 0', \quad \text{et} \quad f\big(s(n)\big) = s'\big(f(n)\big) \text{ pour tout } n \in \mathbb{N}.$$

En d'autre termes, cette bijection préserve le "zéro" et est compatible avec la notion de successeur : si m est le successeur de n dans $\mathbb{N}$, alors $f(m)$ est le successeur de $f(n)$ dans $\mathbb{N}'$. Cette application f et son inverse sont construites facilement à l'aide du Théorème 2.6.

(b) Puisque s est une application, chaque $n \in \mathbb{N}$ possède un successeur $s(n)$. En reprenant la terminologie introduite ci-dessus, les axiomes peuvent s'exprimer aussi de la façon suivante :

(P1) Chaque entier $n \in \mathbb{N}$ différent de 0 est le successeur d'un entier ;

(P2) Deux nombres différents ont des successeurs différents ;

(P3) Si A est un sous-ensemble de $\mathbb{N}$ contenant 0 ainsi que le successeur de chacun de ses éléments, alors $A = \mathbb{N}$.

(c) Les axiomes (P1) et (P2) permettent de déduire que $\mathbb{N}$ contient une infinité d'éléments : en effet, l'application $s : \mathbb{N} \to \mathbb{N}$ est injective par (P2), mais pas surjective par (P1), ce qui est impossible si $\mathbb{N}$ ne contient qu'un nombre fini d'éléments (c'est un résultat sur le quel nous reviendrons plus loin dans ce chapitre). D'autre part, par P(2) et P(3), chaque élément de $\mathbb{N}$ s'obtient à partir de 0 en prenant le successeur un nombre fini de fois. En introduisant les notations ci-dessous, on retrouve les entiers naturels dont on a une intuition depuis l'enfance.

Notation 2.3.

L'axiome de Péano (P3) est appelé l'*axiome de récurrence*, et permet dans de nombreuses situations de démontrer qu'une propriété $\mathcal{P}$ portant sur les éléments de $\mathbb{N}$ est vraie pour tout $n \in \mathbb{N}$: c'est le raisonnement par récurrence, sur le quel nous reviendrons plus en détails par la suite.

Théorème 2.4 (raisonnement par réccurrence)**.** *Soit $\mathcal{P}$ une propriété portant sur les éléments de l'ensemble $\mathbb{N}$. On suppose que :*

(1) *$\mathcal{P}(0)$ est vraie, et*

(2) *si n est un élément de $\mathbb{N}$ tel que $\mathcal{P}(n)$ soit vraie, alors $\mathcal{P}\big(s(n)\big)$ est vraie.*

Alors, $\mathcal{P}(n)$ est vraie pour tout élément n de $\mathbb{N}$.

Remarque 2.5. Dans la pratique, si on souhaite appliquer un raisonnement par récurrence pour montrer qu'une propriété $\mathcal{P}$ portant sur les éléments de l'ensemble $\mathbb{N}$ est vraie pour tout $n \in \mathbb{N}$, on procède alors en deux étapes :

- *Initialisation :* On démontre que $\mathcal{P}(0)$ est vraie
- *Itération* ou *hérédité* : on démontre que pour tout $n \in \mathbb{N}$, si $\mathcal{P}(n)$ est vraie, alors $\mathcal{P}(s(n))$ est vraie, ce qui revient à montrer que l'assertion

$$\big(\forall n \in \mathbb{N}\ ,\ \mathcal{P}(n) \Rightarrow \mathcal{P}(s(n))\big)$$

  est vraie.

Le Théorème 2.4 permet alors de conclure que $\big(\forall n \in \mathbb{N}\ ,\ \mathcal{P}(n)\big)$ est vraie : on dit que l'assertion $\big(\forall n \in \mathbb{N}\ ,\ \mathcal{P}(n)\big)$ a été *démontrée par récurrence*.

Une autre conséquence importante de l'axiome de récurrence est la possibilité de définir des applications $f : \mathbb{N} \to E$ par récurrence, formulée par le théorème suivant. Nous omettons sa démonstration.

Théorème 2.6 (Définition par récurrence)**.** *Soit E un ensemble. Supposons donnés*

(1) *Un élément $a \in E$;*

(2) *Une application $\varphi : E \to E$.*

Alors il existe une unique application $f : \mathbb{N} \to E$ satisfaisant à

$$f(0) = a \ \text{ et } \ f(s(n)) = \varphi(f(n)) \text{ pour tout } n \in \mathbb{N}\,.$$

Remarque 2.7. En fait il existe des résultats plus généraux pour définir $f : \mathbb{N} \to E$ par récurrence, nous en verrons d'autres plus loin. L'idée est que pour définir $f : \mathbb{N} \to E$, il suffit de donner $f(0)$, puis de donner une règle ou une formule indiquant comment on obtient $f(s(n))$ à partir de $f(n)$, pour tout n. Dans le théorème ci-dessus, c'est la fonction $\varphi : E \to E$ qui spécifie cette règle ou formule. Ce principe est très souvent utilisé, par exemple pour définir des *suites récurrentes* $\mathbb{N} \to \mathbb{R}$. Un principe similaire est aussi très utilisé en informatique (boucles en programmation).

À partir de cette définition axiomatique de $\mathbb{N}$, et à l'aide de la définition par récurrence, on peut retrouver les opérations bien connues sur $\mathbb{N}$ (addition et multiplication).

Définition 2.8.

Notation 2.9. En particulier, il suit de la notation $1 = s(0)$ et de la définition de l'addition que pour tout $n \in \mathbb{N}$, on a $s(n) = n + 1$. Désormais, on notera simplement $n + 1$ le successeur de n dans $\mathbb{N}$.

Définition 2.10. Soit E un ensemble. Une *opération binaire* $\star$ sur E est une application

$$E \times E \xrightarrow{\star} E, \quad (x, y) \mapsto x \star y \,.$$

On dit qu'elle est

- *associative* si pour tous $x, y, z \in E$, on a $x \star (y \star z) = (x \star y) \star z$.
- *commutative* si pour tous $x, y \in E$, on a $x \star y = y \star x$.

Proposition 2.11. *L'addition* $\mathbb{N} \times \mathbb{N} \xrightarrow{+} \mathbb{N}$ *et la multiplication* $\mathbb{N} \times \mathbb{N} \xrightarrow{\cdot} \mathbb{N}$ *des entiers sont des opérations binaires associatives et commutatives. De plus, la multiplication est distributive sur l'addition : pour tous* $a, b, c \in \mathbb{N}$*, on a*

$$a(b + c) = ab + ac \,.$$

Démonstration. Ces propriétés se démontrent par récurrence, c'est un exercice assez fastidieux. À titre d'exemple, faisons l'associativité de l'addition.

□

2.1.2. La relation d'ordre sur les entiers naturels

L'ensemble des entiers naturels est aussi muni d'une relation d'ordre bien connue. Donnons d'abord les définitions nécessaires.

Définition 2.12. Soit E un ensemble. *Une relation binaire sur E* est un sous-ensemble

$$\mathrm{R} \subset E \times E\,.$$

Si $(x, y) \in \mathrm{R}$, on dit que *x est en relation avec y (par* R*)*, et on le note $x\mathrm{R}y$. On utilise aussi la notation $x\not\mathrm{R}y$ pour dire $(x, y) \notin \mathrm{R}$.

Définition 2.13. Une relation binaire R sur E est dite

- *réflexive* si pour tout $x \in E$, on a $x\mathrm{R}x$,
- *symétrique* si pour tout $x, y \in E$, on a $x\mathrm{R}y \Leftrightarrow y\mathrm{R}x$,
- *antisymétrique* si pour tout $x, y \in E$ on a $(x\mathrm{R}y \text{ et } y\mathrm{R}x) \Rightarrow (x = y)$,
- *transitive* si pour tous $x, y, z \in E$, on a $(x\mathrm{R}y \text{ et } y\mathrm{R}z) \Rightarrow (x\mathrm{R}z)$.

Exemples 2.14.

Définition 2.15. On appelle *relation d'ordre* (ou *relation d'ordre partiel*) sur un ensemble E une relation binaire R sur E qui est réflexive, antisymétrique et transitive. Un *ensemble ordonné* (E, R) est un ensemble E muni d'une relation d'ordre R.

Notation 2.16. On note souvent $\leqslant$ la relation d'ordre d'un ensemble ordonné.

Exemple 2.17. La relation bien connue *"plus petit ou égal"*, notée comme ci-dessus par le symbole $\leqslant$, sur les ensembles de nombres $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ et $\mathbb{R}$ est une relation d'ordre. Nous la définissons ci-dessous pour $\mathbb{N}$, et l'étendrons ensuite à $\mathbb{Z}$ et $\mathbb{Q}$.

Définition 2.18. On définit sur $\mathbb{N}$ une relation $\leqslant$ par la règle suivante :

$$\text{Si } m, n \in \mathbb{N}\text{, on pose } m \leqslant n \text{ s'il existe } p \in \mathbb{N} \text{ avec } m + p = n.$$

La relation $m \leqslant n$ se lit *m est plus petit ou égal à n*.

Proposition 2.19. *La relation $\leqslant$ sur $\mathbb{N}$ définie ci-dessus est une relation d'ordre.*

Démonstration.

□

Définition 2.20. Soit $(E, \leqslant)$ un ensemble ordonné, et soit $A \subset E$ un sous-ensemble. On dit que $a \in A$ est un *minimum de A* (respectivement un *maximum de A*) si pour tout $x \in A$, on a la relation $a \leqslant x$ (respectivement $x \leqslant a$). On dit que la relation d'ordre $\leqslant$ sur E est un *bon ordre* si tout sous-ensemble $A \subset E$ non-vide admet un minimum.

Proposition 2.21 (Bon ordre)**.** *La relation d'ordre $\leqslant$ sur $\mathbb{N}$ est un* bon ordre.

Démonstration.

□

Définition 2.22. Soit $(E, \leqslant)$ un ensemble ordonné. On dit que deux éléments $x, y \in E$ sont *comparables* si l'on a $x \leqslant y$ ou $y \leqslant x$. On dit que $(E, \leqslant)$ est un ensemble *totalement ordonné* si, quelque soient $x, y \in E$, x, y sont comparables. On dit alors que la relation $\leqslant$ est une *relation d'ordre total sur E*.

Exemple 2.23.

Proposition 2.24. *Si $(E, \leqslant)$ est un ensemble ordonné et si $\leqslant$ est un bon ordre sur E, alors $\leqslant$ est un ordre total. En particulier, $(\mathbb{N}, \leqslant)$ est totalement ordonné.*

Démonstration. Supposons $(E, \leqslant)$ munit d'un bon ordre. Si $x, y \in E$ sont deux éléments quelconques, l'ensemble $A = \{x, y\}$ est un sous-ensemble non-vide de E, et possède donc un minimum. Si x est le minimum, alors $x \leqslant y$, et si c'est y, alors $y \leqslant x$. Donc toute paire est comparable, et $(E, \leqslant)$ est totalement ordonné. □

Lemme 2.25 (Propriété d'Archimède)**.** *Soient $a, b \in \mathbb{N}$. Si $a \neq 0$, alors il existe $n \in \mathbb{N}$ avec $b < n \cdot a$.*

Démonstration.

□

Notations 2.26. Soit $(E, \leqslant)$ un ensemble ordonné.

(1) Nous verrons en TD que la relation $\geqslant$ sur E définie par $x \geqslant y \Leftrightarrow y \leqslant x$ est aussi une relation d'ordre sur E. Elle se lit : *x est plus grand ou égal à y*.

(2) On défini la relation $<$ sur E par

$$x < y \Leftrightarrow (x \leqslant y \text{ et } x \neq y)\,.$$

Elle se lit : *x est strictement plus petit que y*. On définit de même la relation $>$ par $x > y \Leftrightarrow y < x$. Attention, ce ne sont pas des relations d'ordre : elles ne sont pas réflexives !

2.1.3. Démonstrations et définitions par récurrence

Dans cette section, on revient plus en détail sur le principe des démonstrations et définition par récurrence, énoncés dans les Théorèmes 2.4 et 2.6, et on mentionne des variantes. Commençons par trois exemples détaillés.

Exemple 2.27. On souhaite définir, pour tout $m \in \mathbb{N}$, l'entier 2^m à l'aide du Théorème 2.6. On considère l'application $\varphi : \mathbb{N} \to \mathbb{N}$ définie par $\varphi(n) = 2n$. Si on pose $f(0) = 1$, le Théorème 2.6 garantit l'existence d'une unique application

$$f : \mathbb{N} \to \mathbb{N} \text{ avec } f(0) = 1 \text{ et } f(n+1) = 2f(n) \text{ pour tout } n \in \mathbb{N}\,.$$

On définit alors $2^m := f(m)$. Remarquons que par définition, on a $2^0 = 1$. Par un procédé similaire, on peut définir ℓ^m pour tous $\ell, m \in \mathbb{N}$.

Exemple 2.28. On veut montrer que pour tout $\ell, m, n \in \mathbb{N}$, on a $\ell^{m+n} = \ell^m \cdot \ell^n$. On suppose ℓ et $m \in \mathbb{N}$ fixés, et montrons que cette égalité est vraie par récurrence sur n. Posons $\mathcal{P}(n) : \ell^{m+n} = \ell^m \cdot \ell^n$.

(1) *Initialisation.* Il est clair que $\mathcal{P}(0)$ est vraie puisque $\ell^{m+0} = \ell^m = \ell^m \cdot 1 = \ell^m \cdot \ell^0$.

(2) *Itération.* Soit $n \in \mathbb{N}$. Supposons $\mathcal{P}(n)$ vraie. Alors

$$\ell^{m+(n+1)} = \ell^{(m+n)+1} = \ell \cdot \ell^{m+n} = \ell \cdot \ell^m \cdot \ell^n = \ell^m \cdot \ell \cdot \ell^n = \ell^m \cdot \ell^{n+1}\,,$$

ce qui implique que $\mathcal{P}(n+1)$ est vraie. D'après le Théorème 2.4, la propriété $\mathcal{P}(n)$ est vraie pour tout élément n de $\mathbb{N}$.

En passant, remarquons qu'on vient d'utiliser que pour tout $n \in \mathbb{N}$, on a $n \cdot 1 = n$. On peut bien sûr démontrer cette assertion par récurrence !

