Chapitre 1

Structures Algébriques
Construction de $\mathbb{Z}$ et $\mathbb{Q}$

De nombreux ensembles rencontrés en mathématiques ont des propriétés élémentaires communes : par exemple, dans les ensembles de nombres, on peut additionner et multiplier ; certaines fonctions peuvent être ajoutées, multipliées, composées ; etc. On souhaite donc, dans ce chapitre, présenter du vocabulaire permettant de décrire les propriétés élémentaires d'ensembles, lorsque ceux-ci sont munis d'opérations.

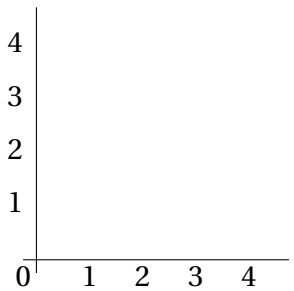
On en profite également pour illustrer l'utilité des relations d'équivalences pour créer de nouveaux ensembles. En l'occurence, $\mathbb{Z}$ et $\mathbb{Q}$; on expliquera alors quelles structures algébriques ces ensembles possèdent.

1.1 Les entiers relatifs

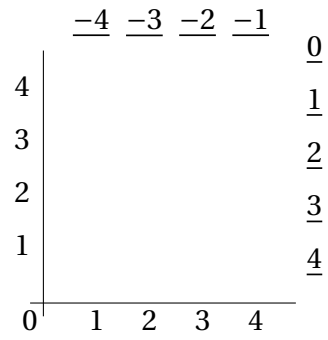
L'ensemble $\mathbb{N}$ étudié dans le chapitre précédent possède un inconvénient : on peut ajouter deux de ses éléments, mais on ne peut pas tous les soustraire les uns aux autres. Par exemple, $4-3$ est une opération qu'on peut effectuer dans $\mathbb{N}$ alors que $3-5$ ne veut rien dire.

En général, si m et n sont deux entiers, l'opération $m-n$ n'a de sens dans $\mathbb{N}$ que si $m \geqslant n$. On souhaite donc créer un ensemble $\mathbb{Z}$, contenant $\mathbb{N}$, dans lequel on peut toujours effectuer l'opération $m-n$ entre deux entiers m et n, même si $m \leqslant n$.

L'ensemble $\mathbb{N}^2$ peut être partitionné en la réunion disjointe des « droites » de pente 1 :



Notre idée, pour « créer » les nombres négatifs est la suivante. L'ensemble de toutes ces droites est appelé $\mathbb{Z}$. La diagonale sera appelée $\underline{0}$; celle immédiatement à droite, partant de $(1,0)$ sera appelée $\underline{1}$; la suivante $\underline{2}$; etc. Celle qui part de $(0,1)$ est appelée $\underline{-1}$; celle immédiatement à gauche, $\underline{-2}$; et ainsi de suite.



Jusqu'à présent, pas de difficulté : il s'agit simplement de donner un nom à des objets. Ce qu'il nous faut vérifier, c'est qu'on peut aussi créer des opérations, notées $\oplus$ et $\otimes$ sur $\mathbb{Z}$, possédant les propriétés usuelles, et telles que la structure additive et multiplicative de $\mathbb{N}$ soit conservée. C'est-à-dire que l'on souhaite que

$$\underline{n} \oplus \underline{m} = \underline{n+m} \qquad \text{et} \qquad \underline{m} \otimes \underline{n} = \underline{n \times m}$$

1.1.1 Construction de $\mathbb{Z}$

On définit $\forall (m,n),(m',n') \in \mathbb{N}^2 \qquad (m,n) \sim (m',n') \iff m'+n = m+n'$

Proposition 1.1.1
$\sim$ est une relation d'équivalence sur $\mathbb{N}^2$.

Preuve : Il s'agit de vérifier que $\sim$ satisfait aux trois propriétés caractérisant une relation d'équivalence.

D'abord, si $(m,n) \in \mathbb{N}^2$, on a $m+n = m+n$ ce qui établit que $(m,n) \sim (m,n)$: $\sim$ est réflexive.

Ensuite, si $(m,n) \sim (m',n')$, on sait que $m'+n = m+n'$. Dans la mesure où l'égalité est une relation symétrique, on a $m+n' = m'+n$. Ceci équivaut à dire que $(m',n') \sim (m,n)$: $\sim$ est symétrique.

Enfin, supposons que $(m,n) \sim (m',n')$ et que $(m',n') \sim (m'',n'')$. Par définition,

$$m'+n = m+n' \qquad \text{et} \qquad m''+n' = m'+n''$$

En ajoutant ces deux égalités membre-à-membre, il vient

$$m'+n+m''+n' = m+n'+m'+n''$$

ou encore $$(m'+n')+(m''+n) = (m'+n')+(m+n'')$$

Les deux membres sont supérieurs à $m'+n'$, donc on a le droit de leur soustraire $m'+n'$, pour obtenir

$$m''+n = m+n''$$

Autrement dit, $(m,n) \sim (m'',n'')$: $\sim$ est transitive. □

Définition 1.1.2
L'ensemble quotient $\mathbb{N}^2/\sim$ est appelé *ensemble des entiers relatifs* et noté $\mathbb{Z}$. Si $(m,n) \in \mathbb{N}^2$, sa classe d'équivalence sera notée $\overline{(m,n)}$. Enfin, pour tout entier n, on notera

$$\underline{n} = \overline{(n,0)}$$

Proposition 1.1.3
L'application $\iota : \begin{array}{ccc} \mathbb{N} & \longrightarrow & \mathbb{Z} \\ n & \longmapsto & \underline{n} \end{array}$ *est injective.*

Preuve : Soient m et n deux entiers tels que $\underline{n} = \underline{m}$. Par définition,

$$\overline{(n,0)} = \overline{(m,0)}$$

ce qui équivaut à dire que

$$m + 0 = n + 0$$

Donc $m = n$ et ι est bien injective. □

On a $\iota(\mathbb{N}) \subset \mathbb{Z}$ et l'injectivité de ι assure que les $(\iota(n))_{n\in\mathbb{N}}$ sont bien distincts deux-à-deux dans $\mathbb{Z}$. Donc on peut considérer (et c'est un abus de notation) que $\mathbb{N} \subset \mathbb{Z}$, puisque les images des éléments de $\mathbb{N}$ par ι sont « bien séparés » dans $\mathbb{Z}$. De fait, par la suite, on considérera que n et $\underline{n}$ sont le même objet si $n \in \mathbb{N}$.

On souhaite maintenant définir une addition $\oplus$ et une multiplication $\otimes$ dans notre nouvel ensemble $\mathbb{Z}$. Et ces opérations doivent prolonger les opérations dans $\mathbb{N}$: il faut que

$$\forall m,n \in \mathbb{N} \qquad \underline{n} \oplus \underline{m} = \underline{m+n} \qquad \text{et} \qquad \underline{n} \oplus \underline{m} = \underline{m \times n}$$

On va définir $\oplus$ et $\otimes$ pour qu'elles fassent juste cela. Donnons-nous deux entiers naturels m et n, ainsi que des couples (a,b) et (c,d) dans $\mathbb{N}^2$, tels que

$$\underline{m} \sim (a,b) \qquad \text{et} \qquad \underline{n} \sim (c,d)$$

c'est-à-dire que $\qquad m + b = a \qquad \text{et} \qquad n + d = c$

Comme m et n sont entiers, on sait que $a \geqslant b$ et $c \geqslant d$ donc on a le droit de calculer $a-b$ et $c-d$ dans $\mathbb{N}$. Par suite,

$$m = a - b \qquad \text{et} \qquad n = c - d$$

de sorte que $\qquad m + n = a + c - (b + d) \qquad \text{et} \qquad mn = ac + bd - ad - bc$

puis $\qquad (m+n) + (b+d) = a + c \qquad \text{et} \qquad mn + (ad + bc) = ac + bd$

c'est-à-dire $\qquad (m+n, 0) \sim (a+c, b+d) \qquad \text{et} \qquad (mn, 0) \sim (ac+bd, ad+bc)$

De manière équivalente, $\qquad \underline{m+n} = \overline{(a+c, b+d)} \qquad \text{et} \qquad \underline{m \times n} = \overline{(ac+bd, ad+bc)}$

Il apparaît donc que la seule manière naturelle de définir la somme et le produit de $\overline{(a,b)}$ par $\overline{(b,c)}$ est la suivante :

$$\overline{(a,b)} \oplus \overline{(b,c)} = \overline{(a+c, b+d)}$$

et

$$\overline{(a,b)} \otimes \overline{(b,c)} = \overline{(ac+bd, ad+bc)}$$

Mais il faut vérifier que la définition est bien posée : est-il bien certain que, si $\overline{(a,b)} = \overline{(a',b')}$ et $\overline{(c,d)} = \overline{(c',d')}$, alors

$$\overline{(a+c,b+d)} \stackrel{?}{=} \overline{(a'+c',b'+d')}$$

et $$\overline{(ac+bd,ad+bc)} \stackrel{?}{=} \overline{(a'c'+b'd',a'd'+b'c')}$$

Le lemme suivant répond à cette question :

