Cours Euler, Première Année

Partie I: Les Nombres

Jérôme Scherer et Nicolas Michel

Table des matières

Introduction 4

Chapitre 1. Théorie des ensembles 5
1. Appartenance et inclusion 5
2. Opérations sur les ensembles 9

Chapitre 2. Les nombres naturels 15
1. L'ensemble des entiers naturels 15
2. Soustraction et division 16
3. Multiples et multiples communs 20
4. Diviseurs et diviseurs communs 22
5. Les nombres premiers 23

Chapitre 3. Les nombres entiers relatifs 28
1. Construction des entiers relatifs 28
2. L'addition 28
3. La soustraction 32
4. Multiplication et division 32
5. Retour à la soustraction 35
6. Priorité des opérations 37

Chapitre 4. Les nombres rationnels 40
1. Construction des nombres rationnels 40
2. La multiplication dans $\mathbb{Q}$ 45
3. L'addition dans $\mathbb{Q}$ 48

Chapitre 5. Un premier aperçu des nombres réels 52
1. Notation et exemples 52
2. L'écriture décimale 54

Introduction

Pendant les premières semaines du cours Euler nous étudierons les nombres. Notre hypothèse de base est que nous connaissons tous l'ensemble $\mathbb{N}$ des nombres entiers naturels. Dans un cours de mathématiques universitaire on construirait ces nombres avec des méthodes ensemblistes, mais cela nous emmènerait trop loin dans le formalisme. Nous allons tout de même commencer par mettre en place quelques bases de théorie des ensembles qui nous seront utiles par la suite dans tous les sujets que nous aborderons. Nous continuerons ensuite en étudiant les propriétés des nombres naturels, puis en construisant à partir de celles-ci les nombres entiers relatifs $\mathbb{Z}$ pour résoudre le problème de la soustraction, puis les nombres rationnels $\mathbb{Q}$ pour résoudre celui de la division. Tout à la fin de cette première partie nous introduirons les nombres réels et le développement décimal.

Chapitre 1

Théorie des ensembles

Nous commençons le cours avec les bases nécessaires à des raisonnements rigoureux. Nous parlerons dans ce premier chapitre d'ensembles et de leurs éléments, puis des opérations qui permettent de créer de nouveaux ensembles à partir d'ensembles connus : intersection, union, différence, etc. Dans le chapitre suivant nous étudierons tout spécialement l'ensemble des nombres naturels.

1. Appartenance et inclusion

De manière intuitive un ensemble est une collection d'objets qu'on appelle ses *éléments*. Si l'objet x est un élément de l'ensemble X, on dit qu'il appartient à X et on note

$$x \in X.$$

La négation de cette affirmation est notée

$$x \notin X$$

et on dit donc que x n'appartient pas à l'ensemble X. Un ensemble est entièrement déterminé par les éléments qui le composent. On définit ainsi l'égalité d'ensembles de la manière suivante. Soient X et Y deux ensembles. Alors

$$\boxed{X = Y \iff \text{pour tout } x \ (x \in X \iff x \in Y)}$$

où le symbole $\iff$ se lit "si et seulement si" et signifie que les affirmations de part et d'autre de ce signe sont équivalentes.

Si l'ensemble étudié n'est pas trop grand, on peut le décrire en donnant la liste de ses éléments entre accolades.

Exemple 1.1. Pour l'ensemble de villes $X = \{\text{Paris} ; \text{Berne} ; \text{Istanbul}\}$, on voit que Paris $\in X$ mais Lausanne $\notin X$.

Pour l'ensemble de nombres : $Y = \{3; 50; 8\}$, on observe que ce même ensemble peut être décrit aussi comme $Y = \{3; 8; 50\}$ ou encore $\{3; 8; 50; 50\}$. Ni l'ordre, ni la répétition n'ont d'influence dans la description d'un ensemble.

Enfin considérons l'ensemble d'ensembles $E = \{X; Y\}$, c'est-à-dire que les éléments de E sont eux-mêmes des ensembles ! Alors Paris $\in X$, l'ensemble $X \in E$, mais Paris $\notin E$.

Définition 1.2. L'*ensemble vide* est l'ensemble qui ne contient aucun élément. On le note $\emptyset$.

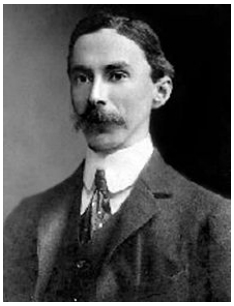
Parfois, en particulier lorsqu'il y a beaucoup d'éléments dans l'ensemble considéré, il est plus aisé de décrire les éléments par une propriété, appelons-la P, qu'ils vérifient tous. On écrit alors

$$\boxed{X = \{a \,|\, a \text{ a la propriété P}\}}$$

qui se lit « X est l'ensemble des objets a tels que a vérifie la propriété P ».

Remarque 1.3. Paradoxe de Russel. Une propriété ne détermine pas nécessairement un ensemble ! Essayons de travailler avec la propriété "être un ensemble qui n'appartient pas à lui-même". L'ensemble X des ensembles qui ont cette propriété fait-il partie de X ? Si on répond oui, alors, comme par définition les membres de cet ensemble n'appartiennent pas à eux-mêmes, il n'appartient pas à lui-même : contradiction. Mais si on répond non, alors il a la propriété requise pour appartenir

à lui-même : contradiction de nouveau. On a donc une contradiction dans les deux cas.



Bertrand Russell illustra ceci sous la forme plus imagée du paradoxe du barbier. Un barbier se propose de raser tous les hommes qui ne se rasent pas eux-mêmes, et seulement ceux-là. La question que l'on se pose est si le barbier doit se raser lui même ! L'étude des deux possibilités conduit de nouveau à une contradiction.

Pour construire de nouveaux ensembles à partir d'ensembles connus, le procédé le plus simple est de former des sous-ensembles.

Définition 1.4. Un ensemble Y est un *sous-ensemble* ou une *partie* d'un ensemble X si tout élément y de Y appartient aussi à X :

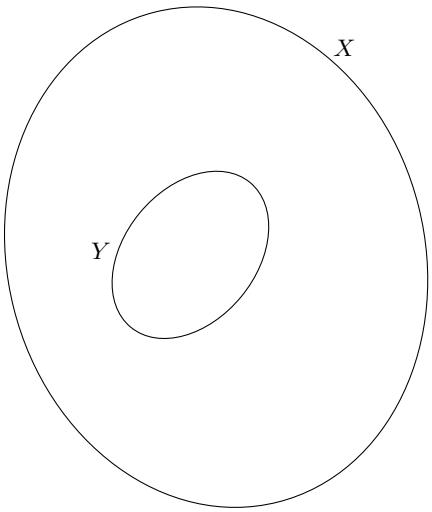
$$\text{Pour tout } x, (x \in Y \Rightarrow x \in X)$$

On note alors $Y \subset X$ et on dit que Y est *contenu* dans X. Sa négation est notée $Y \not\subset X$.