Exemple 2.29. On veut démontrer par récurrence la proposition que pour tout $n \in \mathbb{N}$, l'entier naturel $2^{2n} + 2$ est divisible par 3. On rappelle que si a et b sont deux entiers naturels, on dit que *a est divisible par b* s'il existe $k \in \mathbb{N}$ tel que $a = kb$, et on le note $b|a$. On considère donc la propriété $\mathcal{Q}(n) : \ 3|(2^{2n} + 2)$ portant sur les éléments $n \in \mathbb{N}$, et on veut démontrer la proposition $\big(\forall n \in \mathbb{N}\,,\ \mathcal{Q}(n)\big)$. On doit vérifier les deux conditions données dans le Théorème 2.4.

(1) *Initialisation.* Il est clair que $\mathcal{Q}(0)$ est vraie puisque $2^{2\cdot 0} + 2 = 2^0 + 2 = 1 + 2 = 3$ est bien divisible par 3.

(2) *Itération.* Soit $n \in \mathbb{N}$. Supposons $\mathcal{Q}(n)$ vraie. Cela signifie qu'on suppose que $2^{2n} + 2$ est divisible par 3, c'est-à-dire qu'il existe un élément $k \in \mathbb{N}$ tel que $2^{2n} + 2 = 3k$. On doit démontrer qu'alors, $\mathcal{Q}(n+1)$ est vraie. Or,

$$\begin{aligned} 2^{2(n+1)} + 2 = 2^{2n+2} + 2 = 2^2 2^{2n} + 2 = 4 \cdot 2^{2n} + 2 = (3+1)2^{2n} + 2 \\ = (3 \cdot 2^{2n} + 2^{2n}) + 2 = 3 \cdot 2^{2n} + (2^{2n} + 2) = 3 \cdot 2^{2n} + 3k = 3(2^{2n} + k). \end{aligned}$$

Comme $(2^{2n} + k)$ est un entier, l'égalité $2^{2(n+1)} + 2 = 3(2^{2n} + k)$ montre que 3 divise $2^{2(n+1)} + 2$, c'est-à-dire que $\mathcal{Q}(n+1)$ est vraie.

D'après le Théorème 2.4, la propriété $\mathcal{Q}(n)$ est vraie pour tout élément n de $\mathbb{N}$. En conclusion, on a montré que pour tout $n \in \mathbb{N}$, $2^{2n} + 2$ est divisible par 3.

Énonçons maintenant des variantes des Théorèmes 2.4 et 2.6 souvent utilisées.

Théorème 2.30. *Soient n_0 un élément de $\mathbb{N}$ et $\mathcal{P}$ une propriété portant sur les éléments du sous-ensemble $\{n \in \mathbb{N}\ ;\ n \geqslant n_0\}$ de $\mathbb{N}$. On suppose que :*

(1) *$\mathcal{P}(n_0)$ est vraie, et*

(2) *si $n \in \mathbb{N}$ est tel que $n \geqslant n_0$ et $\mathcal{P}(n)$ soit vraie, alors $\mathcal{P}(n+1)$ est vraie.*

Alors $\mathcal{P}(n)$ est vraie pour tout $n \in \mathbb{N}$ avec $n \geqslant n_0$.

Démonstration. On considère la propriété Q portant sur les éléments de $\mathbb{N}$, définie par

$$Q(n) \Leftrightarrow \mathcal{P}(n_0 + n).$$

Les hypothèses du présent théorème assurent que la propriété Q satisfait aux hypothèses du Théorème 2.4. Le Théorème 2.4 assure donc que $Q(n)$ est vraie pour tout $n \in \mathbb{N}$, ce qui revient à dire que $\mathcal{P}(n)$ est vraie pour tout $n \in \mathbb{N}$ tel que $n \geqslant n_0$. □

Théorème 2.31 (Récurrence forte)**.** *Soit $\mathcal{P}$ une propriété portant sur les éléments de $\mathbb{N}$. On suppose que*

(1) *$\mathcal{P}(0)$ est vraie, et*

(2) *si $n \geqslant 0$ est un entier tel que $\mathcal{P}(k)$ est vraie pour tout $k \leqslant n$, alors $\mathcal{P}(n+1)$ est vraie.*

Alors $\mathcal{P}(n)$ est vraie pour tout élément $n \in \mathbb{N}$.

La version ci-dessus de démonstration par *récurrence forte* est *équivalente* à celle donnée par le Théorème 2.4 : pour l'étape d'itération, si c'est utile pour l'argument, on peut donc sans autre supposer que $\mathcal{P}(k)$ est vraie *pour tout* $k \leqslant n$, et en déduire $\mathcal{P}(n+1)$. On peut bien sûr aussi combiner les Théorèmes 2.30 et 2.31, et faire une récurrence forte pour une propriété portant sur les éléments de $\{n \in \mathbb{N} \,;\, n \geqslant n_0\}$. Un exemple d'utilisation de la possibilité offerte par la récurrence forte est la démonstration que tout nombre entier naturel se décompose en produit de nombres premiers, que nous verrons dans la suite.

Il existe, de même, des variantes de la *définition par récurrence* donnée par le Théorème 2.6, et permettant de définir $f : E \to \mathbb{N}$. On rappelle que pour définir une telle application f, il suffit de définir $f(0)$ ainsi qu'une règle permettant d'obtenir, pour tout $n \in \mathbb{N}$, $f(n+1)$ à partir de $f(n)$. Une variante, s'apparentant à la récurrence forte, est de définir une règle permettant d'obtenir $f(n+1)$ à partir des deux valeurs précédentes $f(n-1)$ et $f(n)$ (ou plusieurs d'entre elles).

Exemple 2.32 (Suite de Fibonacci)**.**

Une autre variante consiste à faire dépendre de n la règle permettant d'obtenir $f(n+1)$ à partir de $f(n)$. Le théorème suivant en est un exemple.

Théorème 2.33 (Définition par récurrence, version 2)**.** *Soit E un ensemble. Supposons donnés*

(1) *Un élément $a \in E$;*

(2) *Une application $\varphi : \mathbb{N} \times E \to E$.*

Alors il existe une unique application $f : \mathbb{N} \to E$ satisfaisant à

$$f(0) = a \quad \text{et} \quad f(s(n)) = \varphi(n, f(n)) \text{ pour tout } n \in \mathbb{N}.$$

Exemple 2.34. L'application $\mathbb{N} \to \mathbb{N}$, $n \mapsto n!$ (n factorielle) peut être facilement définie à l'aide de ce théorème.

2.1.4. Les ensembles finis et leur cardinal

Introduisons d'abord une notation qui nous sera utile dans cette section :

Notation 2.35. Soit $n \in \mathbb{N}$. Notons $[\![n]\!] \subset \mathbb{N}$ le sous-ensemble défini par

$$[\![n]\!] = \{k \in \mathbb{N} \,;\, 1 \leqslant k \leqslant n\}.$$

Par exemple, on a $[\![0]\!] = \emptyset$, $[\![1]\!] = \{1\}$ et $[\![4]\!] = \{1, 2, 3, 4\}$.

Proposition 2.36. *Supposons donnés m et $n \in \mathbb{N}$. Alors les conditions suivantes sur m et n sont équivalentes :*

(a) *On a $m \leqslant n$.*

(b) *Il existe une injection $f : [\![m]\!] \to [\![n]\!]$.*

Démonstration.

□

Corollaire 2.37. *Supposons donnés m et $n \in \mathbb{N}$. Alors les conditions suivantes sur m et n sont équivalentes :*

(a) *On a $m = n$.*

(b) *Il existe une bijection $f : [\![m]\!] \to [\![n]\!]$.*

Démonstration. L'implication (a) $\Rightarrow$ (b) est claire, car il suffit de prendre $f = \mathrm{id}_{[\![m]\!]}$. Inversement, si f est une bijection, alors f et f^{-1} sont injectives, et on applique la Proposition 2.36. □

Définition 2.38. Soit E un ensemble.

(a) On dit que E est *un ensemble fini* s'il existe $n \in \mathbb{N}$ et une bijection $[\![n]\!] \to E$.

(b) On dit que E est *un ensemble infini* si E n'est pas fini.

Proposition 2.39. *Soit E un ensemble.*

(a) *Si E est fini, il existe* un unique *entier $n \in \mathbb{N}$ pour lequel il existe une bijection $[\![n]\!] \to E$.*

(b) *Si E est infini, il existe une injection $\mathbb{N} \to E$.*

Démonstration. L'assertion (a) suit immédiatement du Corollaire 2.37. Nous omettons la démonstration de l'assertion (b). □

Définition 2.40. Soient E et F deux ensembles.

(a) On dit que *E et F ont même cardinal* s'il existe une bijection $E \to F$.

(b) Si E est un ensemble fini, l'unique entier $n \in \mathbb{N}$ pour lequel il existe une bijection $[\![n]\!] \to E$ est appelé *le cardinal de E*. Il est noté $\mathrm{card}(E)$ (ou parfois $\#E$, ou encore $|E|$). On dit aussi que E a n éléments.

(c) Si E est infini, on dit que E est

- *dénombrable* s'il existe une bijection $\mathbb{N} \to E$, et
- *(infini) non dénombrable* sinon.

Exemples 2.41. (a) On a bien sûr $\mathrm{card}([\![n]\!]) = n$ pour tout $n \in \mathbb{N}$. En particulier, $\mathrm{card}(\emptyset) = 0$.

Théorème 2.42. *Soient E et F deux ensembles finis.*

(a) *Il existe une application injective $E \to F$ si et seulement si* $\mathrm{card}(E) \leqslant \mathrm{card}(F)$.

(b) *Supposons $F \neq \emptyset$. Il existe une application surjective $E \to F$ si et seulement si* $\mathrm{card}(E) \geqslant \mathrm{card}(F)$.

(c) *Il existe une application bijective $E \to F$ si et seulement si* $\mathrm{card}(E) = \mathrm{card}(F)$.

Démonstration. Nous démontrons le point (a) à l'aide de la Proposition 2.36. Le point (b) se démontre de façon similaire à l'aide de l'Exercice 8.3, et le point (c) à l'aide du Corollaire 2.37.

□

Proposition 2.43. *Soit E un ensemble fini et $F \subset E$. Alors*

(a) *F est fini et* $\mathrm{card}(F) \leqslant \mathrm{card}(E)$*;*

(b) *Si* $\mathrm{card}(F) = \mathrm{card}(E)$*, alors $F = E$.*

Démonstration. Le résultat se démontre par récurrence sur $n \in \mathrm{card}(E) \in \mathbb{N}$. Si $n = 0$, alors $E = \emptyset$, et donc $F = \emptyset = E$, et le résultat est vrai. Supposons $n \geqslant 1$ et le résultat vrai si $\mathrm{card}(E) = n - 1$. Supposons donné un ensemble E avec $\mathrm{card}(E) = n$, et $F \subset E$. Si $F = E$, alors les assertions sont vérifiées. Il reste à traiter le cas $F \subsetneq E$. En utilisant une bijection, on peut se ramener au cas où $E = [\![n]\!]$. Dans ce cas, comme $F \neq E$, il existe $k \in E \setminus F$, donc $F \subset E \setminus \{k\}$. On construit facilement une bijection $E \setminus \{k\} \to [\![n-1]\!]$, donc $\mathrm{card}(E \setminus \{k\}) = n - 1$. Par hypothèse de récurrence, on en déduit que F est fini, et

$$\mathrm{card}(F) \leqslant \mathrm{card}(E \setminus \{k\}) = n - 1 < n = \mathrm{card}(E),$$

donc $\mathrm{card}(F) < \mathrm{card}(E)$. Ainsi, les assertions (a) et (b) sont vraies si $\mathrm{card}(E) = n$. Par récurrence, la proposition est démontrée pour tout ensemble fini E. □

Théorème 2.44. *Soient E et F deux ensembles finis de même cardinal, et $f : E \to F$ une application. Les assertions suivantes sont équivalentes :*

(1) *l'application f est injective ;*

(2) *l'application f est surjective ;*

(3) *l'application f est bijective.*

Démonstration.

□

La proposition suivante énonce plusieurs formules utiles sur les cardinaux. Sa démonstration est laissée en exercice.

Proposition 2.45. *Soient E et F deux ensembles finis.*

(a) *L'ensemble $E \cup F$ est fini, et* $\mathrm{card}(E \cup F) = \mathrm{card}(E) + \mathrm{card}(F) - \mathrm{card}(E \cap F)$.

(b) *L'ensemble $E \times F$ est fini, et* $\mathrm{card}(E \times F) = \mathrm{card}(E) \times \mathrm{card}(F)$.

(c) *L'ensemble $\mathcal{F}(E, F)$ est fini, et* $\mathrm{card}\left(\mathcal{F}(E, F)\right) = \mathrm{card}(F)^{\mathrm{card}(E)}$.

(d) *L'ensemble $P(E)$ des parties de E est fini, et* $\mathrm{card}\left(P(E)\right) = 2^{\mathrm{card}(E)}$.

Proposition 2.46. *Soit $A \subset \mathbb{N}$. Les conditions suivantes sur A sont équivalentes :*

(a) *L'ensemble A est fini et non-vide.*

(b) *L'ensemble A admet un maximum : il existe $a \in A$ avec $n \leqslant a$ pour tout $n \in A$.*

Démonstration.

□

2.2. Les nombres entiers relatifs

Si $a, b \in \mathbb{N}$ et si $a \leqslant b$, alors, par définition, il existe un (unique) entier $p \in \mathbb{N}$ avec $a + p = b$. On peut noter $p =: b - a$. L'opération de *soustraction* $(b, a) \mapsto b - a$ n'est définie que si $a \leqslant b$. Le groupe des entiers relatifs $\mathbb{Z}$ est défini pour généraliser la soustraction : on souhaite agrandir $\mathbb{N}$ en lui ajoutant des éléments de la forme $-a$ pour tout $a \in \mathbb{N}$, vérifiant $a + (-a) = 0$, tout en préservant l'addition. On pourra ensuite définir la soustraction $b - a$ quelques soient a, b par $b - a := b + (-a)$.

Définition 2.47. Soit G un ensemble, et $\star : G \times G \to G$ une opération binaire sur G. On dit que $(G, \star)$ est *un groupe* si les conditions suivantes sont satisfaites :

(1) L'opération $\star$ est associative ;

(2) L'opération $\star$ admet un élément neutre : il existe $e \in G$ avec $e \star x = x = x \star e$ pour tout $x \in G$.

(3) Tout élément de G admet un inverse pour $\star$: pour tout $x \in G$, il existe $y \in G$ avec $x \star y = e = y \star x$.

On dit que le groupe G est *abélien* ou *commutatif* si de plus, l'opération $\star$ est commutative.

Exemples 2.48. (a) Remarquons que $(\mathbb{N}, +)$ n'est pas un groupe : la condition (3) de la définition n'est pas satisfaite (on dit que $(\mathbb{N}, +)$ est *un monoïde*).