Lemme 1.1.4
Soient (a,b), (c,d), (a',b') et (c',d') dans $\mathbb{N}^2$, tels que

$$(a,b) \sim (a',b') \qquad et \qquad (c,d) \sim (c',d')$$

Alors $\quad (a+c,b+d) \sim (a'+b',c'+d') \quad$ *et* $\quad (ac+bd,ad+bc) \sim (a'c'+b'd',a'd'+b'c')$

Preuve : On sait que $\quad a'+b = a+b' \quad$ et $\quad c'+d = c+d'$

En ajoutant membre-à-membre ces deux relations, il vient

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

d'où $$(a+c,b+d) \sim (a'+c',b'+d')$$

Cette partie était facile. Pour le produit, cela se corse si l'on s'y prend mal. Commençons par partir de $a'+b = a+b'$, qu'on multiplie par c pour obtenir

$$bc+a'c = ac+b'c \tag{1}$$

Puis on multiplie $a+b' = a'+b$ par d :

$$ad+b'd = bd+a'd \tag{2}$$

Ensuite, on multiplie $c'+d = c+d'$ par a' :

$$a'c'+a'd = a'd'+ca' \tag{3}$$

Enfin, on multiplie $c+d' = c'+d$ par b' :

$$b'd'+b'c = b'c'+b'd \tag{4}$$

Et on ajoute membre-à-membre les relations (**1**),..., (**4**) :

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

On constate que le même terme $a'c+b'd+a'd+b'c$ est présent dans les deux membres de cette égalité, ce qui permet de le simplifier d'où

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

ce qui signifie exactement que

$$(ac+bd,ad+bc) \sim (a'c'+b'd',a'd'+b'c') \qquad \square$$

Corollaire 1.1.5
Il existe deux applications $\oplus$ et $\otimes$, de $\mathbb{Z}^2$ dans $\mathbb{Z}$, vérifiant

$$\forall (a,b),(c,d) \in \mathbb{N}^2 \qquad \overline{(a,b)} \oplus \overline{(c,d)} = \overline{(a+c,b+d)}$$

et $\quad \forall (a,b),(c,d) \in \mathbb{N}^2 \qquad \overline{(a,b)} \otimes \overline{(c,d)} = \overline{(ac+bd,ad+bc)}$

1.1.2 Structure de groupe additif de $\mathbb{Z}$

Nous allons étudier les propriétés des deux opérations $\oplus$ et $\otimes$ définies sur $\mathbb{Z}$ au paragraphe précédent. Mais avant cela, on présente du vocabulaire général sur les opérations dans un ensembles.

Définition 1.1.6 (Loi de composition interne)
Soit E un ensemble. On appelle *loi de composition interne sur* E toute application $\star : \mathrm{E} \times \mathrm{E} \longrightarrow \mathrm{E}$. En général, au lieu de noter $\star(x, y)$, on écrira $x \star y$.

Le paragraphe précédent montre que $\oplus$ et $\otimes$ sont des lois de composition internes sur $\mathbb{Z}$.

Définition 1.1.7 (Associativité, commutativité, élément neutre)
Soit $(\mathrm{E}, \star)$ un ensemble muni d'un loi de composition interne. On dira que :

- $\star$ est *associative* si, et seulement si,

$$\forall x, y, z \in \mathrm{E} \qquad (x \star y) \star z = x \star (y \star z)$$

- $\star$ est *commutative* si, et seulement si,

$$\forall x, y \in \mathrm{E} \qquad x \star y = y \star x$$

- $\star$ *admet un élément neutre* si, et seulement si, il existe $e \in \mathrm{E}$ tel que

$$\forall x \in \mathrm{E} \qquad x \star e = e \star x = x$$

Proposition 1.1.8
Soit $(\mathrm{E}, \star)$ *un ensemble muni d'une loi de composition interne. S'il y a un élément neutre, celui-ci est unique.*

Preuve : En effet, soient e et e' deux éléments neutres dans E. Puisque e est neutre, on sait que $e \star e' = e'$; et comme e' est neutre, on a $e \star e' = e$. Par suite, $e = e'$. □

Puisque cet élément neutre, quand il existe, est unique, on lui donne un nom particulier. Généralement, 1_{E} ou tout simplement 1 ; quand en plus la loi $\star$ est commutative, il est de coutume de le noter plutôt 0_{E} ou 0.

Définition 1.1.9 (Inverses)
Soit $(\mathrm{E}, \star)$ un ensemble muni d'une loi de composition interne et admettant un élément neutre noté 1. Soit $x \in \mathrm{E}$. On dira que x *est inversible* si, et seulement si, il existe $y \in \mathrm{E}$ tel que $x \star y = y \star x = 1$. Un tel y est appelé *un inverse de* x.

Définition 1.1.10 (Groupes)
Soit $(\mathrm{E}, \star)$ un ensemble muni d'une loi de composition interne. On dira que E est un *groupe* si, et seulement si,

- $\star$ est associative ;
- E admet un élément neutre ;
- tout élément de E est inversible.

Proposition 1.1.11
Soit $(G,\star)$ *un groupe. Si* $x \in G$*, il admet un inverse et celui-ci est unique. On le note* x^{-1} *en général, mais si* G *est commutatif, on le note plutôt* $-x$*.*

Preuve : Soient y et y' deux inverses de x. Par définition,

$$x \star y = y \star x = 1 \qquad \text{et} \qquad x \star y' = y' \star x = 1$$

Puisque 1 est neutre, on a

$$y' = y' \star 1$$

Or,

$$1 = x \star y$$

donc

$$y' = y' \star 1 = y' \star (x \star y)$$

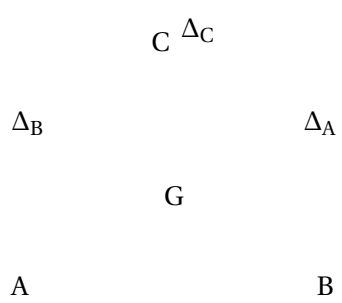
Comme $\star$ est associative,

$$y' = \underbrace{(y' \star x)}_{=1} \star y = 1 \star y = y$$

ce qui prouve que $y' = y$: x admet bien ununique inverse. □

Exemple 1.1.12
Un des exemples fondamentaux de groupes est $\mathbb{Z}$. Démontrer ce fait est l'objectif de ce chapitre et nous le laissons pour plus tard.

En attendant, considérons un autre ensemble qui apparaît en géométrie. Soit ABC un triangle équilatéral. On considère l'ensemble E des applications du plan dans lui-même, laissant ABC invariant. Ce dernier est représenté ci-dessous, ainsi que ses médianes et son centre de gravité G, qui seront utiles pour déterminer les éléments de E.



La loi de composition utilisée sera évidemment la composition des applications. Celle-ci est évidemment interne, puisque si f et g sont dans E, on a

$$f(\text{ABC}) = \text{ABC} \qquad \text{et} \qquad g(\text{ABC}) = \text{ABC}$$

donc

$$f \circ g(\text{ABC}) = f(g(\text{ABC})) = f(\text{ABC}) = \text{ABC}$$

de sorte que

$$\forall f, g \in \text{E} \qquad f \circ g \in \text{E}$$

En outre, on sait déjà que la composition est associative. On peut aussi énumérer les éléments de E. Il y a :

- L'identité, notée Id, qui est d'ailleurs neutre pour E.
- Les rotations r_+ et r_-, de centre G et d'angles respectivement $\frac{2\pi}{3}$ et $-\frac{2\pi}{3}$. Observons d'ailleurs que $r_+ \circ r_- = r_- \circ r_+ = \text{Id}$ donc ces deux éléments de E sont inversibles.

- Les symétries orthogonales s_A, s_B, s_C d'axes respectifs Δ_A, Δ_B, Δ_C. On remarque d'ailleurs que

$$s_A \circ s_A = s_B \circ s_B = s_C \circ s_C = \mathrm{Id}$$

ce qui établit qu'elles sont toutes inversibles.

On peut enfin, pour connaître entièrement la structure de groupe de E, en dresser sa table de Pythagore. Il s'agit d'un tableau donnant tous les résultats de compositions entre éléments de E :

$\circ$	Id	r_+	r_-	s_A	s_B	s_C
Id	Id	r_+	r_-	s_A	s_B	s_C
r_+	r_+	r_-	Id	s_C	s_A	s_B
r_-	r_-	Id	r_+	s_B	s_C	s_A
s_A	s_A	s_B	s_C	Id	r_+	r_-
s_B	s_B	s_C	s_A	r_-	Id	r_+
s_C	s_C	s_A	s_B	r_+	r_-	Id

Cette table est construite de la manière suivante : à la ligne f et colonne g, on place le résultat de la composition $f \circ g$. E est un groupe à 6 éléments.