Lorsque l'on forme le sous-ensemble de X de tous les éléments qui vérifient une propriété P donnée, on l'écrit $\{x \in X \,|\, x \text{ a la propriété P }\}$ pour éviter de devoir écrire $\{x \,|\, x \in X \text{ et } x \text{ a la propriété } P\}$.

Exemple 1.5. Soit X un ensemble. Alors on a toujours $\emptyset \subset X$ et $X \subset X$.

Il est souvent utile de se représenter ensembles et sous-ensembles sous forme de diagramme de Venn, comme ci-dessous où l'on visualise le sous-ensemble Y des oiseaux dans l'ensemble X des animaux.

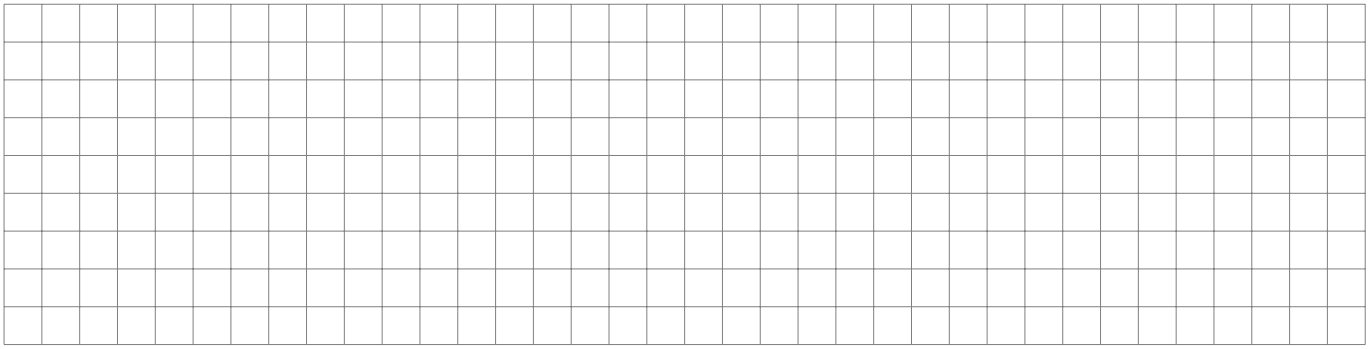


La proposition suivante s'appelle le *principe de la double inclusion*. Ce principe sera souvent bien utile, en particulier pour démontrer que deux ensembles sont les

mêmes. Pour ce faire il suffira de montrer que l'un est contenu dans l'autre et que l'autre est contenu dans l'un !

Proposition 1.6. *Soit X, Y des ensembles. Alors,*

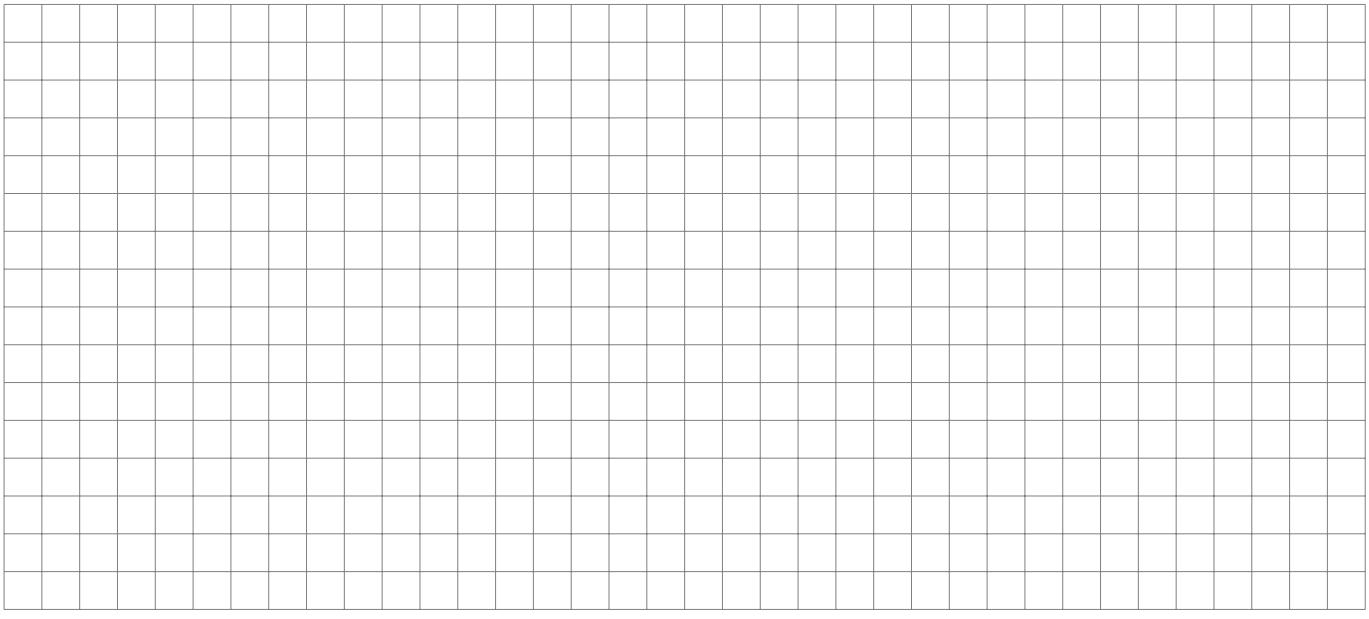
$$X = Y \iff (X \subset Y \text{ et } Y \subset X)$$



Définition 1.7. Soit X un ensemble. L'*ensemble des parties de* X, noté $\mathcal{P}(X)$, est l'ensemble de tous les sous-ensembles de X. Ainsi

$$\mathcal{P}(X) = \{A \,|\, A \subset X\}$$

Exemple 1.8. Si $X = \{x\}$ est un ensemble avec un seul élément, alors



2. Opérations sur les ensembles

On se place maintenant dans un "grand" ensemble contenant des sous-ensembles à l'aide desquels on veut construire de nouveaux sous-ensembles. Pour commencer

la réunion de X et Y est l'ensemble des éléments qui se trouvent soit dans X, soit dans Y.

Définition 2.1. Soient X et Y des ensembles. La *réunion* de X et Y, notée $X \cup Y$, est l'ensemble défini par

$$X \cup Y = \{a \mid a \in X \text{ ou } a \in Y\}$$

Ainsi la réunion se traduit par la conjonction de coordination "ou", dans son sens mathématique : un élément qui appartient à X ou à Y peut appartenir aux deux, ce n'est pas un "ou" exclusif comme dans la question « Est-ce que la boulangerie se trouve à droite ou à gauche de la poste ? ».