Définition 2.49. On appelle *relation d'équivalence* sur un ensemble E une relation binaire sur E qui est réflexive, symétrique et transitive.

Exemples 2.50. (a) L'égalité sur E est une relation d'équivalence.

Notation 2.51. Soit R une relation d'équivalence sur un ensemble E, et soient $a, b \in E$. Comme la relation R est symétrique, si on a $a\mathrm{R}b$, alors on a aussi $b\mathrm{R}a$, et on dit simplement que *a et b sont équivalent (modulo la relation R)*. On le note

$$a \sim b \,(\mathrm{mod}\,\mathrm{R}),$$

ou plus simplement $a \sim b$ si R est sous-entendue. De même, si $a\not\mathrm{R}b$, on dit que *a et b ne sont pas équivalents*, et on le note $a \nsim b \,(\mathrm{mod}\,\mathrm{R})$, ou simplement $a \nsim b$.

Définition 2.52. Soit E un ensemble muni d'une relation d'équivalence R et soit $x \in E$. On appelle *classe d'équivalence de x modulo* R le sous-ensemble de E formé des éléments de E en relation avec x. On le note en général C_x ou $[x]$. Ainsi, on a

$$C_x := [x] := \{y \in E\,;\; y \sim x \,(\mathrm{mod}\,\mathrm{R})\}.$$

Théorème 2.53. *Soit* R *une relation d'équivalence sur E.*

(a) *Pour tout $x \in E$, on a $x \in C_x$, et en particulier $C_x \neq \emptyset$.*

(b) *Pour tout $x, y \in E$, on a $(x \sim y) \Leftrightarrow (C_x = C_y)$.*

(c) *Pour tout $x, y \in E$, on a $(x \nsim y) \Leftrightarrow (C_x \cap C_y = \emptyset)$.*

Démonstration. (a) La relation R étant réflexive, on a $x \sim x$ pour tout $x \in E$, ce qui revient à $x \in C_x$ par définition de C_x.

(b) Supposons $x \sim y$, et soit $z \in C_x$, ce qui équivaut à $z \sim x$. Puisque la relation $\sim$ est transitive, on a donc $(z \sim x \text{ et } x \sim y) \Rightarrow (z \sim y)$, donc $z \in C_y$. On a donc montré

$$(x \sim y) \;\Rightarrow\; (C_x \subset C_y)\,.$$

Or par symétrie de R, on a $(x \sim y) \Rightarrow (y \sim x) \Rightarrow (C_y \subset C_x)$. Ainsi, on démontré que

$$(x \sim y) \;\Rightarrow\; (C_x \subset C_y \text{ et } C_y \subset C_x) \;\Leftrightarrow\; (C_x = C_y)\,.$$

Réciproquement, puisque $x \in C_x$ par (a), si $C_x = C_y$, alors $x \in C_y$ et donc $x \sim y$.

(c) On démontre la contraposée de (c), c'est-à-dire

$$(C_x \cap C_y \neq \emptyset) \Leftrightarrow (x \sim y)\,.$$

Si $C_x \cap C_y \neq \emptyset$, choisissons $z \in C_x \cap C_y$. Alors on a $z \sim x$ et $z \sim y$, donc aussi $x \sim z$, d'où $x \sim y$ par transitivité. Réciproquement, si $x \sim y$ alors $x \in C_x$ et $x \in C_y$, donc $x \in C_x \cap C_y$, ce qui montre que $C_x \cap C_y \neq \emptyset$. □

Exemples 2.54.

Définition 2.55. Soit E un ensemble, et soit $Q \subset P(E)$ un ensemble de parties de E.

(a) On définit *la réunion des sous-ensembles $A \in Q$ de E* par

$$\bigcup_{A\in Q} A = \{x \in E\,;\ (\exists A \in Q,\ x \in A)\} \subset E\,.$$

(b) Si A et $B \in P(E)$, on dit que *A et B sont disjoints* si $A \cap B = \emptyset$. Dans ce cas, on dit que la réunion $A \cup B \subset E$ est *une réunion disjointe*. On utilise souvent la notation suivante :

$$C = A \sqcup B \ \Leftrightarrow\ \big(C = A \cup B \text{ et } A \cap B = \emptyset\big)\,.$$

Similairement, si les éléments de Q sont deux-à-deux disjoints, on dit que *la réunion $\bigcup_{A\in Q} A$ est disjointe*, et on utilise la notation

$$C = \bigsqcup_{A\in Q} A \ \Leftrightarrow\ \left(C = \bigcup_{A\in Q} A \ \text{ et } \ \Big(\forall A \in Q,\ \forall B \in Q,\ (A \neq B \Rightarrow A \cap B = \emptyset)\Big)\right)\,.$$

(c) Soit $Q \subset P(E)$. On dit que Q est *une partition de E* si Q satisfait aux conditions suivantes :

- $\emptyset \notin Q$, et
- $E = \bigsqcup_{A\in Q} A$.

Exemples 2.56.

On peut reformuler le Théorème 2.53 de la façon suivante :

Proposition 2.57. *Soit* R *une relation d'équivalence sur E. Les classes d'équivalence de E modulo* R *forment une partition de E.*

Remarque 2.58. Réciproquement, si on se donne une partition $Q \subset P(E)$ de E, on peut définir une relation d'équivalence R telle que les ensembles $A \in Q$ soient exactement les classes d'équivalence modulo R. Il suffit de définir la relation :

$$x\mathrm{R}y \Leftrightarrow (\exists A \in Q,\ x \in A \text{ et } y \in A).$$

Exemples 2.59.

Définition 2.60. Soit R une relation d'équivalence sur E. Alors l'ensemble

$$E/_{\mathrm{R}} := \{A \in P(E)\,;\ \exists x \in E, A = C_x\}$$

des classes d'équivalences modulo R est appelé *le quotient de E modulo* R. L'application

$$\pi\colon E \to E/_{\mathrm{R}},\ \ x \mapsto \pi(x) := C_x$$

est appelée *l'application quotient*, ou *la surjection canonique (associée à R)*.

Intuitivement, dans l'ensemble quotient, on a *identifié* tous les éléments d'une classe (on les *a rendus égaux entre eux*), et l'application quotient encode ce processus.

Remarque 2.61. Remarquons que par définition $E/_{\mathrm{R}} \subset P(E)$. Donc, il faut bien comprendre qu'un *élément* de $E/_{\mathrm{R}}$ est un *sous-ensemble* de E. Si $A \in E/_{\mathrm{R}}$, on sait qu'il existe $x \in E$ tel que $A = C_x = \pi(x)$ (donc π est bien surjective). Cependant, un tel x est loin d'être unique en général ! En effet, le Théorème 2.53 implique que pour tout $x \in A$, on a $A = C_x$.

Définition 2.62. Soit E un ensemble, R une relation d'équivalence sur E, et $A \in E/_{\mathrm{R}}$. Un élément $x \in E$ avec $A = C_x$ est appelé *un représentant* de la classe A.

Remarque 2.63. Attention ! La notation $A \in E/_{\mathrm{R}}$ ne fait pas intervenir de représentant de A. Si on utilise la notation $C_x \in E/_{\mathrm{R}}$ au lieu de A, on sous-entend qu'un représentant x de la classe A a été choisi !

Exemples 2.64.

Revenons à $\mathbb{Z}$. On souhaite construire, en partant de $\mathbb{N}$ et son addition, un groupe abélien $(\mathbb{Z}, +)$ avec les propriétés suivantes :

(1) $\mathbb{N} \subset \mathbb{Z}$, et l'addition de $\mathbb{N}$ est compatible avec l'addition de $\mathbb{Z}$;

(2) Si $x \in \mathbb{Z}$ alors on a $x \in \mathbb{N}$ ou $-x \in \mathbb{N}$;

(3) On peut définir sur $\mathbb{Z}$ une multiplication compatible avec celle de $\mathbb{N}$.

Nous donnons ci-dessous une définition de $\mathbb{Z}$ comme ensemble quotient de $\mathbb{N} \times \mathbb{N}$ par une relation d'équivalence, de façon à ce que la paire $(a, b) \in \mathbb{N} \times \mathbb{N}$ représente l'élément $a - b \in \mathbb{Z}$. On voit bien que $\mathbb{N} \times \mathbb{N}$ est "trop gros" : par exemple $(1, 2)$ et $(2, 3)$ représentent le même élément $1 - 2 = -1 = 2 - 3$. On veut donc que $(1, 2)$ et $(2, 3)$ soient équivalents dans $\mathbb{N} \times \mathbb{N}$, et deviennent ainsi égaux dans $\mathbb{Z}$. C'est exactement ce que fait la relation suivante.

Lemme 2.65. *On considère sur* $\mathbb{N} \times \mathbb{N}$ *la relation* R *définie par*

$$\forall (a, b) \in \mathbb{N} \times \mathbb{N}, \forall (c, d) \in \mathbb{N} \times \mathbb{N}, \ (a, b) \sim (c, d) \ (\mathrm{mod\ R}) \ \Leftrightarrow \ a + d = b + c.$$

Alors R *est une relation d'équivalence sur* $\mathbb{N} \times \mathbb{N}$. *On note* $\mathbb{Z} := (\mathbb{N} \times \mathbb{N})/_{\mathrm{R}}$ *le quotient de* $\mathbb{N} \times \mathbb{N}$ *modulo* R, *et on l'appelle* l'ensemble des (nombres) entiers relatifs.

Démonstration. La réflexivité de R correspond à la commutativité de + dans $\mathbb{N}$: Pour tous $(a, b) \in \mathbb{N} \times \mathbb{N}$, $(a, b) \sim (a, b) \Leftrightarrow a + b = b + a$. La symétrie de R se démontre similairement :

$$(a, b) \sim (c, d) \Leftrightarrow a + d = b + c \Leftrightarrow c + b = d + a \Leftrightarrow (c, d) \sim (a, b).$$

Enfin, montrons la transitivité ; pour cela, supposons $(a, b) \sim (c, d)$ et $(c, d) \sim (e, f)$. Alors

$$(a + f) + (c + d) = (a + d) + (c + f) = (b + c) + (d + e) = (b + e) + (c + d)$$

où les première et troisième égalités changent l'ordre des termes, et la seconde utilise la définition de R. On en déduit $a + f = b + e$ par simplification, et donc $(a, b) \sim (e, f)$. Ainsi, R est transitive. □

Dans la suite, nous dénoterons par $[(a, b)]$ la classe d'équivalence de $(a, b) \in \mathbb{N} \times \mathbb{N}$ (au lieu de $C_{(a,b)}$).

Proposition 2.66. *On considère sur* $\mathbb{Z}$ *l'opération binaire* $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$*, appelée* addition dans $\mathbb{Z}$*, et donnée par*

$$[(a, b)] + [(c, d)] = [(a + c, b + d)]\,. \tag{2.67}$$

Cette application est bien définie, et munit $\mathbb{Z}$ *d'une structure de groupe abélien, d'élément neutre* $[(0, 0)]$*, et où l'inverse pour* $+$ *d'un élément* $[(a, b)]$*, noté* $-[(a, b)]$*, est donné par* $-[(a, b)] := [(b, a)]$.

Démonstration. Remarquons d'abord que dans la formule (2.67), on utilise qu'un représentant (a, b) de la classe $[(a, b)]$ a été choisi, et idem pour $[(c, d)]$ (comparez avec la Remarque 2.63). Dire que l'application $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ est *bien définie* revient à dire que la formule $[(a + c, b + d)]$ pour $[(a, b)] + [(c, d)]$ *ne dépend pas* des choix des représentants (a, b) et (c, d) choisis. C'est facile à vérifier : supposons $[(a, b)] = [(a', b')]$ et $[(c, d)] = [(c', d')]$. On veut montrer $[(a + c, b + d)] = [(a' + c', b' + d')]$, ce qui se déduit de

$$(a + c) + (b' + d') = (a + b') + (c + d') = (b + a') + (d + c') = (b + d) + (a' + c').$$

Notons que les première et troisième égalités changent l'ordre des termes, alors que la deuxième utilise $[(a, b)] = [(a', b')]$ et $[(c, d)] = [(c', d')]$.

□

On définit une application $i : \mathbb{N} \to \mathbb{Z}$ par $n \mapsto [(n, 0)]$. On vérifie facilement que cette application est injective, et qu'elle est compatible avec l'addition. On dénote désormais simplement n l'élément $[(n, 0)] \in \mathbb{Z}$, et on identifie ainsi $\mathbb{N}$ avec l'ensemble des éléments de $\mathbb{Z}$ de cette forme. L'opposé de $n \in \mathbb{N}$ (c'est-à-dire l'inverse pour $+$) est l'élément $[(0, n)]$, que nous noterons simplement $-n$. Bien sûr, on a $-(-n) = -[(0, n)] = [(n, 0)] = n$. En résumé, si on identifie $[(a, b)]$ avec $a - b$, on retrouve l'ensemble $\mathbb{Z}$ étudié à l'école.

Comme dernière remarque sur la construction de $\mathbb{Z}$, notons qu'on peut définir la multiplication sur $\mathbb{Z}$ de la façon suivante. Nous laissons au lecteur le soin de vérifier que la formule utilisée est *bien définie*. Elle s'inspire bien sûr du calcul $(a - b)(c - d) = (ac + bd) - (ad + bc)$.

Définition 2.68. On définit une opération binaire $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, $(x, y) \mapsto xy$ par la formule

$$[(a, b)][(c, d)] = [(ac + bd, ad + bc)]\,.$$

On l'appelle *la multiplication dans* $\mathbb{Z}$.

Pour décrire les propriétés de l'addition et de la multiplication sur $\mathbb{Z}$, on introduit la structure suivante.

Définition 2.69. Soit $(A, +, \cdot)$ un ensemble A munit de deux opérations binaires

$$A \times A \xrightarrow{+} A,\ \ (a, b) \mapsto a + b \quad \text{et} \quad A \times A \xrightarrow{\cdot} A,\ \ (a, b) \mapsto a \cdot b \ \ (\text{noté souvent } ab)\,,$$

appelées *addition* et *multiplication*, respectivement. On dit que $(A, +, \cdot)$ est *un anneau commutatif unitaire* si les conditions suivantes sont satisfaites :

(a) $(A, +)$ est un groupe abélien ;

(b) La multiplication est associative et commutative ;

(c) La multiplication est distributive sur l'addition : pour tous $a, b, c \in A$, on a $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$;

(d) La multiplication admet un élément neutre $1 \in A$.

Proposition 2.70. *Avec l'addition et la multiplication définies ci-dessus,* $(\mathbb{Z}, +, \cdot)$ *est un anneau commutatif unitaire. L'élément neutre pour l'addition est* $0 = [(0, 0)]$*, et l'élément neutre pour la multiplication est* $1 = [(1, 0)]$.