Théorème 1.1.13 (Calculs d'inverses dans un groupe)
Soit $(G, \star)$ *un groupe. Soient* x *et* y *deux éléments de* G. *Alors*

$$(x \star y)^{-1} = y^{-1} \star x^{-1}$$

En particulier, si G *est commutatif,*

$$-(x+y) = -x - y = -y - x$$

Preuve : C'est une simple vérification, en utilisant l'associativité de $\star$:

$$(x \star y) \star (y^{-1} \star x^{-1}) = ((x \star y) \star y^{-1}) \star x^{-1} = (x \star (\underbrace{y \star y^{-1}}_{=1})) \star x^{-1} = x \star x^{-1} = 1$$

donc $x \star y$ admet bien $y^{-1} \star x^{-1}$ comme inverse. □

Théorème 1.1.14 (Structure de groupe de $\mathbb{Z}$)
$(\mathbb{Z}, \oplus)$ *est un groupe commutatif.*

Preuve : Par construction, la loi $\oplus$ est interne à $\mathbb{Z}$. Vérifions les autres propriétés caractérisant un groupe commutatif.

- **Commutativité** : Soient x et y dans $\mathbb{Z}$. Par définition de $\mathbb{Z} = \mathbb{N}^2/\sim$, il existe des entiers naturels a, b, c et d tels que

$$x = \overline{(a,b)} \qquad \text{et} \qquad y = \overline{(c,d)}$$

D'après le **Corollaire 1.5**,

$$x \oplus y = \overline{(a,b)} \oplus \overline{(c,d)} = \overline{(a+c, b+d)}$$

tandis que $$y \oplus x = \overline{(c,d)} \oplus \overline{(a,b)} = \overline{(c+a, d+b)}$$

Mais l'addition « + » est l'addition dans $\mathbb{N}$; on sait qu'elle est commutative. Donc $x \oplus y = y \oplus x$.

- **Associativité** : Soient x, y et z trois éléments de $\mathbb{Z}$. Puisque $\mathbb{Z} = \mathbb{N}^2/\sim$, il existe des entiers naturels a, b, c, d, e et f tels que

$$x = \overline{(a,b)} \qquad y = \overline{(c,d)} \qquad \text{et} \qquad z = \overline{(e,f)}$$

D'après le **Corollaire 1.5**, on a

$$y \oplus z = \overline{(c,d)} \oplus \overline{(e,f)} = \overline{(c+e, d+f)}$$

puis $$x \oplus (y \oplus z) = \overline{(a,b)} \oplus \overline{(c+e, d+f)} = \overline{(a+(c+e), b+(d+f))}$$

Rappelons que l'addition « + » est l'opération usuelle dans $\mathbb{N}$, dont on sait déjà qu'elle est associative. Donc

$$x \oplus (y \oplus z) = \overline{((a+c)+e, (b+d)+f)}$$

On utilise encore deux fois de suite le **Corollaire 1.5** :

$$x \oplus (y \oplus z) = \overline{(a+c, b+d)} \oplus \overline{(e,f)} = \left(\overline{(a,b)} \oplus \overline{(c,d)}\right) \oplus \overline{(e,f)} = (x \oplus y) \oplus z$$

- **Élément neutre** : Remarquons que $\underline{0}$ est neutre pour $\oplus$. En effet, soit $z \in \mathbb{Z}$; il existe des entiers naturels a et b tels que $z = \overline{(a,b)}$ et d'après le **corollaire 1.15**,

$$\underline{0} \oplus z = \overline{(0,0)} \oplus \overline{(a,b)} = \overline{(a+0, b+0)} = \overline{(a,b)} = z$$

De même, $$z \oplus \underline{0} = z$$

On peut aussi utiliser la commutativité de $\oplus$, déjà démontrée.

- **Existence d'inverses** : Soit $x = \overline{(a,b)} \in \mathbb{Z}$ et posons $x' = \overline{(b,a)}$. On a alors

$$x \oplus x' = \overline{(a,b)} \oplus \overline{(b,a)} = \overline{(b+a, a+b)} = \overline{(0,0)} = \underline{0}$$

puisque $$0 + (b+a) = (a+b) + 0$$

Donc x est inversible, d'inverse x'.

Ceci achève la démonstration. □

> Évidemment, une question naturelle est : « Comment a-t-on deviné quel est l'inverse de x ? » La réponse est simple : on l'a cherché d'abord au brouillon. Il s'agissait de trouver des entiers naturels c et d tels que
>
> $$\overline{(a,b)} \oplus \overline{(c,d)} = \underline{0}$$
>
> c'est-à-dire $$\overline{(a+c, b+d)} = \overline{(0,0)}$$
>
> ou encore $$a + c = b + d$$
>
> C'est là qu'on voit que $c = b$ et $d = a$ font l'affaire.

1.1.3 Relation d'ordre sur $\mathbb{Z}$

Comme expliqué à la **proposition 1.11**, l'inverse d'un élément x d'un groupe commutatif est noté $-x$ et on l'appelle *opposé de x* plutôt qu'*inverse de x*. On a déjà noté

$$\mathbb{N} = \{\underline{n} \mid n \in \mathbb{N}\} \subset \mathbb{Z}$$

Posons aussi $\mathbb{N}^\star = \mathbb{N} \setminus \{\underline{0}\}$ $-\mathbb{N} = \{-\underline{n} \mid n \in \mathbb{N}\}$ $-\mathbb{N}^\star = -\mathbb{N} \setminus \{\underline{0}\}$

Proposition 1.1.15
Soit $(a,b) \in \mathbb{N}^2$. *On a*

$$\overline{(a,b)} = \underline{0} \iff a = b$$

$$\overline{(a,b)} \in \mathbb{N}^\star \iff a > b$$

et

$$\overline{(a,b)} \in (-\mathbb{N}^\star) \iff a < b$$

Preuve : On a successivement

$$\begin{aligned} \overline{(a,b)} = \underline{0} &\iff (a,b) \sim (0,0) \iff 0 + b = a + 0 \\ &\iff a = b \end{aligned}$$

De même

$$\begin{aligned} \overline{(a,b)} \in \mathbb{N}^\star &\iff \exists n \in \mathbb{N} \qquad (a,b) \sim (n,0) \\ &\iff \exists n \in \mathbb{N}^\star \qquad n + b = a \\ &\iff a > b \end{aligned}$$

La dernière proposition se démontre encore de la même manière. Ou bien, on peut utiliser le fait que $-\overline{(a,b)} = \overline{(b,a)}$ et donc

$$\overline{(a,b)} \in (-\mathbb{N}^\star) \iff \underbrace{-\overline{(a,b)}}_{=\overline{(b,a)}} \in \mathbb{N}^\star \iff b > a \qquad \square$$

Mais, étant donnés deux entiers naturels a et b, on sait qu'on peut toujours les comparer et qu'on est nécessairement dans l'un des trois cas ci-dessus. Ceux-ci sont mutuellement exclusifs. Par suite,

Corollaire 1.1.16
Les ensembles $\{\underline{0}\}$, $\mathbb{N}^\star$ *et* $-\mathbb{N}^\star$ *forment une partition de* $\mathbb{Z}$.

En d'autres termes, un entier relatif est soit nul, soit dans $\mathbb{N}^\star$, soit dans $-\mathbb{N}^\star$.

Si l'on regarde le dessin se trouvant au début du chapitre, il est presque naturel de vouloir séparer les « droites » de $\mathbb{N}^2$ en trois catégories : la diagonale $\{\underline{0}\}$, les droites en-dessous de la diagonale (celles-ci forment l'ensemble $\mathbb{N}^\star$) et les droites au-dessus de la diagonale (et qui forment $-\mathbb{N}^\star$). Le théorème précédent met en valeur ce découpage, et toute notre construction donne rend logique les notations $\underline{n}$ et $-\underline{n}$ pour $n \in \mathbb{N}$.

Cela nous donne alors envie de définir les notions d'entiers relatifs positifs et négatifs et de définir un ordre sur $\mathbb{Z}$:

Définition 1.1.17 (Ordre sur $\mathbb{Z}$)

- Si x et y sont deux entiers, on dira que x *est inférieur à* y, ce qu'on notera $x \leqslant y$, si et seulement si $y - x \in \mathbb{N}$.

- Si $0 \leqslant x$, on dira que x *est positif*. Si de plus $x \neq 0$, on dira que x *est strictement positif*, ce qu'on notera $0 < x$.
- Si $x \leqslant 0$, on dira que x *est négatif*. Si de plus $x \neq 0$, on dira que x *est strictement négatif*, ce qu'on notera $x < 0$.

Proposition 1.1.18
La relation $\leqslant$ définit un ordre total sur $\mathbb{Z}$. De plus, celui-ci est compatible avec l'addition :

$$\forall x, y, z, t \in \mathbb{Z} \qquad \left.\begin{array}{l} x \leqslant y \\ z \leqslant t \end{array}\right\} \iff x + z \leqslant y + t$$

Enfin, $$\forall x, y \in \mathbb{Z} \qquad (x \leqslant y \iff (-y) \leqslant (-x))$$

Preuve : Commençons par montrer que $\leqslant$ est un ordre total.