Exemple 2.2. Dans l'ensemble de toutes les villes de Suisse on considère $X = \{\text{Genève} ; \text{Delémont} ; \text{Lausanne}\}$ et $Y = \{\text{Berne}\}$. Alors la réunion de ces deux ensembles est

Sous forme de diagramme de Venn, la réunion se présente ainsi (toutes les régions grisées se trouvent dans l'union) :

Les propriétés (évidentes) de la réunion devraient vous faire penser à certaines propriétés de l'addition :

Proposition 2.3. *Soient X, Y, Z des ensembles. Alors on a :*

(1) $X \cup \emptyset = X$;

(2) $X \cup (Y \cup Z) = (X \cup Y) \cup Z$ *;*

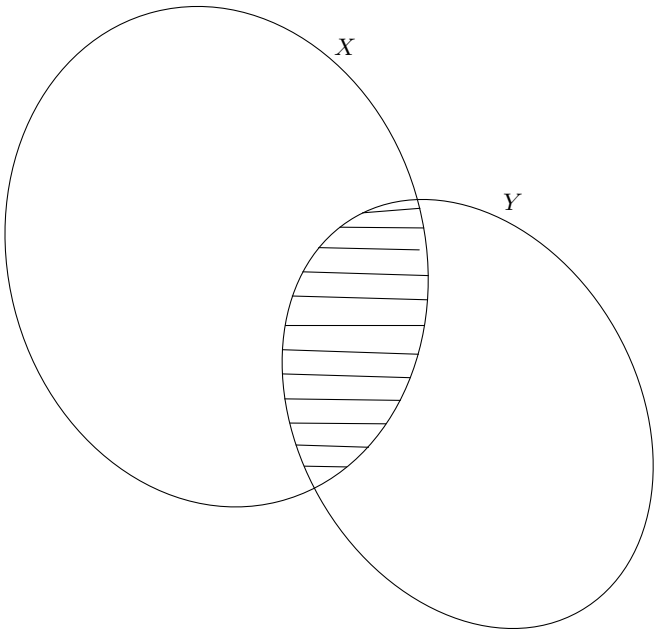
(3) Si $A \subset X$*, alors* $A \cup X = X$ *;*

(4) $X \cup Y = Y \cup X$*.*

L'intersection de X et Y est définie comme le sous-ensemble des éléments qui se trouvent à la fois dans X et dans Y.

Définition 2.4. Soient X et Y des ensembles. L'*intersection* de X et Y, notée $X \cap Y$, est l'ensemble défini par $X \cap Y = \{x \mid x \in X \text{ et } x \in Y\}$. On dit que deux ensembles X et Y sont *disjoints* si leur intersection est vide, c'est-à-dire $X \cap Y = \emptyset$.

Ainsi l'intersection se traduit par la conjonction de coordination "et". Par définition $X \cap Y \subset X \subset X \cup Y$. Voici le diagramme de Venn d'une intersection :



Exemple 2.5. Si $X = \{\text{Genève}\,;\, \text{Delémont}\,;\, \text{Lausanne}\}$ et $Y = \{\text{Berne}\,;\, \text{Fribourg}\}$, alors $X \cap Y = \emptyset$. Si $Z = \{\text{Berne}\,;\, \text{Delémont}\,;\, \text{Genève}\}$, alors $X \cap Z = \{\text{Genève}\,;\, \text{Delémont}\}$.

Cette fois les propriétés de l'intersection devraient nous faire penser à certaines propriétés de la multiplication.

Proposition 2.6. *Soient X, Y, Z des ensembles. Alors on a :*

(1) $X \cap \emptyset = \emptyset$;

(2) $X \cap (Y \cap Z) = (X \cap Y) \cap Z$;

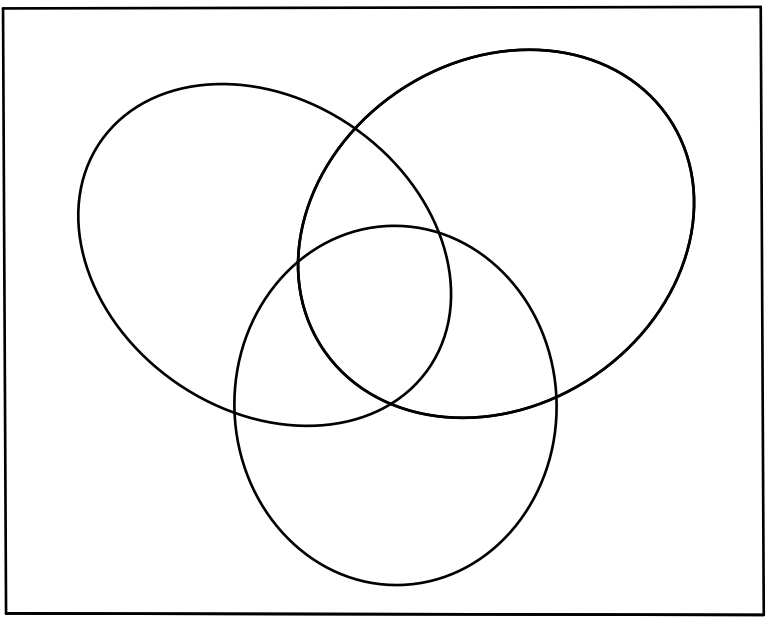
(3) Si $A \subset X$, *alors* $A \cap X = A$;

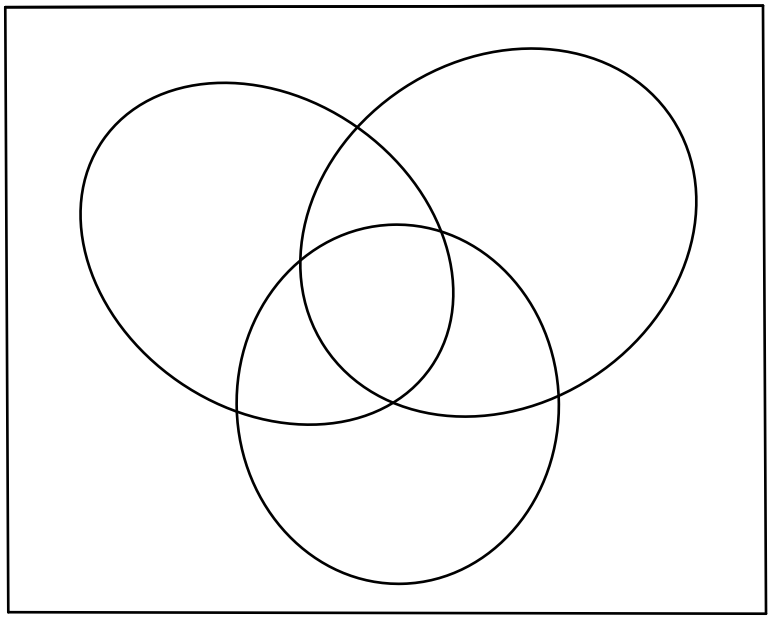
(4) $X \cap Y = Y \cap X$;