Démonstration. Nous omettons cette preuve un peu fastidieuse, dont le début a déjà été fait à la Proposition 2.66 ; la suite est similaire, et le lecteur dispose de tout les éléments nécessaires pour la conduire lui-même. □

Notation 2.71. Soit $(A, +, \cdot)$ un anneau commutatif unitaire. Alors l'élément neutre pour l'addition est noté 0, est l'élément neutre pour la multiplication est noté 1. Tous deux sont uniques. De même, un inverse de $a \in A$ pour l'addition est unique, et est noté $-a$.

Définition 2.72. Soit A un anneau commutatif unitaire. On dit que $a \in A$ est *inversible* s'il admet un inverse pour la multiplication, c'est-à-dire s'il existe $x \in A$ avec $a \cdot x = 1$. Dans ce cas, il est facile de vérifier qu'un tel x est unique. On l'appelle *l'inverse de a* et on le note a^{-1}.

Exemple 2.73. Dans l'anneau $\mathbb{Z}$, les seuls éléments inversibles sont 1 et -1. On le montre facilement un utilisant la définition de la multiplication dans $\mathbb{N}$ et $\mathbb{Z}$, ou en utilisant l'ordre, comme corollaire de la Proposition 2.74.

Les principaux exemples d'anneaux qui seront rencontrés cette année sont l'anneau des entiers $\mathbb{Z}$, les corps $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$, ainsi que les anneaux de polynômes. L'anneau $\mathbb{Z}$ sera étudié beaucoup plus en détail dans le cours d'Arithmétique. La relation d'ordre total sur $\mathbb{N}$ s'étend en une relation d'ordre total sur $\mathbb{Z}$, définie par

$$\text{pour tous } x, y \in \mathbb{Z}, \text{ on pose } x \leqslant y \;\Leftrightarrow\; y - x \in \mathbb{N}.$$

La vérification qu'il s'agit bien d'un ordre total est faite en TD. On résume sans démonstration les propriétés de cet ordre sur $\mathbb{Z}$.

Proposition 2.74. *La relation d'ordre sur $\mathbb{Z}$ a les propriétés suivantes.*

(a) Pour tous $x, y, z \in \mathbb{Z}$, on a $x \leqslant y \;\Leftrightarrow\; x + z \leqslant y + z$.

(b) Pour tous $x, y, z \in \mathbb{Z}$ avec $z > 0$, on a $x \leqslant y \;\Leftrightarrow\; xz \leqslant yz$.

(c) Pour tous $x, y, z \in \mathbb{Z}$ avec $z < 0$, on a $x \leqslant y \;\Leftrightarrow\; xz \geqslant yz$.

(d) Soit $A \subset \mathbb{Z}$. Alors les conditions suivantes sur A sont équivalentes :

- *A est non vide et minoré (il existe $w \in \mathbb{Z}$ avec $w \leqslant x$ pour tout $x \in A$), et*
- *A admet un minimum.*

Définition 2.75. Soit A un anneau commutatif unitaire et $x, y \in A$. On dit que y *divise* x (ou que y *est un diviseur de* x) s'il existe $z \in A$ avec $y \cdot z = x$. On note $y|x$ le fait que y divise z, et l'élément z est souvent noté $z = x : y$ à l'école. On appelle *factorisation de* $x \in A$ toute expression de x comme produit fini d'éléments $y_1, \ldots, y_n \in A$; on introduit pour cela la notation suivante :

$$x = y_1 \cdot \ldots \cdot y_n =: \prod_{k=1}^{n} y_k \,.$$

Dans ce cas, on dit que chaque y_k est un *facteur* de ce produit. Par convention, un produit vide (donc un produit avec aucun facteur) est égal à 1.

Définition 2.76. On dit que $n \in \mathbb{N}$ est *un (nombre) premier* s'il possède exactement deux diviseurs.

Exemples 2.77. (a) Si n est premier, ses seuls diviseurs sont 1 et n. Donc 1 n'est pas premier (il n'a qu'un seul diviseur dans $\mathbb{N}$) et 0 n'est pas premier (il a une infinité de diviseurs).

(b) La liste ordonnée des nombres premiers commence par $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, \ldots$.

Théorème 2.78. *Tout nombre entier $n \geqslant 2$ est un produit de nombres premiers. De plus, une telle factorisation de n en produit de nombres premiers est unique (à l'ordre des facteurs près).*

Exemples 2.79.

Démonstration de 2.78. On va se contenter ici de démontrer l'existence d'une factorisation d'un entier n en premiers, par récurrence (forte) sur n. Soit donc $\mathcal{P}$ la propriété portant sur les éléments de $\{n \in \mathbb{N} \;;\; n \geqslant 2\}$, où $\mathcal{P}(n)$ est l'affirmation que n peut s'écrire comme produit de nombres premiers.

(1) *Initialisation.* Il est clair que $\mathcal{P}(2)$ est vraie puisque 2 est premier.

(2) *Itération.* Soit $n \in \mathbb{N}$, et supposons $\mathcal{P}(k)$ vraie pour tout entier k tel que $2 \leqslant k \leqslant n$. Considérons $n + 1$, pour lequel on distingue deux cas :

- Si $n+1$ est premier, on a terminé.
- Si $n+1$ n'est pas premier, alors il existe donc deux entiers a, b tels que $2 \leqslant a, b \leqslant n$ et $n+1 = ab$. Mais, par hypothèse de récurrence, a et b sont produits de nombres premiers, donc $n+1$ est produit de nombres premiers.

Ainsi, $\mathcal{P}(n+1)$ est vraie. Par le Théorème 2.31 (avec initialisation en $n = 2$), $\mathcal{P}(n)$ est vraie pour tout élément $n \geqslant 2$. □

Rappelons la définition de la valeur absolue $|b|$ de $b \in \mathbb{Z}$, vue en TD : $|b| = \begin{cases} b & \text{si } b \geqslant 0, \\ -b & \text{si } b < 0. \end{cases}$

Théorème 2.80 (Division euclidienne dans $\mathbb{Z}$)**.** *Soient $a, b \in \mathbb{Z}$ deux entiers relatifs, avec $b \neq 0$. Il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que*

$$a = bq + r, \quad \text{et} \quad 0 \leqslant r < |b|\,.$$

Démonstration. Nous omettons la démonstration, qui s'appuie sur la Proposition 2.46. Elle sera étudiée dans le cours d'Arithmétique. □

Cette division est celle que l'on apprend à l'école primaire, quand on effectue des divisions posées de nombre entiers, avec reste. Si on enlève la condition $0 \leqslant r < |b|$, alors il existe une infinité de couples (q, r) tels que $a = bq + r$.

Définition 2.81. Dans le Théorème 2.80, on dit que le couple (q, r) s'obtient à partir de a et b par *division euclidienne*. Le nombre b est appelé *le diviseur*, le nombre q est *le quotient* et le nombre r est *le reste*.

Exemple 2.82.

Il est facile de vérifier que si $n \in \mathbb{N}^*$ et si $d \in \mathbb{N}$ divise n, alors $d \leqslant n$: en effet, on alors $n = d + d(n-1)$. On en déduit que si $m, n \in \mathbb{N}$, l'ensemble $A = \{d \in \mathbb{N}\,;\, d|m \text{ et } d|n\}$ est fini. Comme il est non vide (car $1 \in A$), il admet un maximum par la Proposition 2.46. D'autre part, comme dans $\mathbb{Z}$ on a $(-1)(-1) = 1$, on vérifie facilement que $d|n$ est équivalent à $d|(-n)$. La définition suivante a donc un sens.

Définition 2.83. Soient $m, n \in \mathbb{Z}$, avec $m \neq 0$ ou $n \neq 0$. On appelle *plus grand diviseur commun de m et n* le nombre

$$\text{pgcd}(m, n) = \max\{d \in \mathbb{N}\,;\, d|m \text{ et } d|n\}\,.$$

On dit que *les nombres m et n sont premiers entre eux* si $\text{pgcd}(m, n) = 1$.

Exemples 2.84.

Proposition 2.85. *Soient $a, b \in \mathbb{Z}$ avec $b \neq 0$, et soient q et r le quotient et le reste de la division de a par b, donc $a = bq + r$ avec $|r| < b$. Alors on a* $\text{pgcd}(a, b) = \text{pgcd}(b, r)$.

Démonstration. On vérifie facilement par double inclusion l'égalité suivante :

$$\{d \in \mathbb{N}\,;\; d|a \text{ et } d|b\} = \{d \in \mathbb{N}\,;\; d|b \text{ et } d|r\}$$

Ces ensembles finis étant égaux, leur maxima sont aussi égaux. □

En itérant ce procédé, on obtient un algorithme efficace pour calculer $\text{pgcd}(a, b)$, appelé *algorithme d'Euclide*.

Exemple 2.86. On souhaite calculer pgcd(2640, 768). On effectue les divisions euclidiennes suivantes

$$2640 = 768 \cdot 3 + 336$$
$$768 = 336 \cdot 2 + 96$$
$$336 = 96 \cdot 3 + 48$$
$$96 = 48 \cdot 2 + 0$$

et on en déduit pgcd(2640, 768) = pgcd(768, 336) = pgcd(336, 96) = pgcd(96, 48) = pgcd(48, 0) = 48.

Nous énonçons sans démonstration le résultat suivant, qui sera démontré en Arithmétique.

Lemme 2.87 (Lemme de Gauß)**.** *Soient $a, b, c \in \mathbb{Z}$ avec $a \neq 0$. Supposons que* pgcd$(a, b) = 1$ *et a divise bc. Alors a divise c.*

2.3. Les nombres rationnels

Nous avons construit l'ensemble des nombres entiers relatifs $\mathbb{Z}$ à partir des nombres entiers naturels $\mathbb{N}$ dans le but de pouvoir effectuer des soustractions de la forme $a - b$ sans devoir se soucier si $a \geqslant b$. Nous avons veillé à ce que l'on ait une inclusion $\mathbb{N} \subset \mathbb{Z}$ compatible avec les opérations d'addition et de multiplication et la relation d'ordre (en fait, nous nous sommes aidés de l'addition et de la multiplication de $\mathbb{N}$ et de leurs propriétés pour définir celles de $\mathbb{Z}$ et démontrer leurs propriétés).

Similairement, nous construisons les nombres rationnels $\mathbb{Q}$ à partir de $\mathbb{Z}$ dans le but de pouvoir effectuer des divisions de la forme $a : b$ si $b \neq 0$, sans devoir se soucier si b divise a. Nous souhaitons donc avoir une inclusion $\mathbb{Z} \subset \mathbb{Q}$, et étendre la somme et la multiplication de $\mathbb{Z}$ à $\mathbb{Q}$, de telle sorte que si $b \in \mathbb{Q}$ est non-nul, alors b admet un inverse b^{-1}. En d'autres termes, nous souhaitons que $\mathbb{Q}$ soit *un corps commutatif*. Cette notion a été vue en Analyse 1, nous la rappelons ici.

Définition 2.88. Un anneau commutatif unitaire $(A, +, \cdot)$ est appelé *un corps commutatif* si $0 \neq 1$ et si tout élément non-nul admet un inverse multiplicatif : autrement dit, aux conditions (a), (b), (c) et (d) de la Définition 2.69 on ajoute la condition

(e) On a $0 \neq 1$, et tout $a \in A$ avec $a \neq 0$ est inversible : il existe $b \in A$ avec $ab = 1$.

La construction de $\mathbb{Q}$ à partir de $\mathbb{Z}$ est vraiment du même type que celle de $\mathbb{Z}$ à partir de $\mathbb{N}$, tout en étant un peu plus technique ; nous la traitons brièvement seulement. Soit $\mathbb{Z}^* = \mathbb{Z} \smallsetminus \{0\}$. On va considérer des paires $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$, où la paire (a, b) représentera le résultat de la division de a par b (noté $a \cdot b^{-1}$ ou $\frac{a}{b}$).

Lemme 2.89. *On considère sur $\mathbb{Z} \times \mathbb{Z}^*$ la relation* R *définie par*

$$\forall (a, b) \in \mathbb{Z} \times \mathbb{Z}^*, \forall (c, d) \in \mathbb{Z} \times \mathbb{Z}^*, (a, b) \sim (c, d) \iff ad = bc\,.$$

Alors R *est une relation d'équivalence sur $\mathbb{Z} \times \mathbb{Z}^*$. On note $\mathbb{Q} := (\mathbb{Z} \times \mathbb{Z}^*)/_{\mathrm{R}}$ le quotient de $\mathbb{Z} \times \mathbb{Z}^*$ modulo* R*, et on l'appelle* l'ensemble des nombres rationnels.

Démonstration. La démonstration est similaire à celle du Lemme 2.65, en utilisant cette fois les propriétés de la multiplication dans $\mathbb{Z}$. Nous la laissons en exercice. □

Évidemment, vous avez déjà appris à l'école à manipuler la somme et l'addition dans $\mathbb{Q}$. Les définitions des opérations ci-dessous correspondent aux formules bien connues $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ et $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$.

Proposition 2.90. *On considère sur $\mathbb{Q}$ les opérations binaires $\mathbb{Q} \times \mathbb{Q} \xrightarrow{+} \mathbb{Q}$, appelée* addition (dans $\mathbb{Q}$)*, et $\mathbb{Q} \times \mathbb{Q} \xrightarrow{\cdot} \mathbb{Q}$, appelée* multiplication (dans $\mathbb{Q}$)*, définies par*

$$[(a, b)] + [(c, d)] = [(ad + bc, bd)] \quad \text{et} \quad [(a, b)] \cdot [(c, d)] = [(ac, bd)]\,. \tag{2.91}$$

Ces applications sont bien définies, et munissent $\mathbb{Q}$ d'une structure de corps commutatif, avec les propriétés suivantes :

(a) *Le zéro de $\mathbb{Q}$ est la classe $0 := [(0, 1)]$, et l'unité de $\mathbb{Q}$ est la classe $1 := [(1, 1)]$.*

(b) *L'inverse additif de $[(a, b)]$ est $-[(a, b)] := [(-a, b)] = [(a, -b)]$.*

(c) *On a $[(a, b)] \neq 0 \iff a \neq 0$, et dans ce cas l'inverse multiplicatif de $[(a, b)]$ est donné par*

$$[(a, b)]^{-1} := [(b, a)]\,.$$

Démonstration. Nous omettons aussi la preuve, qui n'est pas difficile mais un peu longue ; elle s'appuie bien sûr fortement sur les propriétés de l'addition et de la multiplication dans $\mathbb{Z}$. À titre d'exemple, faisons le point (c). Si $[(a,b)] = 0$, cela signifie donc $(a,b) \sim (0,1)$, donc $a \cdot 1 = b \cdot 0$ dans $\mathbb{Z}$, ce qui revient bien à $a = 0$. Enfin, si $(a,b) \in \mathbb{Z} \times \mathbb{Z}^*$ avec $a \neq 0$, alors $[(a,b)] \cdot [(b,a)] = [(ab,ab)] = [(1,1)] = 1$, donc on a bien $[(a,b)]^{-1} = [(b,a)]$. Notons que la deuxième égalité ci-dessus suit de la relation $(m,m) \sim (1,1)$ dans $\mathbb{Z} \times \mathbb{Z}^*$, valable quelque soit $m \in \mathbb{Z}^*$. □

Lemme 2.92. *Tout élément de $\mathbb{Q}$, vu comme classe d'équivalence, admet un unique représentant de la forme (m,n) avec $n \in \mathbb{N}^*$ et* $\mathrm{pgcd}(m,n) = 1$. *Un $(m,n) \in \mathbb{Z} \times \mathbb{N}^*$ avec* $\mathrm{pgcd}(m,n) = 1$ *est dit* réduit *ou* irréductible.