- **Réflexivité** : Soit $x \in \mathbb{Z}$. On a $x - x = 0$, puisque $-x$ est l'opposé de x. Donc $x - x \in \mathbb{N}$, ce qui veut dire que $x \leqslant x$.
- **Antisymétrie** : Soient x et y dans $\mathbb{Z}$, tels que $x \leqslant y$ et $y \leqslant x$. Cela signifie donc que

  $$y - x \in \mathbb{N} \qquad \text{et} \qquad x - y \in \mathbb{N}$$

  On déduit de la première relation d'appartenance que $x - y \in (-\mathbb{N})$. Supposons que $x \neq y$, de sorte qu'en fait

  $$x - y \in (-\mathbb{N}^\star) \qquad \text{et} \qquad x - y \in \mathbb{N}^\star$$

  On obtient $$x - y \in \mathbb{N}^\star \cap (-\mathbb{N}^\star)$$

  mais cet ensemble est vide d'après le **corollaire 1.16**. D'où une absurdité et par suite $x = y$.
- **Transitivité** : Soient x, y et z dans $\mathbb{Z}$, tels que $x \leqslant y$ et $y \leqslant z$. Par définition,

  $$y - x \in \mathbb{N} \qquad \text{et} \qquad z - y \in \mathbb{N}$$

  Du coup, $$z - x = (z - y) + (y - x) \in \mathbb{N}$$

  puisque la somme de deux entiers naturels est un entier naturel.
- **Totalité** : Soient x et y dans $\mathbb{Z}$. Alors $y - x$ est soit dans $\mathbb{N}$, soit dans $-\mathbb{N}^\star$ d'apres le **corollaire 1.16**. Dans le premier cas, on a $x \leqslant y$. Dans le second cas, c'est que $x - y \in \mathbb{N}^\star$ donc $y \leqslant x$. x et y sont donc toujours comparables.

Montrons la compatibilité avec l'addition. Soient x, y, z et t quatre entiers relatifs, tels que

$$x \leqslant y \qquad \text{et} \qquad z \leqslant t$$

Par définition, $$y - x \in \mathbb{N} \qquad \text{et} \qquad t - z \in \mathbb{N}$$

Alors, la somme de deux entiers naturels étant un entier naturel,

$$y + t - (x + z) = y + t - x - z = (y - x) + (t - z) \in \mathbb{N}$$

de sorte que $$x + z \leqslant y + t$$

Enfin, montrons que le passage à l'opposé change l'ordre dans $\mathbb{Z}$. Soient x et y dans $\mathbb{Z}$, tels que $x \leqslant y$. Par définition, $y - x \in \mathbb{N}$. Or,

$$y - x = -(-y) + (-x) = (-x) - (-y) \in \mathbb{N}$$

donc $$(-y) \leqslant (-x)$$ □

À ce stade, et compte-tenu du **Corollaire 1.16**, les entiers relatifs sont partagés en trois catégories mutuellement disjointes : $\underline{0}$, les entiers naturels non nuls (qui sont les entiers relatifs strictement positifs) et les opposés des entiers naturels non nuls (qui sont les entiers strictement négatifs). Autrement dit, on retrouve bien ce qu'on avait admis sur l'ensemble $\mathbb{Z}$:

$$\mathbb{Z} = \{\underline{0}, \pm\underline{1}, \pm\underline{2}, \ldots\}$$

De fait, on peut maintenant laisser tomber les soulignés, qui n'étaient là que pour éviter la confusion le $\mathbb{Z}$ qu'on est en train de construire, et le $\mathbb{Z}$ dont l'existence avait été admise dans les classes précédentes.

1.1.4 Structure d'anneau sur $\mathbb{Z}$

Une autre structure algébrique intervenant souvent en mathématiques est celle d'anneau, que nous allons immédiatement définir :

Définition 1.1.19 (Anneau)
Soit E un ensemble, muni de deux lois de composition internes + et $\star$. On dira que E *est un anneau* si, et seulement si, (E, +) est un groupe commutatif d'élément neutre 0 et

- $\star$ est associative ;
- $\star$ admet un élément neutre, noté 1 ;
- $\star$ est distributive sur + :

$$\forall x, y, z \in \mathrm{E} \qquad x \star (y + z) = (x \star y) + (y \star z)$$

et $$\forall x, y, z \in \mathrm{E} \qquad (x + y) \star z = (x \star z) + (y \star z)$$

Si, de plus, $\star$ est commutative, on dira que E *est un anneau commutatif*.

Exemple 1.1.20
Outre $\mathbb{Z}$, dont on va montrer qu'il s'agit d'un anneau, on en a déjà rencontré plusieurs au cours de notre scolarité. Soit A un ensemble ; on note $\mathrm{E} = \mathscr{P}(\mathrm{A})$ l'ensemble de ses parties. On a déjà vu au tout début de l'année que $\cap$ et $\cup$ sont des lois de composition internes sur E.

De plus, $(\mathrm{E}, \cup)$ est un groupe commutatif : on sait que $\cup$ est associative, commutative, admet $\emptyset$ pour élément neutre et que tout sous-ensemble B de A admet un opposé pour $\cup$, qui est B^c.

On sait aussi que $\cap$ est associative, commutative, distributive sur $\cup$ (lois de De Morgan), admet A pour élément neutre. $(\mathrm{E}, \cup, \cap)$ est un anneau commutatif.

Théorème 1.1.21 (Structure d'anneau de $\mathbb{Z}$)
$(\mathbb{Z}, \oplus, \otimes)$ *est un anneau commutatif.*

Preuve : On sait déjà que $(\mathbb{Z}, \oplus)$ est un groupe commutatif : il s'agit du **Théorème 1.14**. Restent à établir :

- **Commutativité de** $\otimes$: Soient x et y dans $\mathbb{Z}$. Soient a, b, c et d dans $\mathbb{N}$ tels que

$$x = \overline{(a,b)} \qquad \text{et} \qquad y = \overline{(c,d)}$$

D'après le **Corollaire 1.5**,

$$x \otimes y = \overline{(ac+bd, ad+bc)} \qquad \text{et} \qquad y \otimes x = \overline{(ca+db, da+cb)}$$

Or, l'addition et la multiplication dans $\mathbb{N}$ sont commutatives, donc

$$ac+bd = ca+db \qquad \text{et} \qquad ad+bc = da+cb$$

et par suite, $$x \otimes y = y \otimes x$$

- **Associativité de** $\otimes$: Soient x, y et z dans $\mathbb{Z}$. Soient a, b, c, d, e et f dans $\mathbb{N}$ tels que

$$x = \overline{(a,b)} \qquad y = \overline{(c,d)} \qquad \text{et} \qquad z = \overline{(e,f)}$$

D'après le **Corollaire 1.5**, on sait que

$$x \otimes y = \overline{(ac+bd, ad+bc)}$$

et $$(x \otimes y) \otimes z = \overline{\big((ac+bd)e + (ad+bc)f, (ac+bd)f + (ad+bc)e\big)}$$

De même, $$x \otimes (y \otimes z) = \overline{\big(a(ce+df) + b(cf+de), a(cf+de) + b(ce+df)\big)}$$

En utilisant les propriétés usuelles de l'addition et de la multiplication dans $\mathbb{N}$, il vient

$$(x \otimes y) \otimes z = \overline{(ace+bde+adf+bcf, acf+bdf+ade+bce)}$$

tandis que $$x \otimes (y \otimes z) = \overline{(ace+adf+bcf+bde, acf+ade+bce+bdf)}$$

La commutativité de l'addition dans $\mathbb{N}$ assure alors qu'on a bien

$$(x \otimes y) \otimes z = x \otimes (y \otimes z)$$

- **Élément neutre pour** $\otimes$: On devine bien que cet élément neutre pour la multiplication sera $1 = \overline{(1,0)}$. On vérifie en effet que si $x = \overline{(a,b)} \in \mathbb{Z}$, alors

$$x \otimes 1 = \overline{(a \times 1 + b \times 0, a \times 0 + b \times 1)} = \overline{(a,b)} = x$$

- **Distributivité de** $\otimes$ **sur** $\oplus$: Soient des entiers relatifs

$$x = \overline{(a,b)} \qquad y = \overline{(c,d)} \qquad \text{et} \qquad z = \overline{(e,f)}$$

On a $$\begin{aligned} x \otimes (y \oplus z) &= \overline{(a,b)} \otimes \overline{(c+e, d+f)} \\ &= \overline{\big(a(c+e) + b(d+f), a(d+f) + b(c+e)\big)} \\ &= \overline{\big((ac+bd) + (ae+bf), (ad+bc) + (af+be)\big)} \\ &= \overline{(ac+bd, ad+bc)} \oplus \overline{(ae+bf, af+be)} \\ x \otimes (y \oplus z) &= (x \otimes y) \oplus (x \otimes z) \end{aligned}$$ □

Proposition 1.1.22 (Relation entre somme et produit)
Soient x et y deux entiers relatifs.