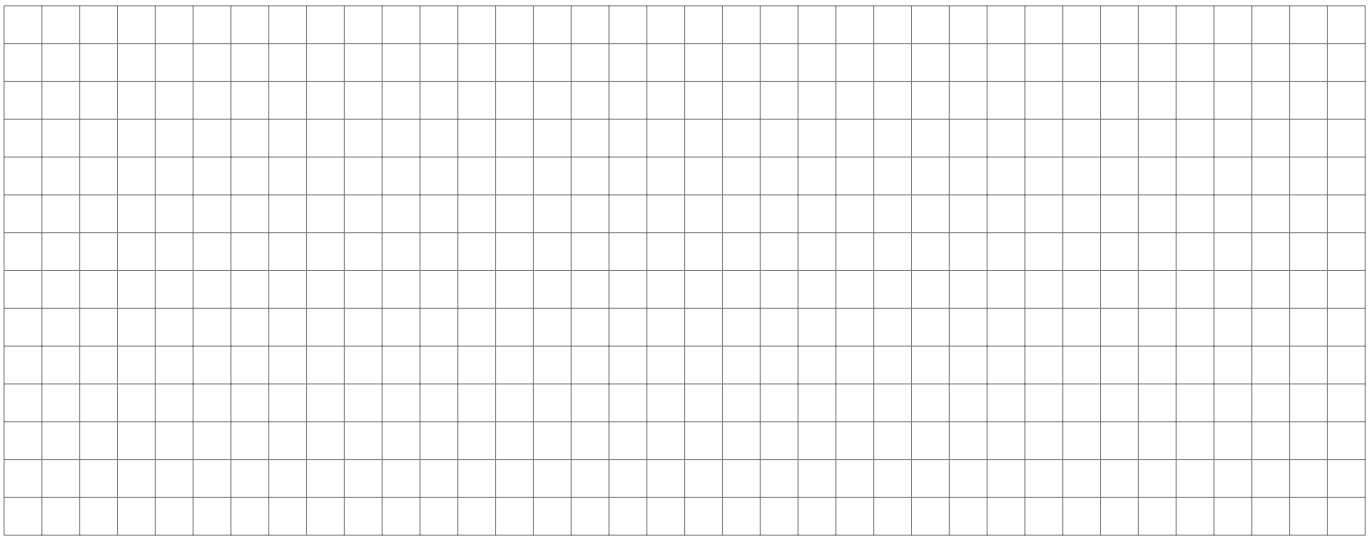
(5) $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$

Démonstration. La première affirmation est intuitivement claire : il n'y a aucun élément qui appartient à la fois à X et à l'ensemble vide puisqu'aucun élément ne se trouve dans l'ensemble vide. Formellement on peut démontrer cela en remarquant que $X \cap \emptyset \subset \emptyset$. Le seul sous-ensemble de $\emptyset$ est $\emptyset$ ce qui termine la démonstration.

La deuxième affirmation peut par exemple se comprendre en observant le diagramme de Venn d'une triple intersection.







□

C'est la première fois dans ce cours que je termine une démonstration en l'indiquant par un carré en fin de ligne. On peut utiliser d'autres symboles, mais c'est agréable de voir à l'avance où la preuve se terminera. De plus j'aime particulièrement le carré car on le dessine en quatre petits traits, qui rappellent les quatre lettres de "CQFD" (ce qu'il fallait démontrer).

Définition 2.7. Soient X et Y deux ensembles. La *différence* de X et Y, notée $X - Y$, ou parfois aussi $X \backslash Y$, est l'ensemble $X - Y = \{x \in X \mid x \notin Y\}$. Si $A \subset X$, le *complémentaire* de A dans X est l'ensemble $X - A$. On le note A^c si le contexte est clair.

On a en particulier $X - X = \emptyset$ et $X - \emptyset = X$.

Exemple 2.8. Considérons les ensembles $X = \{$Genève ; Delémont ; Lausanne ; Berne$\}$ et $Y = \{$ Berne ; Fribourg ; Genève ; Sion ; Aarau $\}$, alors $X - Y = \{$ Delémont ; Lausanne$\}$ et $Y - X = \{$Fribourg ; Sion ; Aarau$\}$.

Chapitre 2

Les nombres naturels

Nous étudions dans ce chapitre les nombres naturels et en particulier les notions de multiple et de diviseur, ce qui nous amènera tout naturellement aux nombres premiers. Nous ne construisons pas les nombres naturels dans ce cours et ne démontrons donc pas les propriétés élémentaires de la première section ci-dessous.

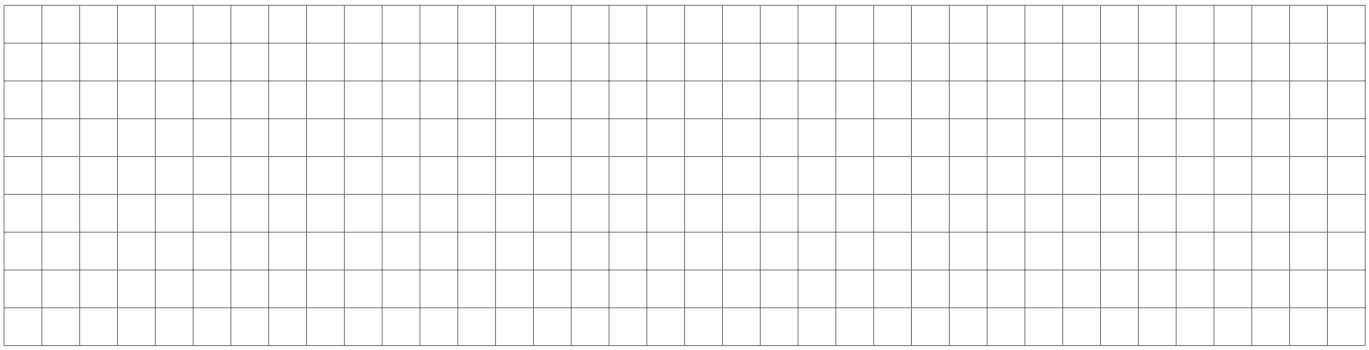
1. L'ensemble des entiers naturels

Pour préparer le terrain nous rappelons quelques faits sur les entiers naturels $\mathbb{N} = \{0; 1; 2; 3; 4; \dots\}$. C'est un ensemble infini muni d'une addition et d'une multiplication. Ces opérations vérifient les cinq propriétés suivantes.

Proposition 1.1. *Soient m, n, k des nombres naturels.*

(i)	*(Associativité)*	$(m+n)+k = m+(n+k)$	*et* $(m \cdot n) \cdot k = m \cdot (n \cdot k)$
(ii)	*(Commutativité)*	$m+n = n+m$	$m \cdot n = n \cdot m$
(iii)	*(Elément neutre)*	$m+0 = m$	$m \cdot 1 = m$
(iv)	*(0 est absorbant)*	$m \cdot 0 = 0$	
(v)	*(Distributivité)*	$m \cdot (n+k) = m \cdot n + m \cdot k$	

Exemple 1.2. La distributivité est illustrée par le principe bien connu de la multiplication en colonnes. On se demande combien il y a d'heures dans une année.



Lorsqu'on multiplie plusieurs fois un nombre naturel n par lui-même, il est pratique d'utiliser la notation en puissance. On pose par définition $n^0 := 1$.