Démonstration. Soit $[(a,b)] \in \mathbb{Q}$. Commençons par démontrer l'existence d'un représentant réduit : si $a = 0$, alors $(a,b) \sim (0,1)$, avec $1 \in \mathbb{N}^*$ et $\mathrm{pgcd}(0,1) = 1$. Si $a \neq 0$, soit $m = \mathrm{pgcd}(a,b)$ Il existe donc $a', b' \in \mathbb{Z}^*$ avec $a = a'm$ et $b = b'm$. Alors $(a,b) \sim (a',b')$ avec $\mathrm{pgcd}(a',b') = 1$. Si $b' \in \mathbb{N}^*$, alors (a',b') est réduit. Sinon, $(a,b) \sim (-a',-b')$ et $(-a',-b')$ est réduit. Pour démontrer l'unicité, il suffit de montrer que si (a,b) et (c,d) sont tous deux réduits avec $(a,b) \sim (c,d)$, alors $(a,b) = (c,d)$. On a en particulier $b, d \in \mathbb{N}^*$ et $ad = bc$, donc b divise ad. Comme $\mathrm{pgcd}(a,b) = 1$, b divise d dans $\mathbb{N}$ par le Lemme de Gauß 2.87. De même, d divise b dans $\mathbb{N}$, donc $b = d$. De $ad = bc$ on déduit alors $a = c$. Ainsi $(a,b) = (c,d)$. □

Proposition 2.93. *L'application $i : \mathbb{Z} \to \mathbb{Q}$ définie par $m \mapsto [(m,1)]$ est injective, et est compatible avec l'addition et la multiplication.*

Démonstration.

□

Définition 2.94. La classe d'équivalence $[(a,b)] \in \mathbb{Q}$ d'un élément $(a,b) \in \mathbb{Z} \times \mathbb{Z}^*$ est dénotée $\frac{a}{b} := [(a,b)]$. On dit que $\frac{a}{b}$ est *une fraction*, dont a est *le numérateur* et b est *le dénominateur*. Une fraction de la forme $\frac{a}{1}$ est notée simplement a.

Par définition, la fraction $\frac{a}{b} \in \mathbb{Q}$ désigne la classe d'équivalence $[(a,b)]$ représentée par (a,b). Pour tout $c \in \mathbb{Z}^*$, on a $(a,b) \sim (ac,bc)$, ce qui se traduit par $\frac{a}{b} = \frac{ac}{bc}$. On retrouve ainsi les nombres rationnels que l'on connait bien, avec leur addition et multiplication, et les règles de calcul usuelles, par exemple

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}, \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}, \quad -\left(\frac{a}{b}\right) = \frac{-a}{b} = \frac{a}{-b}, \quad \text{et} \quad \left(\frac{x}{y}\right)^{-1} = \frac{y}{x} \ (\text{si } y \neq 0).$$

Par la Proposition 2.93, il existe une bijection de $\mathbb{Z}$ avec l'image de $i : \mathbb{Z} \to \mathbb{Q}$, donnée par

$$i(\mathbb{Z}) = \{\tfrac{a}{b} \in \mathbb{Q} \ ; \ b = 1\} = \{\tfrac{c}{d} \in \mathbb{Q} \ ; \ d|c\}\,.$$

Il est usuel de ne pas distinguer $\mathbb{Z}$ de $i(\mathbb{Z})$, ce qui est compatible avec la notation $a = \frac{a}{1}$ donnée dans la notation ci-dessus. Finalement, il faut encore montrer que $\mathbb{Q}$ possède un ordre total compatible avec celui de $\mathbb{Z}$, ce qui fait l'objet d'un exercice.

Théorème 2.95. *L'ensemble $\mathbb{Q}$ des nombres rationnels est dénombrable.*

Démonstration. Dénotons $\mathbb{Q}_{>0} = \{x \in \mathbb{Q} \ ; \ x > 0\}$ l'ensemble des nombres rationnels positifs. Il suffit de démontrer que $\mathbb{Q}_{>0}$ est dénombrable. En effet, si on a une bijection $f : \mathbb{N} \to \mathbb{Q}_{>0}$, alors on montre facilement que

$$g : \mathbb{N} \to \mathbb{Q}, \quad g(n) = \begin{cases} 0 & \text{si } n = 0, \\ f(\frac{n+1}{2}) & \text{si } n \text{ est impair}, \\ -f(\frac{n}{2}) & \text{si } n \text{ est pair} \end{cases}$$

est aussi une bijection. Pour construire une bijection $f : \mathbb{N} \to \mathbb{Q}_{>0}$, on peut placer toutes les fractions irréductibles de la forme $\frac{a}{b}$ avec $a, b \in \mathbb{N}^*$ sur un arbre binaire dont la racine est $1 = \frac{1}{1}$, et où chaque sommet

$\frac{a}{b}$ a deux descendants : $\frac{a}{a+b}$ à gauche, et $\frac{a+b}{b}$ à droite. On montre que chaque fraction irréductible $\frac{m}{n} \in Q_{>0}$ apparait exactement une fois dans l'arbre. On peut dénombrer ses sommets en comptant de haut en bas et de gauche à droite, établissant ainsi une bijection entre $\mathbb{N}$ et $\mathbb{Q}_{>0}$.

□

2.4. Les nombres réels

Les nombres rationnels ont été construits à partir de $\mathbb{Z}$ en introduisant des inverses multiplicatifs, ce qui permet de faire dans $\mathbb{Q}$ des divisions par n'importe quel nombre non nul. Si l'on souhaite utiliser les nombres pour mesurer des longueurs, on se rend compte que les rationnels ne suffisent pas : il n'existe pas de $\mathbb{Q}$ de nombre dont le carré est 2, même si on peut en trouver des approximations arbitrairement proches dans $\mathbb{Q}$. Cela a conduit les mathématiciens à rechercher une construction d'un corps totalement ordonné contenant $\mathbb{Q}$, et satisfaisant à *l'axiome de la borne supérieure* : c'est le corps des nombres réels $\mathbb{R}$. Il existe plusieurs constructions de $\mathbb{R}$ équivalentes, mais c'est au-delà des objectifs de ce cours ; citons la construction par *coupures de Dedekind*, et la construction par *suites de Cauchy dans* $\mathbb{Q}$ *modulo les zéro-suites*.

Dans la pratique, on utlise des approximations arbitarirement bonnes des nombres réels par des rationnels, car il n'est pas possible de décrire un nombre réel arbitraire par une expression numérique finie. L'une des notations couremment utilisée est l'écriture décimale d'un nombre réel, à l'aide d'une suite $(a_i)_{i\in\mathbb{N}}$ dans $\mathbb{Z}$, avec $a_0 \in \mathbb{Z}$, $0 \leqslant a_i \leqslant 9$ pour tout $i \geqslant 1$, et telle que pour tout $i \in \mathbb{N}$, il existe $j > i$ avec $a_j \neq 9$:

$$a_0, a_1a_2a_3a_4 \ldots := a_0 + \sum_{i=1}^{\infty} \frac{a_i}{10^i} \in \mathbb{R} \ . \tag{2.96}$$

Sous les conditions sur la suite $(a_i)_{i\geqslant 1}$ données, cette somme infinie (on appelle cela une *série*) *converge*, donc définit bien un nombre réel, et tout nombre réel peut s'écrire sous cette forme de façon unique. Si on s'interesse à une approximation à 10^{-n} près, on s'arrête à la n-ème décimale : on considère le nombre rationnel

$$a_0, a_1 \ldots a_n s = a_0 + \sum_{i=1}^{n} \frac{a_i}{10^i} \in \mathbb{Q} \ .$$

On peut toujours représenter un nombre rationnel sous forme décimale. Les nombres rationnels sont caractérisés par un développement périodique.

Exemple 2.97.

L'étude du corps des nombres réels $\mathbb{R}$ a débuté dans le Chapitre 1 du cours d'Analyse 1, et se poursuivra dans les cours d'Analyse suivants (où on montrera en particulier la convergence des séries de la forme (2.96) donnée ci-dessus). Mentionnons le théorème suivant, dont nous esquissons une démonstration.

Théorème 2.98. *L'ensemble des nombres réels* $\mathbb{R}$ *n'est pas dénombrable.*

Esquisse de démonstration. La fonction $g : \mathbb{R} \to (0, 1)$ définie par $g(x) = \frac{1}{1+e^{-x}}$ est une bijection entre $\mathbb{R}$ et l'intervalle ouvert $(0, 1)$. Il suffit donc de montrer que l'intervalle $(0, 1)$ n'est pas dénombrable.

□

Chapitre 3

Le corps des nombres complexes

Le corps $\mathbb{Q}$ des nombres rationnels a été construit à partir des entiers relatifs pour permettre la division par n'importe que nombre. Le corps des nombres réels $\mathbb{R}$ a été construit pour *compléter* $\mathbb{Q}$, c'est-à-dire pour inclure $\mathbb{Q}$ dans un corps ordonné qui satisfasse à l'axiome de la borne supérieure. Le corps des nombres complexes, quant'à lui, est construit pour inclure $\mathbb{R}$ dans un corps dans le quel n'importe quel nombre admet une racine carrée. Ce n'est en effet pas le cas dans $\mathbb{R}$: si $m \in \mathbb{R}$, alors $\{x \in \mathbb{R} \ ; \ x^2 = m\}$ est vide si $m < 0$, ce qui revient à dire que l'équation $x^2 = m$ n'a aucune solution dans $\mathbb{R}$. On voudrait construire un corps qui contient $\mathbb{R}$ et dans lequel une telle équation a toujours une solution. Le corps des nombres complexes $\mathbb{C}$ a cette propriété. Les nombres complexes ont fait leur première apparition documentée au 16ème siècle, dans les travaux de l'italien Gerolamo Cardano.

3.1. Construction du corps des nombres complexes

3.1.1. Remarques sur les corps commutatifs

Lemme 3.1. *Soit K un corps commutatif, de zéro $0 \in K$ et d'unité $1 \in K$. On a les propriétés suivantes :*

(a) *Pour tout $a \in K$, on a l'égalité $0 \cdot a = 0$.*

(b) *Pour tous $a, b \in K$, on a l'équivalence $(a \cdot b = 0) \Leftrightarrow (a = 0 \text{ ou } b = 0)$.*

Démonstration.

□

Définition 3.2. Soit $(L, +, \cdot)$ un corps, d'unité $1 \in L$, et soit $K \subset L$ un sous-ensemble. On dit que K est *un sous-corps de L* si les conditions suivantes sont satisfaites :

(a) Pour tous $a, b \in K$, on a $a + b \in K$ et $a \cdot b \in K$;

(b) Si $a \in K$ alors $-a \in K$, et si de plus $a \neq 0$ alors $a^{-1} \in K$;

(c) On a $1 \in K$.

Remarque 3.3. Si K est un sous-corps de L, alors grâce à la condition (a), les opérations de L se restreignent à des opérations binaires sur K :

$$K \times K \xrightarrow{+} K, \quad (a, b) \mapsto a + b \text{ (somme dans } L),$$

$$K \times K \xrightarrow{\cdot} K, \quad (a, b) \mapsto a \cdot b \text{ (multiplication dans } L).$$

Il est facile de vérifier qu'avec ces opérations, $(K, +, \cdot)$ est aussi un corps, de même zéro, de même unité que L.

Définition 3.4. Soient K et L deux corps commutatifs. On dit qu'une application $f : K \to L$ est *un homomorphisme de corps* si elle est compatible à l'addition, à la multiplication, et si elle préserve l'unité : autrement dit, f satisfait aux trois conditions suivantes :

(a) Pour tous $a, b \in K$, on a $f(a + b) = f(a) + f(b)$.

(b) Pour tous $a, b \in K$, on a $f(a \cdot b) = f(a) \cdot f(b)$.

(c) On a $f(1_K) = 1_L$, où $1_K \in K$ et $1_L \in L$ sont les unités.

On dit que $f : K \to L$ est un *isomorphisme de corps* s'il existe un homomorphisme de corps $g : L \to K$ avec $g \circ f = \mathrm{id}_K$ et $f \circ g = \mathrm{id}_L$. Lorsque $K = L$, un isomorphisme de corps $K \to K$ est appelé *un automorphisme du corps K*.

Exemple 3.5. Si K est un sous-corps de L, alors l'inclusion $K \to L$ est un homomorphisme de corps. Par exemple, $\mathbb{Q}$ est un sous-corps de $\mathbb{R}$, et l'inclusion $\mathbb{Q} \to \mathbb{R}$ est un homomorphisme de corps.

Remarque 3.6. On verra en TD que les autres conditions qu'on s'attend à trouver dans la définition d'un homomorphisme de corps découlent toutes de (a), (b) et (c) : par exemple, on a $f(0_K) = 0_L$ et $f(-a) = -f(a)$ pour tout $a \in K$. Qu'en est-il de l'inverse ? Si $a \neq 0$, on voudrait vérifier l'égalité $f(a^{-1}) = \big(f(a)\big)^{-1}$ (qui est en effet vraie), mais pourquoi a-t-on $f(a) \neq 0$ dans ce cas ? Le lemme suivant répond à cette question.

Lemme 3.7. *Soit $f : K \to L$ un homomorphisme de corps commutatifs. Alors f est injectif, et son image $f(K) \subset L$ est un sous-corps de L.*

Démonstration.

□

Remarque 3.8. On verra en TD qu'un homomorphisme de corps est un isomorphisme de corps si et seulement s'il est bijectif.