- *Si* $x > 0$, $$x \otimes y = \underbrace{y \oplus y \oplus \cdots \oplus y}_{x \text{ fois}}$$
- *Si* $x < 0$, $$xy = -(\underbrace{y \oplus y \oplus \cdots \oplus y}_{-x \text{ fois}})$$

Preuve : Fixons $y \in \mathbb{Z}$. On pose

$$\forall n \in \mathbb{N}^\star \qquad u_n = n \otimes y$$

Alors $$u_1 = 1 \otimes y = y$$

et $$\forall n \in \mathbb{N}^\star \qquad u_{n+1} = (n+1) \otimes y = n \otimes y + y = u_n + y$$

Mais on a vu dans le cours sur les nombres entiers qu'il y a une seule suite définie par récurrence de cette maniere : c'est celle de terme général $\sum_{k=1}^{n} y$. Par suite,

$$\forall n \in \mathbb{N}^\star \qquad u_n = \sum_{k=1}^{n} y = y \oplus \cdots \oplus y$$

Ceci démontre la première assertion. La seconde en est une conséquence : soit $x \in (-\mathbb{N}^\star)$ et notons $n = -x \in \mathbb{N}^\star$. Alors

$$x \otimes y = -(-x \otimes y) = -n \otimes y = -(\underbrace{y \oplus \cdots \oplus y}_{n \text{ fois}})$$ □

On a établi les propriétés bien connues de $\mathbb{Z}$, ce qui justifie le retour aux notations habituelles $+$ et $\times$ pour l'addition et la multiplication.

1.2 Construction de $\mathbb{Q}$

Cependant, $\mathbb{Z}$ présente un inconvénient : les seuls entiers relatifs inversibles sont 1 et -1. En effet, soit $x \in \mathbb{Z}$, inversible pour la multiplication. Il existe $y \in \mathbb{Z}$, tel que $xy = 1$. On remarque que x et y sont de même signe pour que leur produit soit positif.

Supposons qu'ils sont tous deux positifs ; aucun d'eux ne peut être nul, puisque leur produit serait nul. Et si $x > 1$, alors $x \geqslant 2$ et $xy \geqslant 2y \geqslant 2$ ce qui contredit le fait que $xy = 1$. Par suite, $x = 1$.

De même, si x et y sont négatifs, alors $-x$ et $-y$ sont positifs et vérifient $(-x)(-y) = 1$. D'après ce qui précède, $-x = 1$ et $x = -1$.

Ainsi, dans $\mathbb{Z}$, on ne peut diviser que par 1 et -1. Et pourtant, il est tout-a-fait imaginable de diviser un entier par un autre : une pomme peut être coupée en deux moitiés égales, un gateau peut être coupé en parts égales, etc.

On cherche donc à construire un ensemble, contenant $\mathbb{Z}$, dans lequel il soit en outre possible de diviser. Commençons par une définition :

Définition 1.2.1 (Anneaux intègre)
Soit A un anneau. On dit qu'un élément $x \in A$ est *un diviseur de 0* si, et seulement si,

$$\exists y \in A \setminus \{0\} \qquad xy = 0$$

Un anneau qui n'a pas de diviseur de 0 autre que 0 est dit *intègre*.

Exemple 1.2.2
Prenons l'ensemble A de fonctions de $\mathbb{R}$ dans $\mathbb{R}$. C'est un anneau pour les opérations d'addition et de multiplication des fonctions. Celui-ci contient des diviseurs de 0.

Par exemple, on considère les fonctions f et g définies par

$$\forall x \in \mathbb{R} \qquad f(x) = \begin{cases} 1 & \text{si } x \geqslant 0 \\ 0 & \text{si } x < 0 \end{cases} \qquad \text{et} \qquad g(x) = \begin{cases} 0 & \text{si } x \geqslant 0 \\ 1 & \text{si } x < 0 \end{cases}$$

f et g sont toutes deux dans $\mathrm{A} \setminus \{0\}$, puisqu'elles ne sont pas identiquement nulles. Et pourtant $fg = 0$.

La procédure permettant de construire $\mathbb{Q}$ à partir de $\mathbb{Z}$ est très générale et peut être en fait appliquée à tout anneau commutatif intègre. Commençons par établir que

Proposition 1.2.3 (Intégrité de $\mathbb{Z}$)
$\mathbb{Z}$ est un anneau intègre, ce qui signifie que

$$\forall x, y \in \mathbb{Z} \qquad xy = 0 \implies (x = 0 \quad ou \quad y = 0)$$

Preuve : Soient x et y deux entiers relatifs tels que $xy = 0$. S'ils sont tous deux positifs, c'est qu'ils sont en fait dans $\mathbb{N}$ et on sait alors que $x = 0$ ou $y = 0$. Si l'un d'eux est négatif, par exemple x, on a aussi $0 = -xy = (-x)y$ et on est ramené au cas précédent. □

Dans ce qui suit, A est un anneau commutatif intègre. On notera $\mathrm{A}^\star = \mathrm{A} \setminus \{0\}$ et on définit sur $\mathrm{A} \times \mathrm{A}^\star$ la relation suivante :

$$\forall (a,b),(c,d) \in \mathbb{A} \times \mathrm{A}^\star \qquad (a,b) \sim (c,d) \iff ad - bc = 0$$

Proposition 1.2.4
$\sim$ est une relation d'équivalence sur $\mathrm{A} \times \mathrm{A}^\star$.

Preuve : Comme d'habitude, on vérifie la réflexivité, la symétrie et la transitivité de $\sim$.

- **Réflexivité** : Soient a et b dans A, avec $b \neq 0$. Alors

$$ab - ba = ab - ab = 0 \qquad \text{d'où} \qquad (a,b) \sim (a,b)$$

- **Symétrie** : Soient (a,b) et (c,d) dans $\mathrm{A} \times \mathrm{A}^\star$ tels que $(a,b) \sim (c,d)$. Par définition, $ad - bc = 0$; mais l'addition et la multiplication sont commutatives dans A donc $cb - da = 0$ ce qui prouve que $(c,d) \sim (a,d)$.
- **Transitivité** : Soient (a,b), (c,d) et (e,f) dans $\mathrm{A} \times \mathrm{A}^\star$. On suppose que

$$(a,b) \sim (c,d) \qquad \text{et} \qquad (c,d) \sim (e,f)$$

Alors $$ad - bc = 0 \qquad \text{et} \qquad cf - de = 0$$

On multiplie la première relation par f et l'on utilise la deuxième pour trouver :

$$adf = bcf = bde$$

donc $$d(af - be) = 0$$

Mais $d \neq 0$ et A est intègre donc $af - be = 0$. Ce qui assure que $(a,b) \sim (e,f)$. □

Définition 1.2.5
L'ensemble quotient $(A \times A^\star)/\sim$ est noté $\mathbb{K}$. On l'appelle *corps des fractions sur* A.

Si $(a,b) \in A \times A^\star$, sa classe d'équivalence est notée $\frac{a}{b}$. Auquel cas,

- a est appelé *numérateur* de la fraction $\frac{a}{b}$;
- b est appelé *dénominateur* de la fraction $\frac{a}{b}$.

Le passage au quotient par la relation d'équivalence $\sim$ est exactement ce qu'il fallait pour retrouver les règles de simplification de fractions dont on a l'habitude. Par exemple, $\frac{2}{3} = \frac{10}{15}$ puisque $2 \times 15 - 3 \times 10 = 0$. On constate bien en effet que 5 est multiple commun du numérateur et du dénominateur de $\frac{10}{15}$, et tout se passe comme si on l'avait simplifié.

Plus généralement, si $\frac{a}{b} \in \mathbb{K}$, alors

$$\forall c \in A^\star \qquad \frac{a}{b} = \frac{ac}{bc} \qquad \text{puisque} \qquad abc - bac = 0$$

Proposition 1.2.6 (Injection de A dans $\mathbb{K}$)
L'application ι *définie par*

$$\forall m \in A \qquad \iota(m) = \frac{m}{1}$$

est injective.

Preuve : Soient m et n dans A tels que $\iota(m) = \iota(n)$, c'est-à-dire que $\frac{m}{1} = \frac{n}{1}$. Par définition,

$$m \times 1 - 1 \times n = 0$$

donc $m = n$: ι est injective. □

On voit donc que les éléments $\left(\frac{m}{1}\right)_{m \in A}$ sont deux-à-deux distincts dans $\mathbb{K}$, ce qui permet de considérer que A se trouve dans $\mathbb{K}$. De fait, on identifiera A et $\iota(A)$, c'est-à-dire que toute fraction $\frac{m}{1}$ avec $m \in A$ sera simplement notée m, comme s'il s'agissait d'un élément de A.

On souhaite maintenant définir des opérations sur $\mathbb{K}$, puisque, rappelons-le, notre objectif est d'avoir un ensemble contenant A, dans lequel on a en plus le droit de diviser par tout élément non nul.

L'addition et la multiplication dans $\mathbb{K}$ doivent répondre évidemment au cahier des charges suivant : sur A, elles doivent coïncider avec l'addition et la multiplication usuelles. Soient $\frac{a}{b}$ et $\frac{c}{d}$ deux fractions. Supposons temporairement que ce sont aussi des éléments de A, notés m et n, de sorte que

$$\frac{a}{b} = m \qquad \text{et} \qquad \frac{c}{d} = n$$

ce qui veut dire que $a = bm$ et $c = dn$

Par suite, $ad = mbd$ et $bc = nbd$

d'où $ad + bc = (m+n)bd$

et $$\frac{ad+bc}{bd} = m + n$$

On a donc envie de poser $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$.