Notation 1.3. Pour tout $k \in \mathbb{N}$ différent de zéro, on pose

$$n^k := \underbrace{n \cdot n \cdot \ldots \cdot n}_{k \text{ facteurs}}$$

L'une des propriétés remarquables des puissances est que

$$n^k \cdot n^l = n^{k+l}$$

puisque le produit de k copies de n avec celui de l copies de n est exactement le produit de $k+l$ copies de n. Par exemple $3^2 \cdot 3^3 = 9 \cdot 27 = 243 = 3^5$. C'est pour que cette propriété soit satisfaite pour tous les entiers naturels k et l que nous devons poser $n^0 = 1$.

2. Soustraction et division

La soustraction n'est pas à proprement parler une opération sur $\mathbb{N}$ car elle peut « sortir » de $\mathbb{N}$. Par exemple,

$$7 - 3 = 4 \in \mathbb{N}, \text{ mais } 3 - 7 \text{ n'est pas défini dans } \mathbb{N}.$$

Définition 2.1. Soient $m, n \in \mathbb{N}$. On dit que m est *plus petit (ou égal)* à n, ce qui se note $m \leq n$, s'il existe un nombre naturel k tel que

$$n = m + k. \tag{1}$$

On dit que m est *strictement plus petit* que n, ce qui se note $m < n$, si $m \leq n$ et $m \neq n$. On note $m \geq n$ pour $n \leq m$ et on dit que m est *plus grand (ou égal)* à n.

Remarque 2.2. Lorsque $m \leq n$, le nombre k de l'égalité (1) est uniquement déterminé par m et n.

Définition 2.3. Soient $m, n \in \mathbb{N}$ tels que $m \leq n$. La *différence* de n et m, notée $n - m$, est l'unique nombre naturel k vérifiant $n = m + k$.

Des propriétés de l'addition on déduit les propriétés suivantes de la soustraction.

Proposition 2.4. *Soient $m, n, k \in \mathbb{N}$. Alors*

(1) $m - (n + k) = (m - n) - k$, *si* $n + k \leq m$.

(2) $m - (n - k) = (m + k) - n$ *si* $k \leq n$ *et* $n - k \leq m$.

(3) $m + (n - k) = (m + n) - k$ *si* $k \leq n$.

(4) $m \cdot (n - k) = m \cdot n - m \cdot k$ *si* $k \leq n$.

(5) $m - 0 = m$ *et* $m - m = 0$.

Exemple 2.5. On a par exemple

$$11 - (5 + 3) = 11 - 8 = 3 = 6 - 3 = (11 - 5) - 3$$

Pour illustrer la quatrième propriété on a par exemple

$$3 \cdot (25 - 21) = 3 \cdot 4 = 12 = 75 - 63 = 3 \cdot 25 - 3 \cdot 21$$

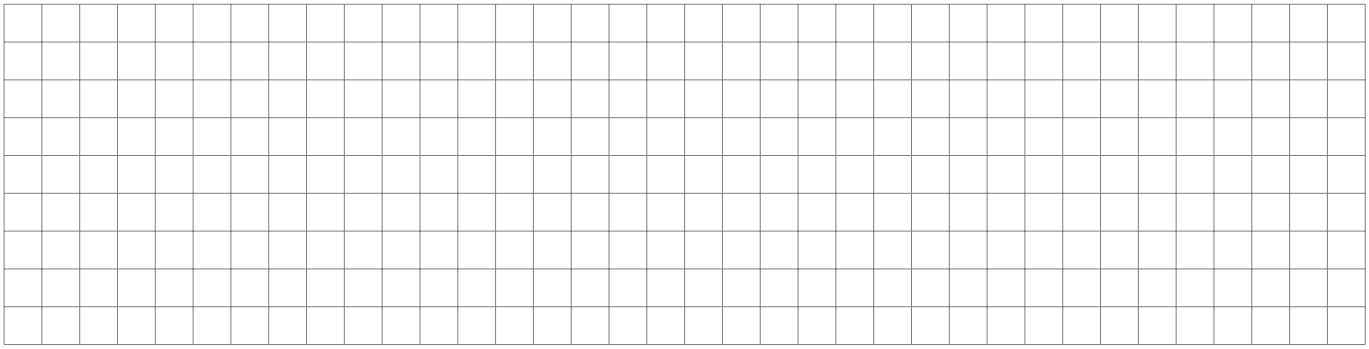
La division n'est pas non plus une opération sur $\mathbb{N}$ pour la même raison : elle n'est pas toujours définie. Par exemple,

$$8 : 2 = 4 \in \mathbb{N}, \text{ mais } 8 : 3 \text{ n'est pas défini dans } \mathbb{N}.$$

Définition 2.6. Soient $m, n \in \mathbb{N}$. On dit que m *divise* n (ou m est un *diviseur* de n, ou encore n est *divisible* par m) s'il existe un nombre naturel k tel que $n = m \cdot k$. On note $m \mid n$ cette affirmation.

Exemple 2.7. Le nombre 15 est divisible par 3, mais pas par 2. Le nombre 0 ne divise aucun autre nombre sauf lui-même. En effet $0 = 0 \cdot 1$, mais pour $n \neq 0$, on n'a jamais $n = 0 \cdot k$.

Remarque 2.8. Si $m \mid n$ et $m \neq 0$, alors il existe un unique nombre naturel k tel que $n = m \cdot k$.



Définition 2.9. Soient $m, n \in \mathbb{N}$ tels que $m \mid n$ et $m \neq 0$. Le *quotient* de n par m, noté $n : m$, est l'unique nombre naturel k tel que $n = m \cdot k$.

De la même façon que les propriétés de l'addition expliquent celles de la soustraction, les propriétés de la multiplication ont des conséquences pour la division. Il est utile de penser à une situation concrète pour garder à l'esprit le sens de ces égalités et ne pas être tenté de manipuler ces opérations en oubliant ce qu'elles signifient. Par exemple pour la propriété (1), j'aime penser à une tarte que l'on divise en $6 = 2 \cdot 3$. C'est équivalent à partager la tarte en 2, puis chaque moitié en 3.

Proposition 2.10. *Soient $m, n, k \in \mathbb{N}$. Alors*

(1) $m : (n \cdot k) = (m : n) : k$, *si* $n \cdot k \mid m$.

(2) $m : (n : k) = (m \cdot k) : n$ *si* $k \mid n$ *et* $(n : k) \mid m$.

(3) $m \cdot (n : k) = (m \cdot n) : k$ *si* $k \mid n$.