3.1.2. Propriétés souhaitées pour le corps des nombres complexes

On souhaite construire un corps commutatif K avec les propriétés suivantes :

(A) Le corps $\mathbb{R}$ est un sous-corps de K ;

(B) L'équation $x^2 = m$ a une solution dans K pour tout $m \in \mathbb{R}$.

Nous allons procéder comme souvent en mathématiques :

- On suppose qu'un tel corps existe, et on étudie ses propriétés élémentaires ;
- On s'inspire de ces propriétés pour trouver une définition d'un tel corps.

Supposons donc qu'un tel corps commutatif K, satisfaisant aux conditions (A) et (B), existe. Remarquons que la condition (B) est équivalente à la condition suivante :

(B') Il existe un élément $i \in K$ avec $i^2 = -1$.

Démonstration de (B) $\Leftrightarrow$ (B'). Il est clair que (B) $\Rightarrow$ (B') (il suffit de choisir une solution i de l'équation $x^2 = -1$). Montrons donc (B') $\Rightarrow$ (B). Soit $m \in \mathbb{R}$ donné, et définissons

$$z = \begin{cases} \sqrt{m} & \text{si } m \geqslant 0, \\ \sqrt{-m} \cdot i & \text{si } m < 0. \end{cases}$$

Si $m \geqslant 0$, on a bien sûr $z^2 = (\sqrt{m})^2 = m$; dans le deuxième cas, si $m < 0$, on a, bien sûr $-m \geqslant 0$, donc $\sqrt{-m}$ est défini et la formule $z = \sqrt{-m} \cdot i$ a un sens ; en utilisant les règles de calculs valables dans un corps commutatif, on obtient $z^2 = (\sqrt{-m} \cdot i)^2 = (\sqrt{-m})^2 \cdot (i)^2 = (-m) \cdot (-1) = m$. □

Supposons donc choisi un élément $i \in K$ avec $i^2 = -1$. Si $a, b \in \mathbb{R}$, on a $a, b \in K$ (car $\mathbb{R} \subset K$), et on peut former, à l'aide des opérations dans K l'élément $a + b \cdot i \in K$. Désormais, on omet le point dans la notation pour le produit, par exemple on écrit $a + bi$ au lieu de $a + b \cdot i$. Alors on a les propriétés suivantes pour les éléments de K de la forme $a + bi$ avec $a, b \in \mathbb{R}$:

(C) Pour $a, b \in \mathbb{R}$, on a

$$\Big(a + bi = 0 \text{ dans } K\Big) \;\Leftrightarrow\; \Big((a, b) = (0, 0) \text{ dans } \mathbb{R} \times \mathbb{R}\Big).$$

(D) Dans K, on a pour tous $a, b, c, d \in \mathbb{R}$ l'égalité

$$(a + bi) + (c + di) = (a + c) + (b + d)i\,.$$

(E) Dans K, on a pour tous $a, b, c, d \in \mathbb{R}$ l'égalité

$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i\,.$$

(F) L'application $\varphi : \mathbb{R} \times \mathbb{R} \to K$ définie par $\varphi(a, b) = a + bi$ est injective.

Démonstration de ces assertions.
(C) Supposons que $a + bi = 0$ dans K. Supposons par l'absurde que $b \neq 0$. On obtient

$$a + bi = 0 \;\Leftrightarrow\; i = -b^{-1}a \in \mathbb{R}$$

ce qui est absurde car -1 n'a pas de racine dans $\mathbb{R}$. Donc $b = 0$. Mais alors $bi = 0$ par le Lemme 3.1(a), et

$$a = a + 0 = a + bi = 0\,.$$

Ainsi, on a montré $(a + bi = 0) \Rightarrow \big((a, b) = (0, 0)\big)$. Réciproquement, si $a = b = 0$, alors $bi = 0$ par le Lemme 3.1(a), donc $a + bi = 0 + 0 = 0$.

□

3.1.3. La définition du corps $\mathbb{C}$

On n'a pas encore d'exemple d'un corps K satisfaisant aux conditions (A) et (B) de la Section 3.1.2. Cependant, la condition (F) ci-dessus nous dit que si un tel corps existe, on a aura forcément une injection $\varphi : \mathbb{R} \times \mathbb{R} \to K$. Les conditions (D) et (E) nous disent alors comment on peut munir $\mathbb{R} \times \mathbb{R}$ d'une addition et d'un produit compatibles avec ceux de ce K hypothétique. En fait, il s'avère que cela fait de $\mathbb{R} \times \mathbb{R}$ un corps ! Ici, le lecteur est censé sauter de joie. Ces observations motivent la définition suivante.

Définition 3.9. On munit l'ensemble $\mathbb{R} \times \mathbb{R}$ des opérations suivantes :

$$(\mathbb{R} \times \mathbb{R}) \times (\mathbb{R} \times \mathbb{R}) \xrightarrow{+} \mathbb{R} \times \mathbb{R}\,, \quad (a, b) + (c, d) = (a + c, b + d)\,,$$

$$(\mathbb{R} \times \mathbb{R}) \times (\mathbb{R} \times \mathbb{R}) \xrightarrow{\cdot} \mathbb{R} \times \mathbb{R}\,, \quad (a, b)(c, d) = (ac - bd, ad + bc)\,.$$

Théorème 3.10. *L'ensemble* $(\mathbb{R} \times \mathbb{R}, +, \cdot)$ *est un corps commutatif, dont le zéro est* $(0, 0)$ *et l'unité est* $(1, 0)$. *L'opposé de* (a, b) *est* $-(a, b) := (-a, -b)$, *et si* $(a, b) \neq (0, 0)$, *son inverse est*

$$(a, b)^{-1} := \left(\tfrac{a}{a^2+b^2}, -\tfrac{b}{a^2+b^2}\right)\,.$$

Il vérifie de plus les propriétés suivantes :

(a) *L'application* $f : \mathbb{R} \to \mathbb{R} \times \mathbb{R}$ *définie par* $f(a) = (a, 0)$ *est un homomorphisme de corps.*

(b) *On a* $(0, 1)^2 = -(1, 0)$.

Démonstration. La démonstration est un exercice routinier qui se base sur les propriétés de l'addition et de la multiplication dans $\mathbb{R}$. Faisons par exemple l'associativité de la multiplication.

□

Définition 3.11. Le corps $(\mathbb{R}\times\mathbb{R}, +, \cdot)$ donné par le Théorème 3.10 est appelé *le corps des nombres complexes*. On le dénote par $\mathbb{C}$. Un élément $z \in \mathbb{C}$ est appelé *un nombre complexe*.

Remarquons que l'assertion (b) du théorème correspond à la propriété (B'), elle-même équivalente à (B). L'assertion (a) va nous permettre de redéfinir $\mathbb{R}$ comme un sous-corps de $\mathbb{C}$, ce qui reviendra à dire que $\mathbb{C}$ satisfait à la condition (A). Le corps $K = \mathbb{C}$ satisfait donc aux hypothèses de la Section 3.1.2.

Définition 3.12. On définit sur $\mathbb{C}$ une loi externe, $\mathbb{R}\times\mathbb{C} \to \mathbb{C}$, appelée *action de* $\mathbb{R}$ *sur* $\mathbb{C}$, par

$$\mathbb{R}\times\mathbb{C} \to \mathbb{C}\,, \quad \big(\lambda, (a,b)\big) \mapsto \lambda(a,b) := (\lambda a, \lambda b)\,.$$

Remarque 3.13. Rappelons que par le Théorème 3.10, on a un homomorphisme de corps $f : \mathbb{R} \to \mathbb{C}$ défini par $f(\lambda) = (\lambda, 0)$. Si $\lambda \in \mathbb{R}$ et $(a,b) \in \mathbb{C}$, on remarque que

$$f(\lambda)(a,b) = (\lambda,0)(a,b) = (\lambda a, \lambda b) = \lambda(a,b)\,.$$

Donc l'action définie en 3.12 ci-dessus correspond à considérer $\lambda \in \mathbb{R}$ comme le nombre complexe $f(\lambda) = (\lambda, 0)$, puis à le multiplier avec (a,b) dans $\mathbb{C}$. Les propriétés suivantes de l'action se démontrent facilement, en utilisant la formule $\lambda(a,b) = (\lambda a, \lambda b)$ et la définition de l'addition et la multiplication dans $\mathbb{C}$: pour tous $\lambda, \mu \in \mathbb{R}$ et tous $(a,b), (c,d) \in \mathbb{C}$, on a

$$\begin{aligned}(\lambda+\mu)(a,b) &= \lambda(a,b) + \mu(a,b)\\ \lambda\big(\mu(a,b)\big) &= (\lambda\mu)(a,b)\\ \lambda\big((a,b)+(c,d)\big) &= \lambda(a,b) + \lambda(c,d)\\ 1(a,b) &= (a,b)\,.\end{aligned}$$

Notations 3.14. Dans le corps $\mathbb{C}$, introduisons les notations suivantes :

$$1_{\mathbb{C}} = (1,0) \quad \text{et} \quad i = (0,1)\,.$$

L'élément $1_{\mathbb{C}}$ est bien sûr l'unité dans le corps $\mathbb{C}$, et i satisfait à $i^2 = -1_{\mathbb{C}}$. Alors, à l'aide de l'action de $\mathbb{R}$ sur $\mathbb{C}$, on voit que

$$(a,b) = a(1,0) + b(0,1) = a1_{\mathbb{C}} + bi\,. \tag{3.15}$$

L'assertion (b) du Théorème 3.10 nous dit qu'il existe un homomorphisme de corps $f : \mathbb{R} \to \mathbb{C}$, forcément injectif par le Lemme 3.7. Son image $f(\mathbb{R})$ est un sous-corps de $\mathbb{C}$, et

$$f : \mathbb{R} \to f(\mathbb{C}) = \{(a,b) \in \mathbb{C}\ ;\ b = 0)\} = \{a1_{\mathbb{C}} \in \mathbb{C}\ ;\ a \in \mathbb{R}\}$$

est un isomorphisme de corps. D'habitude, on identifie $\mathbb{R}$ avec le sous-corps $\{a1_{\mathbb{C}}\ ;\ a \in \mathbb{R}\}$ de $\mathbb{C}$; du coup, on écrit a au lieu de $a1_{\mathbb{C}}$, et on peut réécrire l'expression (3.15) sous la forme

$$(a,b) = a + bi\,.$$

On peut résumer la discussion du paragraphe 3.1.2, à l'aide de l'action et des notations ci-dessus, par la proposition suivante.

Proposition 3.16. *Soit* $\mathbb{C}$ *le corps de nombres complexes. Si on identifie* $\mathbb{R}$ *avec le sous-corps de* $\mathbb{C}$ *donné par* $\{a := a1_{\mathbb{C}} \in \mathbb{C}\ ;\ a \in \mathbb{R}\}$ *alors tout nombre complexe* $(a,b) \in \mathbb{C}$, $a, b \in \mathbb{R}$, *s'écrit de façon unique sous la forme*

$$(a,b) = a + bi\,,$$

appelée forme cartésienne *du nombre complexe* (a,b). *En représentant un nombre complexe sous cette forme, on a les formules suivantes, où* $a, b, c, d \in \mathbb{R}$ *:*

Le zéro	$a + bi = 0_{\mathbb{C}} \Leftrightarrow a = b = 0_{\mathbb{R}}$
L'unité	$a + bi = 1_{\mathbb{C}} \Leftrightarrow a = 1_{\mathbb{R}}$ et $b = 0_{\mathbb{R}}$
L'addition	$(a+bi) + (c+di) = (a+c) + (b+d)i$
La multiplication	$(a+bi)(c+di) = (ac-bd) + (ad+bc)i$
L'opposé	$-(a+bi) = (-a) + (-b)i = -a - bi$
L'inverse si $(a+bi \neq 0)$	$(a+bi)^{-1} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i$

Démonstration. Il s'agit d'une reformulation du Théorème 3.10 en utilisant la notation $(a, b) = a + bi$. Comme expliqué dans la Section 3.1.2, une fois le corps commutatif $\mathbb{C}$ construit, toutes ces formulent découlent des axiomes de corps, la seule règle à retenir étant $i^2 = -1$. □

Notation 3.17. Avec la convention où $\mathbb{R}$ est un sous-corps de $\mathbb{C}$, on a $0_{\mathbb{R}} = 0_{\mathbb{C}}$, que l'on note simplement 0, et $1_{\mathbb{R}} = 1_{\mathbb{C}}$, que l'on note simplement 1. Dans la suite, on utilise souvent la notation $z = a + bi \in \mathbb{C}$ pour un nombre complexe, où on sous-entendra toujours que $a, b \in \mathbb{R}$.

Définition 3.18. Soit $z = a + bi \in \mathbb{C}$.

- On appelle *partie réelle de* z et on note $\mathrm{re}(z)$ le nombre réel a.
- On appelle *partie imaginaire de* z et on note $\mathrm{im}(z)$ le nombre réel b.

En particulier, on a $z = \mathrm{re}(z) + \mathrm{im}(z)i$ pour tout $z \in \mathbb{C}$.

Exemples 3.19.

Lemme 3.20. *Tout nombre réel $a \in \mathbb{R} \subset \mathbb{C}$ non nul possède exactement deux racines carrées dans $\mathbb{C}$, à savoir*

$$\begin{cases} \sqrt{a} \quad \text{et} \quad -\sqrt{a} & \text{si } a > 0, \text{ et} \\ (\sqrt{-a})i \quad \text{et} \quad -(\sqrt{-a})i & \text{si } a < 0\,. \end{cases}$$

Démonstration. Si $a > 0$, alors z est une racine carrée de a si et seulement si $\frac{1}{\sqrt{a}}z$ est une racine carrée de 1. Si $a < 0$, alors z est une racine carrée de a si et seulement si $\frac{1}{\sqrt{-a}}z$ est une racine carrée de -1. Il suffit dont de vérifier que 1 et -1 on exactement deux racines carrées dans $\mathbb{C}$. On fait le cas de -1, le cas de 1 étant similaire. On a résout

$$(a + bi)^2 = -1 \;\Leftrightarrow\; \begin{cases} a^2 - b^2 = -1 \\ 2ab = 0 \end{cases} \;\Leftrightarrow\; \begin{cases} a^2 + 1 = b^2 \\ a = 0 \quad \text{ou} \quad b = 0\,. \end{cases}$$

Or on ne peut pas avoir $b = 0$, car alors la première équation $a^2 + 1 = b^2 = 0$ n'a pas de solution $a \in \mathbb{R}$. On a donc $a = 0$, et la première équation devient $b^2 = 1$, donc $b = 1$ ou $b = -1$. Ainsi, -1 a exactement deux racines carrées, ce sont i et $-i$. □

Remarque 3.21. L'unité $1 \in \mathbb{C}$ est déterminée de façon unique dans $\mathbb{C}$, et il en est de même de l'opposé de l'unité -1 (c'est en fait le cas pour n'importe quel corps). Par contre, un nombre complexe de carré -1, ou l'unité imaginaire, n'est pas déterminé de façon unique par la structure de corps : on peut choisir i ou $-i$. C'est cette liberté qui nous permet de définir la *conjugaison* dans $\mathbb{C}$.