Pour définir le produit, c'est plus simple, puisqu'on a simplement

$$ac = bdmn \qquad \text{ce qui veut dire que} \qquad \frac{ac}{bd} = mn$$

Il est donc naturel de définir $\frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}$. Il faut, avant cela, vérifier la compatibilité de ces opérations avec la relation $\sim$.

Lemme 1.2.7
Soient a, b, c, d, a', b', c' et d' dans A*, avec b, b', d, d' non nuls, tels que*

$$\frac{a}{b} = \frac{a'}{b'} \qquad et \qquad \frac{c}{d} = \frac{c'}{d'}$$

Alors
$$\frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'} \qquad et \qquad \frac{ac}{bd} = \frac{a'c'}{b'd'}$$

Preuve : Commençons par montrer que $\frac{ac}{bd} = \frac{a'c'}{b'd'}$ car c'est assez simple. On sait que

$$ab' = ba' \qquad \text{et} \qquad cd' = dc'$$

donc
$$acb'd' = bda'c' \qquad \text{ou encore} \qquad (ac)(b'd') - (bd)(a'c') = 0$$

Autrement dit,
$$\frac{ac}{bd} = \frac{a'c'}{b'd'}$$

On repart de $ab' = ba'$ et $cd' = dc'$. En multipliant la première relation par dd' et la deuxième par bb', il vient

$$adb'd' = bda'd' \qquad \text{et} \qquad bcb'd' = bdb'c'$$

On ajoute alors ces deux expressions :

$$(ad+bc)b'd' = bd(a'd'+b'c')$$

d'où
$$\frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'}$$ □

Corollaire 1.2.8
Il existe deux lois de composition internes sur $\mathbb{K}$, notées $+$ et $\times$, telles que

$$\forall (a,b),(c,d) \in \mathrm{A} \times \mathrm{A}^\star \qquad \frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \qquad et \qquad \frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}$$

Définition 1.2.9 (Corps)
Soit E un ensemble muni de deux lois de composition internes $+$ et $\star$. On dit que E *est un corps* si, et seulement si,

- $(\mathrm{E}, +, \star)$ est un anneau, d'éléments neutre 0 ;
- Tout élément de E, autre que 0, est inversible pour la loi $\star$.

Théorème 1.2.10
Le corps des fractions d'un anneau commutatif est un corps commutatif.

Preuve : Il s'agit de montrer que $\mathbb{K}$ est un corps. Rappelons les étapes : $(\mathbb{K},+)$ doit être un groupe commutatif, $(\mathbb{K},\times)$ doit être un anneau commutatif et tout élément de $\mathbb{K}$ autre que le neutre pour $+$ doit être inversible pour $\times$.

- $+$ **et** $\times$ **sont commutatives** : On a, d'après la commutativité de l'anneau A,

$$\forall \frac{a}{b},\frac{c}{d}\in\mathbb{K} \qquad \frac{a}{b}\times\frac{c}{d}=\frac{ac}{bd}=\frac{ca}{db}=\frac{c}{d}\times\frac{a}{b}$$

et $$\forall \frac{a}{b},\frac{c}{d}\in\mathbb{K} \qquad \frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}=\frac{bc+ad}{db}=\frac{c}{d}+\frac{a}{b}$$

- $+$ **et** $\times$ **sont associatives** : Soit $\frac{a}{b}$, $\frac{c}{d}$ et $\frac{e}{f}$ trois éléments de $\mathbb{K}$. On commence par le cas de $\times$, un peu moins calculatoire. D'après le **Corollaire 2.5**,

$$\frac{a}{b}\times\frac{c}{d}=\frac{ac}{bd} \qquad \text{et} \qquad \frac{c}{d}\times\frac{e}{f}=\frac{ce}{df}$$

puis $$\left(\frac{a}{b}\times\frac{c}{d}\right)\times\frac{e}{f}=\frac{(ac)e}{(bd)f} \qquad \text{et} \qquad \frac{a}{b}\times\left(\frac{c}{d}\times\frac{e}{f}\right)=\frac{a(ce)}{b(df)}$$

Or, A est un anneau donc la multiplication dans A est associative d'où

$$(ac)e=a(ce) \qquad \text{et} \qquad (bd)f=b(df)$$

Par suite, $$\left(\frac{a}{b}\times\frac{c}{d}\right)\times\frac{e}{f}=\frac{a}{b}\times\left(\frac{c}{d}\times\frac{e}{f}\right)$$

On passe maintenant à l'addition. Toujours d'après le **Corollaire 2.5**,

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}$$

et $$\left(\frac{a}{b}+\frac{c}{d}\right)+\frac{e}{f}=\frac{(ad+bc)f+(bd)e}{(bd)f}$$

De même, $$\frac{a}{b}+\left(\frac{c}{d}+\frac{e}{f}\right)=\frac{a(df)+b(cf+de)}{b(df)}$$

Mais comme A est un anneau, l'addition et la multiplication y sont associatives, et la multiplication se distribue sur l'addition. Donc

$$(ad+bc)f+(bd)e=adf+bcf+bde=a(df)+b(cf+de)$$

et $$(bd)f=b(df)$$

Finalement, $$\left(\frac{a}{b}+\frac{c}{d}\right)+\frac{e}{f}=\frac{a}{b}+\left(\frac{c}{d}+\frac{e}{f}\right)$$

L'addition dans $\mathbb{K}$ est associative.

- **Éléments neutre pour** $+$ **et** $\times$: Il suffit de remarquer que

$$\forall \frac{a}{b}\in\mathbb{K} \qquad \frac{a}{b}+\frac{0}{1}=\frac{a\times1+0\times b}{b\times1}=\frac{a}{b}$$

et $$\forall \frac{a}{b} \in \mathbb{K} \qquad \frac{a}{b} \times \frac{1}{1} = \frac{a \times 1}{b \times 1} = \frac{a}{b}$$

Donc les fractions $0 = \frac{0}{1}$ et $1 = \frac{1}{1}$ sont neutre dans $\mathbb{K}$, respectivement pour l'addition et la multiplication.

- **Inverses** : Remarquons que

$$\forall \frac{a}{b} \in \mathbb{K} \qquad \frac{a}{b} + \frac{-a}{b} = \frac{ab + (-ab)}{b^2} = \frac{ab - ab}{b^2} = \frac{0}{1} = 0$$

donc tout élément $\frac{a}{b}$ de $\mathbb{K}$ est inversible, d'inverse $\frac{-a}{b}$.
Ensuite, si $\frac{a}{b}$ est une fraction dans $\mathbb{K}$, non nulle, on sait que

$$\frac{a}{b} \neq \frac{0}{1} \qquad \text{ou encore} \qquad a \times 1 \neq 0 \times b$$

c'est-à-dire que $$a \neq 0$$

De fait, on peut former la fraction $\frac{b}{a}$. Du coup,

$$\frac{a}{b} \times \frac{b}{a} = \frac{ab}{ba} = \frac{ab}{ab} = \frac{1}{1}$$

et $\frac{a}{b}$ est inversible pour $\times$, d'inverse $\frac{b}{a}$. □

Puisque $\mathbb{Z}$ est un anneau intègre, le paragraphe précédent montre que l'on peut former son corps des fractions.

Définition 1.2.11
Le corps des fractions de $\mathbb{Z}$ est noté $\mathbb{Q}$. On l'appelle **ensemble des rationnels**. C'est un corps commutatif, contenant $\mathbb{Z}$.

1.3 Compléments de vocabulaire sur les structures

1.3.1 Sous-groupes et morphismes de groupes

Définition 1.3.1 (Sous-groupes)
Soit $(G, \star)$ un groupe. Soit H une partie de G. On dira que H est un sous-groupe de G si, et seulement si, $(H, \star)$ est un groupe.

Commençons par lever deux ambiguïtés. On suppose qu'on a un groupe G et un sous-groupe H. Alors G a un élément neutre qu'on appelle 1_G et H a un élément neutre qu'on appelle 1_H. On sait

$$\forall x \in G \qquad x \star 1_G = 1_G \star x = x$$

En particulier, $$1_H \star 1_G = 1_H$$

Mais aussi $$1_H \star 1_H = 1_H$$

donc $$1_H \star 1_H = 1_H \star 1_G$$

Ne reste qu'à multiplier cette égalité par 1_H^{-1} à gauche pour trouver $1_H = 1_G$: le neutre pour la structure de groupe de G est aussi le neutre pour la structure de groupe de H.