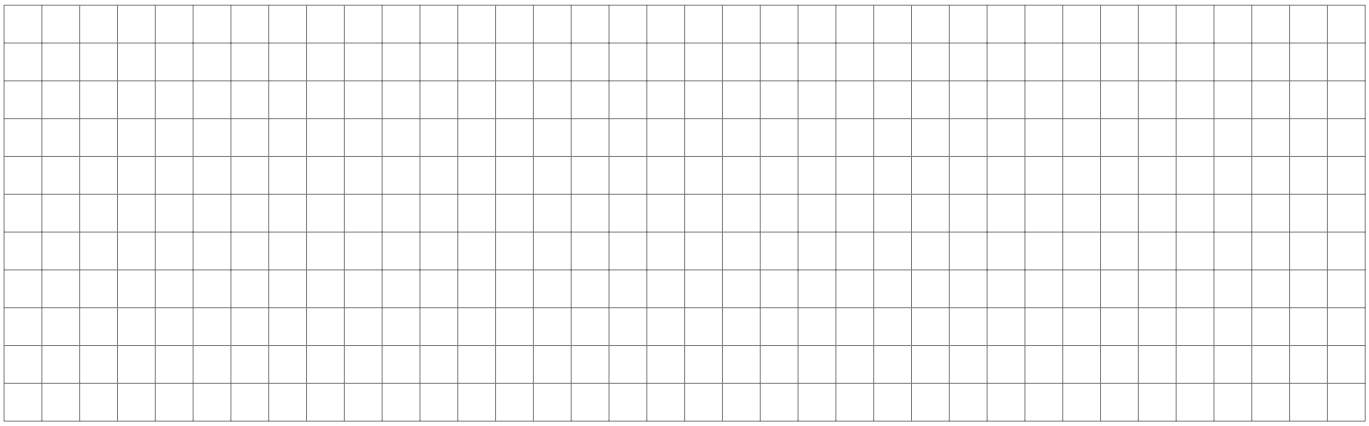
(4) Simplification : $(m \cdot n) : (m \cdot k) = n : k$ *si* $k \mid n$.

(5) $m : 1 = m$ *et* $m : m = 1$.

DÉMONSTRATION. *de la partie (4).* Puisque k divise n, il existe un nombre naturel q tel que $n = k \cdot q$. Alors

$$m \cdot n = m \cdot (k \cdot q) = (m \cdot k) \cdot q$$

ce qui montre que $(m \cdot n) : (m \cdot k) = q = n : k$. □



Remarque 2.11. Nous avons vu au début de ce chapitre les propriétés d'associativité, de commutativité, etc. de la somme et du produit des nombres naturels. Nous avons aussi remarqué que l'union et l'intersection d'ensembles satisfont à des propriétés analogues. Ceci justifie l'introduction de la notion suivante. Un ensemble X, muni de deux opérations $\star$ et $\circ$ vérifiant les propriétés (1)-(5) ci-dessous s'appelle un *semi-anneau commutatif.*

(1) Associativité : $(x \star y) \star z = x \star (y \star z)$ et $(x \circ y) \circ z = x \circ (y \circ z)$ pour tous $x, y, z \in X$.

(2) Commutativité : $x \star y = y \star x$ et $x \circ y = y \circ x$ pour tous $x, y \in X$.

(3) Eléments neutres : Il existe des éléments $e, \eta \in X$ tels que $x \star e = x$ et $x \circ \eta = x$ pour tous $x \in X$.

(4) e est absorbant pour $\circ$: pour tout $x \in X$, on a $x \circ e = e$.

(5) Distributivité : $x \circ (y \star z) = x \circ y \star x \circ z$ pour tous $x, y, z \in X$.

L'ensemble $\mathbb{N}$ muni des opération $+$ et $\cdot$ est un semi-anneau commutatif. Etant donné un ensemble X, son ensemble des parties $\mathcal{P}(X)$ muni des opérations $\cup$ et $\cap$ aussi.

Pour bien comprendre ce que les cinq propriétés ci-dessus veulent dire dans cette situation, il faut donc penser que les éléments x, y, z sont des sous-ensembles de X, disons A, B et C. Pour bien lire les propriétés il faudra ensuite remplacer chaque $\star$ par un symbole d'union $\cup$ et chaque $\circ$ par un symbole d'intersection $\cap$. La distributivité par exemple signifie dans cette situation que

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

C'est ce que nous avons vu dans la Proposition 2.6 (5).

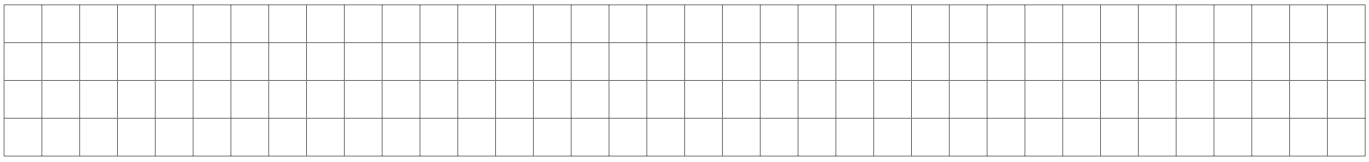
3. Multiples et multiples communs

Nous passons maintenant à l'étude des diviseurs et des multiples d'un nombre naturel donné, une section où la théorie des ensembles nous sera bien utile...

Définition 3.1. Soient $m, n \in \mathbb{N}$. Le nombre m est *multiple* de n si n est un diviseur de m, c'est-à-dire s'il existe un nombre naturel k tel que $m = n \cdot k$.

On note M_n l'ensemble des multiples de $n \in \mathbb{N}$:

$$\begin{aligned} M_n &= \{m \in \mathbb{N} \mid \text{il existe } k \in \mathbb{N} \text{ tel que } m = n \cdot k\} \\ &= \{0; n; 2 \cdot n; 3 \cdot n; 4 \cdot n; \ldots\} \end{aligned}$$

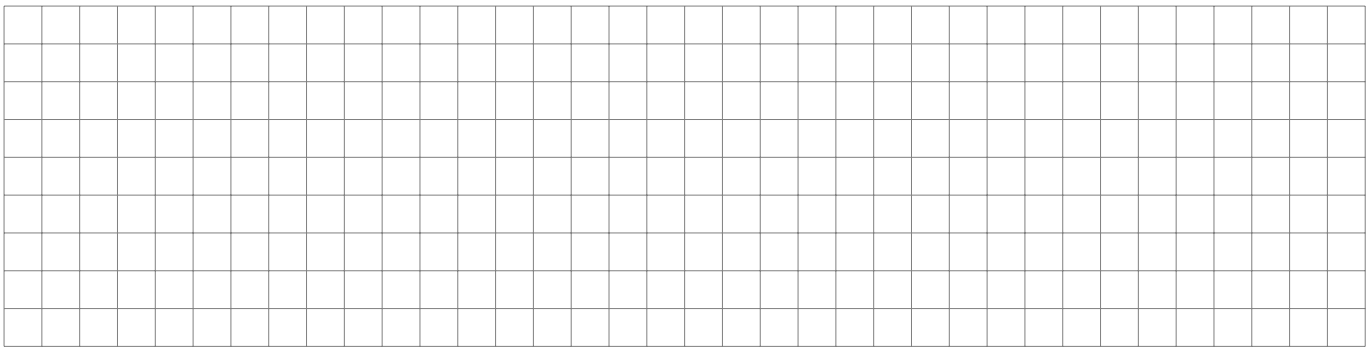


Définition 3.2. Soient $m, n \in \mathbb{N}$. Le nombre k est un *multiple commun* de m et n si c'est un multiple de m et un multiple de n. L'ensemble des multiples communs de m et n est donc l'intersection $M_m \cap M_n$.