Définition 3.22. On appelle *conjugaison* l'application

$$c : \mathbb{C} \to \mathbb{C}\,, \quad a + bi \mapsto a - bi\,.$$

Si $z = a + bi$, l'élément $c(z) = a - bi$ est appelé *le conjugué (complexe) de* z, et est habituellement noté

$$\overline{z} = \overline{a + bi} = a - bi\,.$$

Théorème 3.23. *La conjugaison $c : \mathbb{C} \to \mathbb{C}$ est un automorphisme du corps $\mathbb{C}$. Elle satisfait aux conditions suivantes :*

(a) *La conjugaison est involutive, c'est-à-dire que $c \circ c = \mathrm{id}_{\mathbb{C}}$, et*

(b) *Pour tout $z \in \mathbb{C}$, on a $z \in \mathbb{R} \;\Leftrightarrow\; \overline{z} = z$.*

(c) *Pour tout $z \in \mathbb{C}$, on a $z + \overline{z} = 2\mathrm{re}(z)$ et $z - \overline{z} = 2\,\mathrm{Im}(z)i$.*

Démonstration. La propriété (a) est évidente, et on en déduit que c est bijective, car elle admet une application réciproque : elle-même ! La propriété (b) est claire car si $z = a + bi$, alors $z \in \mathbb{R} \Leftrightarrow b = 0$. Or $z - \overline{z} = 2bi$, donc $b = 0 \Leftrightarrow \overline{z} = z$. Il reste donc à vérifier que c est un homomorphisme de corps, c'est-à-dire qu'il satisfait aux conditions de la Définition 3.4, à savoir

$$\overline{w + z} = \overline{w} + \overline{z}, \quad \overline{w \cdot z} = \overline{w} \cdot \overline{z} \quad \text{et} \quad \overline{1} = 1$$

pour tous $w = a + bi$ et $z = c + di \in \mathbb{C}$. Ce sont des calculs faciles laissés en exercice.

□

Définition 3.24. Soit $z = a + bi \in \mathbb{C}$. On définit *le module* de z comme le nombre réel

$$|z| := \sqrt{a^2 + b^2} \in \mathbb{R} .$$

Le module définit une application $\mathbb{C} \to \mathbb{R}, \quad z \mapsto |z|$.

Remarque 3.25. Si $z = a + bi \in \mathbb{C}$ est en fait un nombre réel (donc si $b = 0$), le module $|z|$ de z est égal à la valeur absolue de z vu comme nombre réel : tous deux sont égaux à $\sqrt{a^2}$. Il n'y a donc pas de conflit de notation. De plus, si $\lambda \in \mathbb{R}$ et $w \in \mathbb{C}$, on la formule $|\lambda w| = |\lambda||w|$. On le voit directement, mais c'est aussi un cas pariculier de la Proposition 3.27. On en déduit $|-w| = |w|$, qui rappelle la propriété similaire pour la valeur absolue.

Exemples 3.26.

Proposition 3.27. *L'application $\mathbb{C} \to \mathbb{R}, \quad z \mapsto \overline{z}$ satisfait aux conditions suivantes. Pour tous $w, z \in \mathbb{C}$, on a*

- **(a)** $|z|^2 = z\overline{z}$ *et donc* $|z| = \sqrt{z\overline{z}}$.
- **(b)** $(|z| = 0) \Leftrightarrow (z = 0)$.
- **(c)** $|\mathrm{re}(z)| \leqslant |z|$, $|\mathrm{im}(z)| \leqslant |z|$ *et* $|\overline{z}| = |z|$.
- **(d)** $|wz| = |w||z|$ *et* $|z^{-1}| = |z|^{-1}$.
  En particulier le module se restreint à un homomorphisme de groupes $(\mathbb{C}^*, \cdot) \to (\mathbb{R}^*, \cdot)$.
- **(e)** $|w + z| \leqslant |w| + |z|$ *(inégalité triangulaire).*
- **(f)** $||w| - |z|| \leqslant |w - z|$ *(inégalité triangulaire inverse).*

Démonstration. Les points (a) et (c) sont des calculs très simples laissés en exercice.
(b) On a $(|z| = 0) \Leftrightarrow (|z|^2 = 0) \Leftrightarrow (a^2 + b^2 = 0) \Leftrightarrow (a = b = 0) \Leftrightarrow (z = 0)$.
(d) On a $|wz| = \sqrt{wz(\overline{wz})} = \sqrt{wz(\overline{w})(\overline{z})} = \sqrt{w\overline{w}z\overline{z}} = \sqrt{w\overline{w}}\sqrt{z\overline{z}} = |w||z|$, où les première et dernière égalités utilisent le point (a).
(e) C'est la propriété la plus difficile à vérifier. D'abord, on a

$$|w + z|^2 = (w + z)\overline{(w + z)} = (w + z)(\overline{w} + \overline{z}) = |w|^2 + w\overline{z} + \overline{w}z + |z|^2 = |w|^2 + 2\mathrm{re}(w\overline{z}) + |z|^2 . \qquad (3.28)$$

La dernière égalité utilise $w\overline{z} + \overline{w}z = 2\mathrm{re}(w\overline{z})$: on la déduit du Théorème 3.23.(c) en remarquant que $\overline{w}z = \overline{w\overline{z}}$ (car c est un homomorphisme de corps). Or, en utilisant les points (c) et (d) de cette proposition, on trouve

$$2\mathrm{re}(w\overline{z}) \leqslant 2|w\overline{z}| = 2|w||\overline{z}| = 2|w||z| .$$

On juxtaposant (3.28) avec cette dernière inégalité, on obtient

$$|w + z|^2 \leqslant |w|^2 + 2|w||z| + |z|^2 = (|w| + |z|)^2 .$$

La fonction $\sqrt{-} : \mathbb{R}^+ \to \mathbb{R}$ étant croissante, on en déduit le résultat.
(f) Si on considère $w = (w - z) + z$, on déduit de (e) que

$$|w| = |(w - z) + z| \leqslant |w - z| + |z|, \quad \text{donc } |w| - |z| \leqslant |w - z|.$$

De même, en partant de $z = -(w - z) + w$ on trouve

$$|z| = |-(w - z) + w| \leqslant |-(w - z)| + |w| = |w - z| + |w|, \quad \text{donc } |z| - |w| \leqslant |w - z|.$$

De ces deux inégalités on déduit $||w| - |z|| \leqslant |w - z|$. □

3.2. Forme trigonométrique et représentation géométrique

La fonction exponentielle réelle $\exp_{\mathbb{R}} : \mathbb{R} \to \mathbb{R}$, $x \mapsto e^x$, a déjà été partiellement étudiée au lycée et dans le cours d'Analyse 1. Il existe plusieurs définitions possibles de la fonction exponentielle, la plus utile étant celle donnée par *une série* : pour $x \in \mathbb{R}$, on considère la suite réelle $(S_k)_{k\in\mathbb{N}}$ définie par $S_k = \sum_{n=0}^{k} \frac{x^n}{n!}$. On peut montrer que cette suite converge, et on dénote par

$$e^x := \sum_{n=0}^{\infty} \frac{x^n}{n!} := \lim_{k\to\infty} S_k$$

sa limite. Alors $x \mapsto e^x$ définit une fonction continue, notée ici $\exp_{\mathbb{R}} : \mathbb{R} \to \mathbb{R}$, et dont les propriétés essentielles ont été donnée dans le cours d'Analyse 1. Les *séries*, c'est-à-dire les expressions de la forme d'une somme infinie comme ci-dessus, et leur convergence, ne seront étudiées qu'en deuxième année.

3.2.1. La fonction exponentielle complexe

Il existe aussi une version complexe de l'exponentielle, dont la définition est analogue à celle de l'exponentielle réelle donnée ci-dessus. Nous ne pouvons pas, avec les moyens à disposition dans ce cours, démontrer les résultats qui suivent, mais nous les présentons ici pour donner un aperçu de l'origine de la *formule d'Euler* reliant l'exponentielle complexe et les fonction trigonométriques.

Lemme 3.29. *Pour tout $z \in \mathbb{C}$, la série $\sum_{n=0}^{\infty} \frac{z^n}{n!}$ converge (absolument) dans $\mathbb{C}$. On note e^z sa somme :*

$$e^z := \sum_{n=0}^{\infty} \frac{z^n}{n!}\,. \tag{3.30}$$

Remarquons que pour $z \in \mathbb{C}$, la notion du nombre *e à la puissance z* n'a pas de sens algébrique ; ici e^z est juste une notation pour la somme de la série.

Définition 3.31. On appelle *exponentielle complexe* l'application

$$\exp_{\mathbb{C}} : \mathbb{C} \to \mathbb{C}\,, \quad z \mapsto \exp_{\mathbb{C}}(z) = e^z\,.$$

Les fonctions trigonométriques *cosinus* et *sinus* ont été définies en Analyse 1 à l'aide de la notion d'angle. En fait, on peut aussi les définir en terme de séries convergentes, données par les formules suivantes : pour tout $x \in \mathbb{R}$,

$$\cos(x) = \sum_{n=0}^{\infty} (-1)^n \frac{x^{2n}}{(2n)!} \quad \text{et} \quad \sin(x) = \sum_{n=0}^{\infty} (-1)^n \frac{x^{2n+1}}{(2n+1)!}\,.$$

Si on décompose la somme pour e^{ix} en ses parties réelles et imaginaires, on trouve pour $x \in \mathbb{R}$:

$$e^{ix} = \sum_{n=0}^{\infty} \frac{(ix)^n}{n!} = \sum_{n=0}^{\infty} i^n \frac{x^n}{n!} = \sum_{k=0}^{\infty} (-1)^k \frac{x^{2k}}{(2k)!} + i \sum_{k=0}^{\infty} (-1)^k \frac{x^{2k+1}}{(2k+1)!} = \cos(x) + i\sin(x)\,.$$

Il faut bien sûr démontrer qu'un telle manipulation de sommes infinies convergentes est possible, mais c'est bien le cas ici. La proposition suivante résume les propriétés de l'exponentielle complexe. Sa démonstration suit facilement de résultats généraux sur la convergence des séries.

Proposition 3.32. *L'exponentielle complexe $\exp_{\mathbb{C}} : \mathbb{C} \to \mathbb{C}$, $z \mapsto \exp_{\mathbb{C}}(z) = e^z$ a les propriétés suivantes :*

- **(a)** *Pour tous $w, z \in \mathbb{C}$, on a $e^{w+z} = e^w \cdot e^z$.*
- **(b)** *Pour tout $z \in \mathbb{C}$, on a $e^{\overline{z}} = \overline{e^z}$.*
- **(c)** *Pour tout $x \in \mathbb{R}$, $\exp_{\mathbb{C}}(x) = \exp_{\mathbb{R}}(x)$, et donc la notation e^x n'est pas ambigüe.*
- **(d)** *Pour tout $x \in \mathbb{R}$, on a $\mathrm{re}(e^{ix}) = \cos(x)$ et $\mathrm{im}(e^{ix}) = \sin(x)$ ou, de façon équivalente,*

$$\boxed{e^{ix} = \cos(x) + i\sin(x).}$$

Cette égalité s'appelle Formule d'Euler.

Remarque 3.33. On déduit donc des propriétés (a), (c) et (d) que pour tout $z = a + bi \in \mathbb{C}$, on a

$$e^{a+bi} = e^a\big(\cos(b) + i\sin(b)\big)\,. \tag{3.34}$$

Si les fonctions exponentielles réelles, cosinus et sinus ont été définies par ailleurs, on peut utiliser cette formule comme *définition* de l'exponentielle complexe.

Corollaire 3.35. *Les fonctions trigonométriques* cosinus *et* sinus *satisfont aux formules suivantes : pour tous* $x, y \in \mathbb{R}$*, on a*

$$\cos(x+y) = \cos(x)\cos(y) - \sin(x)\sin(y), \quad \text{et}$$
$$\sin(x+y) = \cos(x)\sin(y) + \sin(x)\cos(y).$$

Démonstration.

□

3.2.2. Le groupe unitaire

Nous avons défini la structure de groupe en 2.47. Voici deux exemples fondamentaux.

Proposition 3.36. *Soit* $(K, +, \cdot)$ *un corps.*

(a) $(K, +)$ *est un groupe abélien, appelé* le groupe additif *du corps* K*. Son élément neutre est* $0 \in K$*.*

(a) $(K \smallsetminus \{0\}, \cdot)$ *est un groupe abélien, appelé* le groupe multiplicatif *du corps* K*. Son élément neutre est* $1 \in K \smallsetminus \{0\}$*. On le dénote par* $(K^\times, \cdot)$*.*

Démonstration. Celui suit immédiatement de la définition d'un corps commutatif. Rappelons que dans un corps, on exige $0 \neq 1$, ce qui implique en particulier que $\{0\} \subsetneq K$ et donc que $K^\times \neq \emptyset$. □

Définition 3.37. Soit $(G, \star)$ un groupe, d'élément neutre $e \in G$. On dit qu'un sous-ensemble $H \subset G$ est *un sous-groupe* de G si H satisfait aux conditions suivantes :

(c) H est stable pour l'opération $\star$: pour tous $x, y \in H$, on a $x \star y \in H$.

(b) H est stable pour l'inverse : pour tout $x \in H$, on on $x^{-1} \in H$.

(c) On a $e \in H$.

La proposition suivante découle immédiatement des définitions.

Proposition 3.38. *Soit* $(G, \star)$ *un groupe, d'élément neutre* $e \in G$*, et soit* $H \subset G$ *un sous-groupe. Alors la restriction de l'opération de* G *à* H*,*

$$H \times H \to H, \quad (x, y) \mapsto x \star y,$$

munit H *d'une structure de groupe, d'élément neutre* e*, et qui est abélien si* G *est abélien.*

Définition 3.39. Soient $(G, \star)$ et $(G', \star)$ deux groupes. Une application $f : G \to G'$ est *un homomorphisme de groupes* si

$$f(x \star y) = f(x) \star f(y) \text{ pour tout } x, y \in G.$$

Remarque 3.40. Les autres propriétés qu'on est en droit d'attendre d'un homomorphisme de groupes, à savoir qu'il préserve l'élément neutre et l'inverse, suivent de la définition ci-dessus.