Faisons de même pour les inverses. Si $x \in \mathrm{H}$, il admet un inverse dans H puisque H est un groupe : il existe $x_{\mathrm{H}}^{-1} \in \mathrm{H}$ tel que

$$x \star x_{\mathrm{H}}^{-1} = x_{\mathrm{H}}^{-1} \star x = 1_{\mathrm{H}}$$

Mais il admet aussi un inverse x_{G}^{-1} pour la structure de groupe de G :

$$x \star x_{\mathrm{G}}^{-1} = x_{\mathrm{G}}^{-1} \star x = 1_{\mathrm{G}}$$

Or, on vient de voir que $1_{\mathrm{G}} = 1_{\mathrm{H}}$. Donc x_{G}^{-1} est aussi inverse de x dans H. L'inverse dans un groupe étant unique (**Proposition 1.11**), il vient $x_{\mathrm{G}}^{-1} = x_{\mathrm{H}}^{-1}$.

Tout ceci se résume en :

Lemme 1.3.2
Soient G *un groupe et* H *un sous-groupe. Alors* $1_{\mathrm{G}} = 1_{\mathrm{H}}$ *; de plus, pour tout* $x \in \mathrm{H}$*, son inverse pour la structure de groupe de* H *est son inverse pour la structure de groupe de* G.

Du coup, il n'y a pas d'ambiguïté possible lorsqu'on parle de 1 ou de x^{-1} lorsque $x \in \mathrm{H}$.

Donnons maintenant une caractérisation des sous-groupes, qui permettra d'établir facilement qu'un objet est un groupe.

Proposition 1.3.3
Soit $(\mathrm{G}, \star)$ *un groupe. Soit* H *une partie non vide de* G*. Alors* H *est un sous-groupe de* G *si, et seulement si,*

$$\forall x, y \in \mathrm{H} \qquad x \star y^{-1} \in \mathrm{H}$$

Preuve : Supposons que H est un sous-groupe de G. Étant donnés x et y dans H, y^{-1} se trouve aussi dans H ; et la loi $\star$ étant interne à H, on a $x \star y^{-1} \in \mathrm{H}$.

Réciproquement, supposons que

$$\forall x, y \in \mathrm{H} \qquad x \star y^{-1} \in \mathrm{H}$$

Commençons par montrer que $\star$ est une loi de composition interne à H. Soit $x \in \mathrm{H}$; un tel x existe puisque H n'est pas vide. On sait alors que $x \star x^{-1} \in \mathrm{H}$ donc $1 \in \mathrm{H}$. Du coup, $1 \star x^{-1} \in \mathrm{H}$ et on a montré que

$$\forall x \in \mathrm{H} \qquad x^{-1} \in \mathrm{H}$$

Donnons-nous deux éléments x et y dans H. On sait maintenant que $y^{-1} \in \mathrm{H}$; on sait également que $(y^{-1})^{-1} = y$ donc

$$x \star y = x \star (y^{-1})^{-1} \in \mathrm{H}$$

Ceci établit bien que $\star$ est une loi de composition interne à H.

Elle est associative, puisque $\mathrm{H} \subset \mathrm{G}$ et qu'elle est associative sur G. On a vu que $1 \in \mathrm{H}$, qui est alors neutre pour H vu qu'il l'est pour G. Enfin, si $x \in \mathrm{H}$, on a vu que $x^{-1} \in \mathrm{H}$ également : tout élément de H admet un inverse. □

Ce théorème est utile pour montrer qu'un objet H est un groupe sans avoir à vérifier tous les axiomes d'un groupe : en effet, si l'on sait que H est un sous-ensemble d'un groupe G, alors il suffit de vérifier que H n'est pas vide et que

$$\forall x, y \in \mathrm{H} \qquad x \star y^{-1} \in \mathrm{H}$$

pour avoir que H est un groupe.

On a déjà montré que $\mathbb{Z}$ et $\mathbb{Q}$ sont des groupes additifs. D'autres exemples de groupes sont $\mathbb{R}$ et $\mathbb{C}$; ou encore $\mathbb{G}^A$, l'ensemble des fonctions d'un ensemble A dans un groupe G ; ou enfin, l'ensemble des bijections d'un ensemble A, qui est un groupe pour la composition des applications. Tous ces exemples, vus en cours, peuvent être utilisés comme étant des groupes bien connus. Et lorsqu'on doit montrer qu'un ensemble H est un groupe, on pourra simplement montrer que c'est un sous-groupe d'un de ces groupes connus.

Exemple 1.3.4
Soit n un entier naturel. On considère l'ensemble

$$\{nx \mid x \in \mathbb{Z}\} = \{0, \pm n, \pm 2n, \ldots\}$$

Celui-ci est communément noté $n\mathbb{Z}$. Il n'est bien sûr pas vide, puisqu'il contient 0 ; et l'on a $n\mathbb{Z} \subset \mathbb{Z}$.

Soient m et p deux éléments de $n\mathbb{Z}$. Par définition, il existe des entiers relatifs x et y tels que

$$m = nx \qquad \text{et} \qquad p = ny$$

Alors
$$m - p = nx - ny = n(x - y)$$

Or, $x - y \in \mathbb{Z}$ donc $m - p$ est bien dans $n\mathbb{Z}$. De ce fait, $n\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$.

Exemple 1.3.5
Dans le cours sur les nombres complexes, on a été amené à considérer l'ensemble $\mathbb{U}$ des nombres complexes de module 1 :

$$\mathbb{U} = \{z \in \mathbb{C} \mid |z| = 1\}$$

C'est un sous-ensemble de $\mathbb{C}^\star$, qui est un groupe pour la multiplication. Montrons que c'en est un sous-groupe. On sait, d'après les propriétés du module, que

$$\forall z, w \in \mathbb{U} \qquad |zw^{-1}| = \frac{|z|}{|w|} = \frac{1}{1} = 1$$

donc
$$\forall z, w \in \mathbb{U} \qquad zw^{-1} \in \mathbb{U}$$

ce qui montre que $\mathbb{U}$ est un groupe.

Exemple 1.3.6
Si n est un entier naturel non nul, on considère maintenant l'ensemble $\mathbb{U}_n$ des racines n-ème de l'unité :

$$\mathbb{U}_n = \{z \in \mathbb{C} \mid z^n = 1\}$$

On sait déjà que $\mathbb{U}_n \subset \mathbb{U}$ (voir cours sur les nombres complexes). Montrons qu'il s'agit d'un sous-groupe de $\mathbb{U}$. Si z et w sont dans $\mathbb{U}_n$, on a

$$(zw^{-1})^n = \frac{z^n}{w^n} = \frac{1}{1} = 1$$

donc
$$zw^{-1} \in \mathbb{U}_n$$

$\mathbb{U}_n$ est un sous-groupe de $\mathbb{U}$.

Définition 1.3.7 (Morphismes de groupes)
Soient $(G, \star)$ et $(G', \bullet)$ deux groupes. On dira qu'une application $f : G \longrightarrow G'$ est un *morphisme de groupes* si, et seulement si,

$$\forall x, y \in G \qquad f(x \star y) = f(x) \bullet f(y)$$

Définition 1.3.8 (Isomorphisme de groupes)
On appelle *isomorphisme de groupes* tout morphisme de groupes bijectif.

Définition 1.3.9 (Endomorphisme, automorphisme)
Un *endomorphisme* de groupe est un morphisme d'un groupe dans lui-même. Un *automorphisme* de groupe est un endomorphisme bijectif.

Les morphismes de groupes sont tout simplement les applications qui sont compatibles avec la structure de groupe.

Exemple 1.3.10
Considérons les groupes $G = 2\mathbb{Z}$ et $H = 6\mathbb{Z}$. L'application

$$\begin{aligned} f : \ 6\mathbb{Z} &\longrightarrow 2\mathbb{Z} \\ x &\longmapsto x \end{aligned}$$

est un morphisme de groupes. Elle est clairement injective ; en revanche, elle n'est pas surjective car 4 n'a pas d'antécédent par f.

On peut aussi considérer

$$\begin{aligned} g : \ 2\mathbb{Z} &\longrightarrow 6\mathbb{Z} \\ x &\longmapsto 3x \end{aligned}$$

C'est aussi un morphisme de groupes. L'injectivité est claire. Enfin, si $y \in 6\mathbb{Z}$, c'est un multiple de 6, donc en particulier $\frac{y}{3}$ est un entier pair et se trouve dans $2\mathbb{Z}$. Et on a $f(\frac{y}{3}) = y$ donc f est un isomorphisme de groupes.

On voit donc que $2\mathbb{Z}$ et $6\mathbb{Z}$ sont isomorphes, c'est-à-dire qu'ils ont à peu près la même structure. Ce qui n'est pas étonnant, puisque tous deux « ressemblent » à $\mathbb{Z}$. Dans un cas, on n'a gardé que les entiers relatifs pairs, dans l'autre les multiples de 6.

Exemple 1.3.11
Les ensembles $(\mathbb{R}_+^\star, \times)$ et $(\mathbb{R}, +)$ sont des groupes, d'éléments neutres respectivement 1 et 0. On sait que

$$\forall x > 0 \qquad \ln(xy) = \ln x + \ln y$$

et que le logarithme réalise une bijection de $\mathbb{R}_+^\star$ sur $\mathbb{R}$. En d'autres termes, ln est un isomorphisme de $(\mathbb{R}^\star, \cdot)$ sur $(\mathbb{R}, +)$.