Exemple 3.3. Le nombre 15 est un multiple de 3, mais pas de 6. Ce n'est donc pas un multiple commun de 3 et 6. Il s'agit par contre d'un multiple commun de 3 et 5. On a deux cas très particuliers d'ensembles de multiples, $M_1 = \mathbb{N}$ et $M_0 = \{0\}$.

Définition 3.4. Soient $m, n \in \mathbb{N}$ des nombres non nuls. Le *plus petit multiple commun* de m et n, noté $\text{ppmc}(m, n)$, est le plus petit nombre entier naturel non nul qui est un multiple de m et de n. Si m ou n est égal à zéro, alors $\text{ppmc}(m, n) = 0$.

Les exemples suivants indiquent que le ppmc de m et n est "au pire" égal au produit $m \cdot n$, mais qu'il peut être plus petit, auquel cas c'est un diviseur de $m \cdot n$.

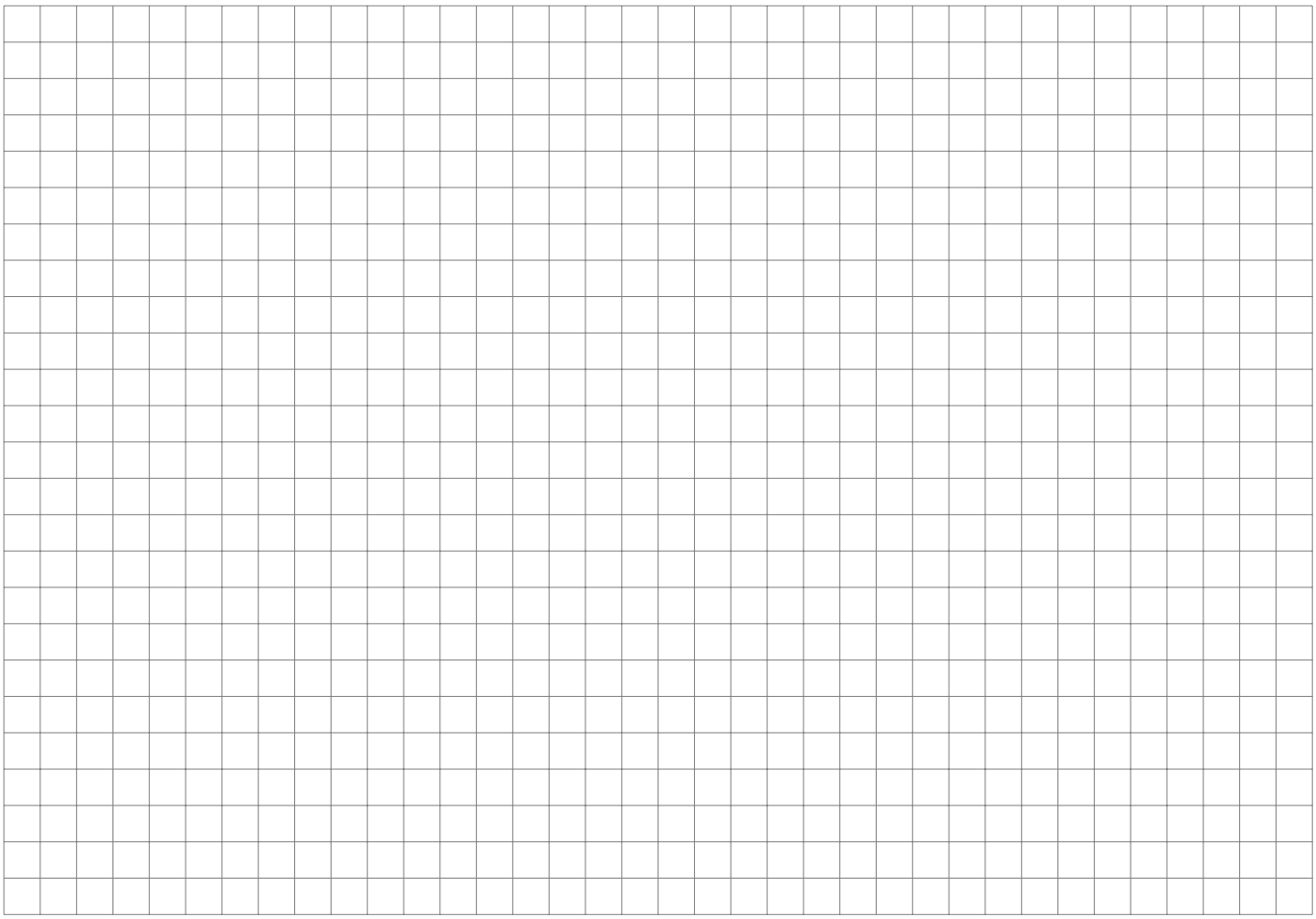


Proposition 3.5. *Soient $m, n \in \mathbb{N}$. Alors $M_m \cap M_n = M_{\text{ppmc}(m,n)}$.*

Démonstration. Pour démontrer l'égalité de ces deux ensembles nous appliquons le *principe de la double inclusion*. Pour commencer le ppmc de m et n est un

multiple commun de m et n. Ainsi $M_{\text{ppmc}(m,n)} \subset M_m$ et $M_{\text{ppmc}(m,n)} \subset M_n$, si bien que $M_{\text{ppmc}(m,n)}$ est contenu dans l'intersection.

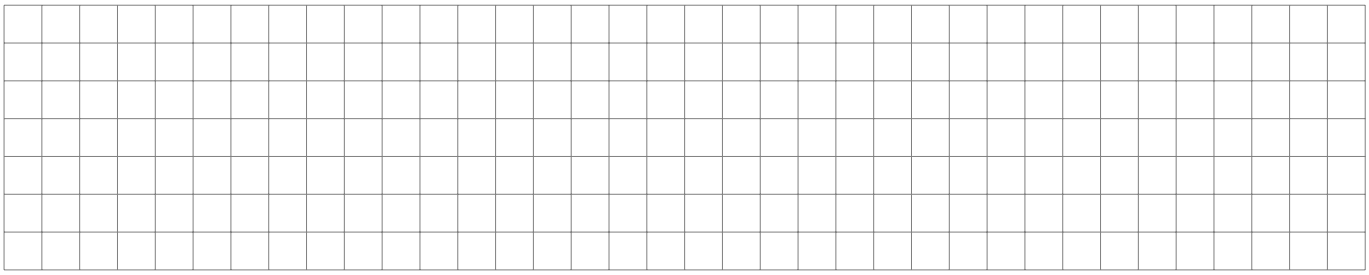
Pour montrer l'égalité il faut encore montrer l'inclusion $M_m \cap M_n \subset M_{\text{ppmc}(m,n)}$. La traduction française : Si k est un multiple de m et de n, alors c'est un multiple du ppmc de m et n.