Exemples 3.41.

Proposition 3.42. *Le sous-ensemble* $U(1) = \{z \in \mathbb{C} \ ; \ |z| = 1\}$ *est un sous-groupe du groupe multiplicatif* $(\mathbb{C}^\times, \cdot)$.

Démonstration. Cela se déduit aisément des propriétés du module données dans la Proposition 3.27.(d) :

□

Définition 3.43. Le sous-groupe $U(1)$ de $(\mathbb{C}^\times, \cdot)$ est appelé *le groupe unitaire de rang* 1.

Proposition 3.44. *L'application* $\mathbb{R} \to \mathbb{C}$, $x \mapsto e^{ix} = \cos(x) + i\sin(x)$ *est un homomorphisme surjectif du groupe additif* $(\mathbb{R}, +)$ *sur le groupe unitaire* $U(1)$. *Elle est périodique de période* 2π *: pour tous* $x, y \in \mathbb{R}$, *on a*

$$(e^{ix} = e^{iy}) \Leftrightarrow (\exists k \in \mathbb{Z}, x - y = 2\pi k)\,.$$

Démonstration.

□

Corollaire 3.45 (Formules de Moivre)**.** *Pour tout* $x \in \mathbb{R}$ *et tout* $n \in \mathbb{N}$, *on a*

$$\cos(nx) + i\sin(nx) = \big(\cos(x) + i\sin(x)\big)^n\,.$$

Démonstration. Cela suit de la formule suivante : si $f : (G, \star) \to (G', \star)$ est un homomorphisme de groupes, alors on peut montrer facilement par récurrence sur n que pour tout $x \in G$, on a $f(x^{\star n}) = \big(f(x)\big)^{\star n}$. Ici $x^{\star n}$ est défini par récurrence, en posant $x^{\star 0} = e$, l'élément neutre, et $x^{\star(n+1)} := x^{\star n} \star x$. Dans le cas présent, on applique cette remarque à l'homomorphisme de groupes $(\mathbb{R}, +) \to (U(1), \cdot)$, avec les notations habituelles : si $x \in \mathbb{R}$, alors $nx = x^{+n}$, et si $y \in (\mathbb{C}, \cdot)$, $y^n = y^{\cdot n}$. La formule de Moivre correspond à $e^{i(nx)} = \big(e^{ix}\big)^n$.

□

Remarque 3.46. La formule de Moivre permet de déduire des formules pour $\cos(nx)$ et $\sin(nx)$. Le cas $n = 2$ est couvert par le Corollaire 3.35 en prenant $x = y$. À titre d'exemple, faisons le cas $n = 3$: on a

$$\begin{aligned}\cos(3x) + i\sin(3x) = \big(\cos(x) + i\sin(x)\big)^3 &= \\ &= \cos(x)^3 + 3\cos(x)^2 i\sin(x) + 3\cos(x)\big(i\sin(x)\big)^2 + \big(i\sin(x)\big)^3 = \\ &= \big(\cos(x)^3 - 3\cos(x)\sin(x)^2\big) + i\big(3\cos(x)^2\sin(x) - \sin(x)^3\big)\,.\end{aligned}$$

On en déduit, en utilisant $\cos(x)^2 + \sin(x)^2 = 1$,

$$\begin{aligned}\cos(3x) &= \cos(x)^3 - 3\cos(x)\sin(x)^2 = \cos(x)\big(1 - 4\sin(x)^2\big)\,,\\ \sin(3x) &= 3\cos(x)^2\sin(x) - \sin(x)^3 = \sin(x)\big(4\cos(x)^2 - 1\big)\,.\end{aligned}$$

C'est un premier exemple de l'utilité des nombres complexes.

3.2.3. Forme trigonométrique

Définition 3.47. On considère sur $\mathbb{R}$ la relation d'équivalence $(x \sim y \bmod 2\pi) \Leftrightarrow (\exists k \in \mathbb{Z}, x - y = 2\pi k)$. Si $x \sim y$, on dit que *x est équivalent à y modulo 2π*. On dénote par $\mathbb{R}/2\pi\mathbb{Z}$ l'ensemble des classes d'équivalence pour cette relation.

On remarque que par la Proposition 3.44, deux nombres réels x et y sont équivalents modulo 2π si et seulement si $e^{ix} = e^{iy}$. Remarquons aussi que si on a $z \in \mathbb{C}$ avec $z \neq 0$, alors

$$\left|\frac{z}{|z|}\right| = \frac{1}{|z|}|z| = 1\,,$$

donc $\frac{z}{|z|} \in U(1)$. Puisque l'application $\mathbb{R} \to U(1)$ donnée par $x \mapsto e^{ix}$ est surjective, il existe $\alpha \in \mathbb{R}$ avec $e^{i\alpha} = \frac{z}{|z|}$.

Définition 3.48. Soit $z \in \mathbb{C}$ avec $z \neq 0$, et soit $\alpha \in \mathbb{R}$ avec $\frac{z}{|z|} = e^{i\alpha}$. On appelle *argument de z* et on note $\arg(z)$ la classe de α modulo 2π.

Définition 3.49. Soit $z \in \mathbb{C}$ avec $z \neq 0$. On peut exprimer z sous la forme

$$z = re^{i\alpha} = r\big(\cos(\alpha) + i\sin(\alpha)\big)$$

où $\alpha \in \arg(z)$ est un représentant de l'argument de z, et $r = |z| \in \{t \in \mathbb{R}\ ;\ t > 0\}$ est le module de z. Cette expression s'appelle *la forme trigonométrique* ou *la forme polaire* de z.

Remarque 3.50. On remarque que par la Proposition 3.44, la forme trigonométrique d'un nombre complexe $z \neq 0$ est *unique* au sens suivant. Supposons que $r, s \in \{t \in \mathbb{R}\ ;\ t > 0\}$ et $\alpha, \beta \in \mathbb{R}$. Alors

$$(re^{i\alpha} = z = se^{i\beta}) \quad \Leftrightarrow \quad (r = |z| = s \quad \text{et} \quad \alpha \sim \beta \bmod 2\pi)\,.$$

En effet, puisque $|e^{i\alpha}| = 1 = |e^{i\beta}|$, on a $r = |re^{i\alpha}| = |se^{i\beta}| = s$, et alors $e^{i\alpha} = \frac{z}{r} = \frac{z}{s} = e^{i\beta}$, donc $a \sim \beta \bmod 2\pi$.

Exemples 3.51.

Les opérations multiplicatives sur $\mathbb{C}$ sont données par des formules faciles à manipuler lorsque les nombres complexes sont donnés sous forme trigonométrique. Commençons par rappeler les formules de passage entre la forme cartésienne $z = a + bi$ et la forme trigonométrique $z = re^{i\alpha}$:

$z = a + bi$	$z = re^{i\alpha} = r\big(\cos(\alpha) + i\sin(\alpha)\big)$
$a = r\cos(\alpha)$ $b = r\sin(\alpha)$	$r = \lvert z\rvert = \sqrt{a^2 + b^2}$ α avec $\begin{cases}\cos(\alpha) = \frac{a}{\sqrt{a^2+b^2}}\\ \sin(\alpha) = \frac{b}{\sqrt{a^2+b^2}}\end{cases}$

Exemples 3.52.

Proposition 3.53. *Soient $w, z \in \mathbb{C}$ avec $w \neq 0 \neq z$, donnés sous forme trigonométrique par*

$$w = re^{i\alpha} \quad \text{et} \quad z = se^{i\beta}\,.$$

Alors on les formules suivantes :

$w \cdot z = (rs)e^{i(\alpha+\beta)}$	$z^{-1} = s^{-1}e^{-i\beta}$	$\frac{w}{z} = \frac{r}{s}e^{i(\alpha-\beta)}$	$w^n = r^n e^{i\alpha n}$

Démonstration. La formule pour wz suit directement des formules $|wz| = |w||z|$ et $e^{i\alpha}e^{i\beta} = e^{i(\alpha+\beta)}$ données par les Propositions 3.27.(d) et 3.32.(a). On en déduit la formule pour z^{-1}, car

$$\left(se^{i\beta}\right)\left(s^{-1}e^{-i\beta}\right) = \left(ss^{-1}\right)e^{i(\beta-\beta)} = 1e^0 = 1\,.$$

La formule pour $\frac{w}{z}$ s'obtient en combinant les deux formules précédentes, et la formule pour w^n s'obtient de la première formule avec $w = z$, par récurrence sur n. □

Remarque 3.54. La forme cartésienne et la forme trigonométrique nous permettent d'interpréter géométriquement les opérations de $\mathbb{C}$ dans le plan complexe, appelé souvent *plan d'Argand* (ou *Argand-Cauchy*, ou encore *Argand-Gauß*).

Corollaire 3.55. *Soit $z = re^{i\alpha}$ un nombre complexe non-nul, et $n \in \mathbb{N}$ avec $n \geqslant 2$. Alors z possède exactement n racines n-èmes dans $\mathbb{C}$, données par*

$$w_k = \sqrt[n]{r} \cdot e^{\frac{\alpha+2\pi k}{n}} \quad \text{pour} \quad k \in \mathbb{N} \text{ avec } 0 \leqslant k \leqslant n-1\,.$$

Démonstration. Pour tout $\ell \in \mathbb{Z}$, posons $w_\ell := \sqrt[n]{r} \cdot e^{\frac{\alpha+2\pi\ell}{n}}$. Par la formule pour w^n du Corollaire 3.53, on a $w_\ell^n = z$, donc w_ℓ est bien une racine n-ème de z. Inversement, si $w = se^{i\beta}$ est une racine n-ème de z, on a

$$s^n e^{i\beta n} = \left(se^{i\beta}\right)^n = re^{i\alpha}\,,$$

donc on a, par la Remarque 3.50,

$$s^n = r \quad \text{et} \quad \exists \ell \in \mathbb{Z} \quad \text{avec} \quad n\beta = \alpha + 2\pi\ell\,.$$

On en déduit qu'il existe $\ell \in \mathbb{Z}$ avec $w = w_\ell$. En conclusion tous les w_ℓ sont des racines n-èmes de z, et toutes les racines sont de ce type. Il reste à montrer que pour tout $\ell \in \mathbb{Z}$, il existe un unique nombre $k \in \mathbb{N}$ avec $0 \leqslant k \leqslant n-1$ et $w_\ell = w_k$. Or, comme $|w_\ell| = |w_k|$, on voit par la Remarque 3.50 que

$$\begin{aligned}(w_\ell = w_k) &\Leftrightarrow \tfrac{\alpha+2\pi\ell}{n} \sim \tfrac{\alpha+2\pi k}{n} \bmod 2\pi \Leftrightarrow \exists m \in \mathbb{Z}\,,\ \tfrac{\alpha+2\pi\ell}{n} - \tfrac{\alpha+2\pi k}{n} = 2\pi m \\ &\Leftrightarrow \exists m \in \mathbb{Z}\,, \ell - k = mn \Leftrightarrow \exists m \in \mathbb{Z}\,, \ell = mn + k\,.\end{aligned}$$

Or la condition $0 \leqslant k \leqslant n-1$ nous dit que k est le reste de la division euclidienne de ℓ par n, donc est bien unique. □

Exemple 3.56. Soit $z = 2 + 2\sqrt{3}i$. Cherchons les racines 3-èmes de z. On le met d'abord sous forme trigonométrique : on trouve $z = 4e^{i\frac{\pi}{3}}$. On a donc les trois racines 3-èmes

$$w_k = \sqrt[3]{4}\, e^{i\left(\frac{\pi}{9} + \frac{2\pi}{3}k\right)},\ k = 0, 1, 2\,.$$

Par opération sur les fractions, on trouve donc

$$w_0 = \sqrt[3]{4}\, e^{i\left(\frac{\pi}{9}\right)},\ \ w_1 = \sqrt[3]{4}\, e^{i\left(\frac{7\pi}{9}\right)} \ \text{ et } \ w_2 = \sqrt[3]{4}\, e^{i\left(\frac{13\pi}{9}\right)}\,.$$

Définition 3.57. Soit $n \in \mathbb{N}$ avec $n \geqslant 1$. On désigne par

$$\mu_n := \{z \in \mathbb{C} \; ; \; z^n = 1\} \subset \mathbb{C}$$

l'ensemble des racines n-èmes de $1 \in \mathbb{C}$. On appelle les éléments de μ_n *les racines n-èmes de l'unité*.

Proposition 3.58. *Soit $n \in \mathbb{N}$ avec $n \geqslant 1$. On a $\mu_n \subset U(1)$, et μ_n est un sous-groupe fini de $U(1)$, de cardinal n. C'est donc aussi un sous-groupe de $(\mathbb{C}^\times, \cdot)$. On le note souvent*

$$\mu_n = \{\zeta_k \; ; \; k \in \mathbb{N} \;\text{ avec }\; 0 \leqslant k \leqslant n-1\},$$

où $\zeta_k = e^{i\frac{2\pi+k}{n}}$ (en particulier, $\zeta_0 = 1$).

Démonstration. On sait par le Corollaire 3.55 que μ_n est de cardinal n. Il faut vérifier que μ_n satisfait aux conditions de la Définition 3.37 :

(a) μ_n est stable pour le produit de $U(1)$, qui est la multiplication dans $\mathbb{C}$: si $z, w \in \mu_n$, alors

$$(zw)^n = z^n w^n = 1 \cdot 1 = 1\,.$$

donc $zw \in \mu_n$ car c'est une racine n-ème de 1.

(b) De même, si $z \in \mu_n$, alors

$$(z^{-1})^n = (z^n)^{-1} = 1^{-1} = 1\,,$$

donc $z^{-1} \in \mu_n$.

(c) Finalement, $1^n = 1$ donc $1 \in \mu_n$. Ainsi, μ_n est bien un sous-groupe de $U(1)$. □

Remarque 3.59. Les racines n-èmes de l'unité sont placées sur les sommets d'un polygone régulier à n arrêtes dans le plan d'Argand, inscrit dans un cercle de centre 0 et de rayon 1. Remarquons que si $w \in \mathbb{C}$ est non-nul, et si w_0 est une racine n-ème de w, alors les racines n-èmes de w sont données par

$$\{w_0\zeta_k \; ; \; k \in \mathbb{N} \;\text{ avec }\; 0 \leqslant k \leqslant n-1\}\,.$$

Les racines n-èmes de w sont aussi placées sur les sommets d'un polygone régulier à n arrêtes, inscrit dans un cercle de centre 0 et de rayon $\sqrt[n]{|w|}$.