Exemple 1.3.12
On considère les groupes $(\mathbb{R}, +)$ et $\mathbb{U}$. On définit

$$\forall x \in \mathbb{R} \qquad f(x) = \mathrm{e}^{\mathrm{i}x}$$

Le cours sur les nombres complexes nous dit que f est un morphisme surjectif de $(\mathbb{R}, +)$ sur $\mathbb{U}$.

En revanche, f n'est pas injectif puisque $f(2\pi) = f(0) = 1$.

Définition 1.3.13 (Noyau, Image)
Soient G et G′ deux groupes, soit f un morphisme de G dans G′. On appelle *noyau* de f l'ensemble

$$\mathrm{Ker}\, f = \{g \in \mathrm{G} \mid f(g) = 1_{\mathrm{G}'}\}$$

On appelle *image* de f l'ensemble

$$\mathrm{Im}\, f = \{f(g) \mid g \in \mathrm{G}\} = f(\mathrm{G})$$

Exemple 1.3.14
Reprenons le dernier exemple :

$$\forall x \in \mathbb{R} \qquad f(x) = \mathrm{e}^{\mathrm{i}x}$$

On a $$\mathrm{Ker}\, f = \{x \in \mathbb{R} \mid f(x) = 1\} = \{x \in \mathbb{R} \mid \mathrm{e}^{\mathrm{i}x} = 1\}$$

Le cours sur les nombres complexes assure que $\mathrm{Ker}\, f = 2\pi\mathbb{Z}$. Tandis que $\mathrm{Im}\, f = \mathbb{U}$, d'après l'existence de la forme trigonométrique.

Proposition 1.3.15
Soient G *et* G′ *deux groupes, soit* f *un morphisme de* G *dans* G′. *On a*

$$f(1_G) = 1_{G'} \qquad \textit{et} \qquad \forall x \in G \qquad f(x^{-1}) = f(x^{-1})$$

De plus,

- f *est injective si, et seulement si,* $\mathrm{Ker}\, f = \{1_G\}$;
- f *est surjective si, et seulement si,* $\mathrm{Im}\, f = G'$.

Preuve : Notons $y = f(1_G)$. On a alors, puisque f est un morphisme de groupes,

$$y \bullet y = f(1_G) \bullet f(1_G) = f(1_G \star 1_G) = f(1_G) = y$$

Comme G′ est un groupe, il contient y^{-1} qu'on multiplie à gauche membre-à-membre pour obtenir $y = 1_{G'}$.

Ensuite, soit $x \in G$. On a

$$f(x) \bullet f(x^{-1}) = f(x \star x^{-1}) = f(1_G) = 1_{G'}$$

donc $f(x^{-1})$ est l'inverse de $f(x)$.

La proposition sur la surjectivité de f est une trivialité, dans la mesure où $\mathrm{Im}\, f = f(G)$; f est surjective si et seulement si elle atteint tout élément de G′, c'est-à-dire si $f(G) = G'$.

Montrons enfin que f est injective si, et seulement si, $\mathrm{Ker}\, f = \{1_G\}$. On suppose d'abord que f est injective ; alors $1_{G'}$ a un seul antécédent. Mais on sait déjà que $f(1_G) = 1_{G'}$; donc $\mathrm{Ker}\, f = \{1_G\}$. Réciproquement, supposons que $\mathrm{Ker}\, f = \{1_G\}$. Soient x et y dans G tels que $f(x) = f(y)$. Alors

$$f(x \star y^{-1}) = f(x) \bullet f(y^{-1}) = f(x) \bullet f(y)^{-1} = f(x) \bullet f(x)^{-1} = 1_{G'}$$

donc $$x \star y^{-1} \in \mathrm{Ker}\, f \qquad \text{et} \qquad x \star y^{-1} = 1_G$$

Il s'ensuit que $x = y$ et f est injective. □

1.3.2 Sous-anneaux et morphismes d'anneaux

Définition 1.3.16 (Sous-anneaux)
Soit $(A, +, \star)$ un anneau, soit $B \subset A$. On dit que B *est un sous-anneau de* A si, et seulement si, $1_A \in B$ et $(B, +, \star)$ est un anneau.

Si B est un sous-anneau de A, on sait en particulier que $(B, +)$ est un sous-groupe de $(A, +)$. Le **lemme 3.2** peut être appliqué pour en déduire que $0_B = 0_A$ et que l'opposé d'un $x \in B$ est le même pour les deux structures d'anneaux de A et B.

Montrons aussi que $1_B = 1_A$. Comme 1_A est neutre pour A, on a en particulier

$$\forall x \in \mathrm{B} \qquad 1_\mathrm{A} \star x = x \star 1_\mathrm{A} = x$$

Ce qui veut dire que 1_A est neutre pour $(\mathrm{B}, \star)$ et appartient à B. La **Proposition 1.8** montre alors que $1_\mathrm{A} = 1_\mathrm{B}$.

Également, montrons que les notions d'inverse dans B et A coïncident. Soit $x \in \mathrm{B}$, inversible, dont on note y l'inverse dans B. Alors

$$x \star y = y \star x = 1_\mathrm{B} = 1_\mathrm{A}$$

Donc x est aussi inversible dans A et y est son inverse pour la structure d'anneau de A.

Lemme 1.3.17
Soient A *un anneau et* B *un sous-anneau. Alors*

- $0_\mathrm{B} = 0_\mathrm{A}$ *et* $1_\mathrm{B} = 1_\mathrm{A}$ *;*
- *L'opposé d'un* $x \in \mathrm{B}$ *est le même pour les structures d'anneau de* A *et* B*. On a le même résultat pour les inverses, si* x *est inversible dans* B*.*

Proposition 1.3.18
Soient A *un anneau et* B *un sous-ensemble de* A*. Alors* B *est un sous-anneau de* A *si, et seulement si,* B *contient* 1_A *et*

$$\forall x, y, z \in \mathrm{B} \qquad xy + z \in \mathrm{B}$$

Preuve : La preuve n'est pas plus compliquée que celle de la **Proposition 3.3**. □

Définition 1.3.19 (Morphismes d'anneaux)
Soient $(\mathrm{A}, +, \times)$ et $(\mathrm{A}', \oplus, \otimes)$ deux anneaux. Soit $f : \mathrm{A} \longrightarrow \mathrm{A}'$; on dira que f *est un morphisme d'anneaux* si, et seulement si, $f(1_\mathrm{A}) = 1_{\mathrm{A}'}$ et

$$\forall x, y, z \in \mathrm{A} \qquad f(x \times y + z) = f(x) \otimes f(y) \oplus f(z)$$

On observe qu'un morphisme f entre les anneaux A et A′ est en particulier un morphisme entre les groupes commutatifs $(\mathrm{A}, +)$ et $(\mathrm{A}', \oplus)$, de sorte que ce qui a été vu dans le paragraphe précédent s'applique :

$$f(0_\mathrm{A}) = 0_{\mathrm{A}'} \qquad \text{et} \qquad \forall x \in \mathrm{A} \qquad f(-x) = -f(x)$$

Définition 1.3.20 (Noyau, Image)
Soit f un morphisme entre les anneaux A et A′. On appelle *noyau* de f l'ensemble

$$\mathrm{Ker}\, f = \{x \in \mathrm{A} \mid f(x) = 0_{\mathrm{A}'}\}$$

et *image* de f l'ensemb ;e

$$\mathrm{Im}\, f = \{f(x) \mid x \in \mathrm{A}\} = f(\mathrm{A})$$

Puisqu'un morphisme d'anneaux est aussi un morphisme de groupes, on utilise la **Proposition 3.15** pour en déduire

Proposition 1.3.21
Soit f *un morphisme entre les anneaux* A *et* A′*. Alors*

- f *est injective si, et seulement si,* $\mathrm{Ker}\, f = \{0_\mathrm{A}\}$ *;*
- f *est surjective si, et seulement si,* $\mathrm{Im}\, f = \mathrm{A}'$*.*

1.3.3 Règles de calcul dans un anneau

Proposition 1.3.22
Soit $(A,+,\star)$ *un anneau. Alors*

$$\forall x \in A \qquad x \star 0_A = 0_A \star x = 0_A$$

et

$$\forall x \in A \qquad (-1_A) \star x = x \star (-1_A) = -x$$

Preuve : Soit $x \in A$ et notons $y = x \star 0_A$. On a alors, par distributivité de $\star$ sur $+$,

$$y + y = x \star 0_A + x \star 0_A = x \star (0_A + 0_A) = x \star 0_A = y$$

On ajoute alors $-y$ aux deux membres pour trouver $y = 0_A$. On procède de la même manière pour $0_A \star x$.

Ensuite, notons $z = (-1_A) \star x$. Alors, toujours à l'aide de la distributivité de $\star$ sur $+$:

$$z + x = (-1_A) \star x + 1_A \star x = (-1_A + 1_A) \star x = 0_A \star x = 0_A$$

Donc z est un opposé de x ; mais dans un groupe, tout élément a un unique opposé donc $z = -x$.
On montrerait de la même manière que $x \star (-1_A) = -x$. □