□

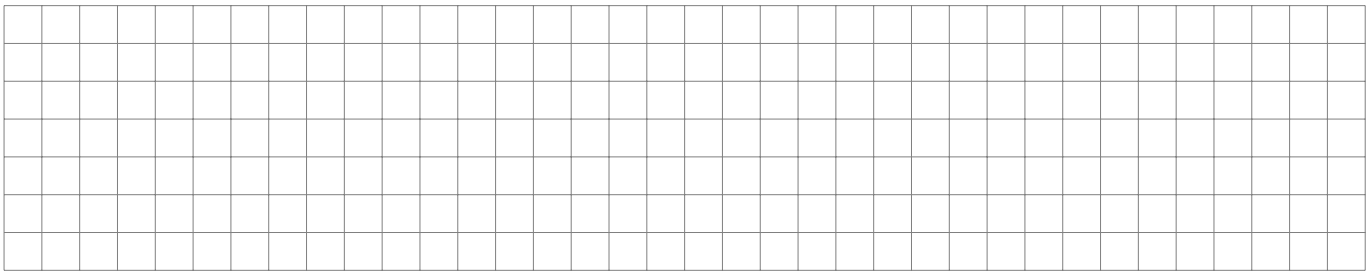
4. Diviseurs et diviseurs communs

L'ensemble des diviseurs d'un nombre naturel n est noté D_n. Lorsque $n = 0$, on a $D_0 = \mathbb{N}$. Sinon, l'ensemble D_n est un ensemble fini de nombres naturels . Par exemple le nombre 0 n'est un diviseur d'aucun nombre naturel, sauf de 0 lui-même.



Définition 4.1. Soient $m, n \in \mathbb{N}$. Le nombre k est un *diviseur commun* de m et n s'il divise m et divise n. L'ensemble des diviseurs communs de m et n est donc l'intersection $D_m \cap D_n$.

On pourrait aussi se représenter les exemples suivants par des diagrammes de Venn en tous points semblables à ceux des multiples.



Définition 4.2. Soient $m, n \in \mathbb{N}$. Si m ou n est non nul, le *plus grand diviseur commun* de m et n est le plus grand nombre naturel, noté $\text{pgdc}(m, n)$, qui est à la fois un diviseur de m et un diviseur de n. Lorsque $m = n = 0$, on pose $\text{pgdc}(m, n) = 0$.

Nous avons par exemple $\text{pgdc}(8, 24) = 8$ et $\text{pgdc}(36, 24) = 12$.

Proposition 4.3. *Soient $m, n \in \mathbb{N}$. Alors, $D_m \cap D_n = D_{\text{pgdc}(m,n)}$.*

5. Les nombres premiers

Nous terminons la leçon avec une liste des critères de divisibilité dont nous avons parlé la première semaine. Saurais-tu tous les démontrer ?

Critères de divisibilité

Un nombre naturel se divise par :

2	s'il se termine par 0, 2, 4, 6 ou 8 ; on dit alors qu'il est pair
3	si la somme de ses chiffres se divise par 3
4	si le nombre formé par ses deux derniers chiffres se divise par 4, notamment s'il se termine par 00
5	s'il se termine par 0 ou par 5
6	s'il se divise par 2 et par 3
9	si la somme de ses chiffres se divise par 9
10	s'il se termine par 0
25	s'il se termine par 00, 25, 50 ou 75
50	s'il se termine par 00 ou 50

Définition 5.1. Un nombre naturel p est *premier* s'il a exactement deux diviseurs.

Observons en particulier que le nombre 1 n'est pas premier, un fait qui prendra son importance dans le Théorème fondamental.

Nombre premier – liste des nombres premiers inférieurs à 1000

2	101	211	307	401	503	601	701	809	907
3	103	223	311	409	509	607	709	811	911
5	107	227	313	419	521	613	719	821	919
7	109	229	317	421	523	617	727	823	929
11	113	233	331	431	541	619	733	827	937
13	127	239	337	433	547	631	739	829	941
17	131	241	347	439	557	641	743	839	947
19	137	251	349	443	563	643	751	853	953
23	139	257	353	449	569	647	757	857	967
29	149	263	359	457	571	653	761	859	971
31	151	269	367	461	577	659	769	863	977
37	157	271	373	463	587	661	773	877	983
41	163	277	379	467	593	673	787	881	991
43	167	281	383	479	599	677	797	883	997
47	173	283	389	487		683		887	
53	179	293	397	491		691			
59	181			499					
61	191								
67	193								
71	197								
73	199								
79									
83									
89									
97									

Les deux diviseurs d'un nombre premier sont donc 1 et lui-même. C'est le cas de 31 que nous avons rencontré tout-à-l'heure, mais pas du nombre 1, qui n'est donc pas premier.

Remarque 5.2. La distribution exacte des premiers parmi les naturels reste un mystère jusqu'à ce jour. C'est le sujet de la conjecture de Riemann, probablement le plus célèbre problème mathématique non résolu.

Le plus grand nombre premier connu à ce jour (2016, source : Wikipedia) est un nombre dit « de Mersenne »(du type $2^n - 1$). Ce nombre découvert en 2016 a $22'338'618$ chiffres. Il s'agit de $2^{74'207'281} - 1$. Pour l'écrire il faudrait un cahier de près de 400 pages à raison de 50 lignes de 66 caractères par page !

THÉORÈME 5.3. **Théorème fondamental de l'arithmétique** *Tout nombre naturel $n \geq 2$ admet une décomposition en produit de facteurs premiers, unique à permutation des facteurs près. Autrement dit, il existe des premiers distincts et uniques $p_1, \ldots, p_k$ et des entiers naturels $r_1 > 0, \ldots, r_k > 0$ tels que*

$$n = p_1^{r_1} \cdot \ldots \cdot p_k^{r_k}$$

Par exemple, le nombre $362'880$ se décompose comme $2^7 \cdot 3^4 \cdot 5 \cdot 7$. En effet, les divisions successives par des diviseurs évidents donnent

$$\begin{aligned} 362'880 &= 10 \cdot 36'288 = 2 \cdot 5 \cdot 4 \cdot 9072 \\ &= 2^3 \cdot 5 \cdot 4 \cdot 2268 = 2^5 \cdot 5 \cdot 4 \cdot 567 \\ &= 2^7 \cdot 5 \cdot 9 \cdot 63 = 2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 9 = 2^7 \cdot 3^4 \cdot 5 \cdot 7 \end{aligned}$$

Ce théorème s'applique au calcul du ppmc et du pgdc, comme nous l'avons vu en exercices.

Corollaire 5.4. *Soient $m, n \geq 2$ des nombres naturels. Soient $m = p_1^{l_1} \cdot \ldots \cdot p_i^{l_i}$ et $n = q_1^{k_1} \cdot \ldots \cdot q_j^{k_j}$ leurs décompositions en produit de facteurs premiers. Alors leur ppmc est le produit des facteurs premiers apparaissant dans la décomposition de m ou de n avec le plus grand exposant. Leur pgdc est le produit des facteurs premiers apparaissant dans la décomposition de m et n avec le plus petit exposant. S'il n'y a pas de facteurs communs, alors le pgdc vaut* 1.

Exemple 5.5. Nous voulons calculer le ppmc et le pgdc de $362'880$ et $1'100$.

Une autre conséquence importante du Théorème fondamental est le premier résultat sur la répartition des nombres premiers, dû à Euclide, III^{e} siècle av. J.-C (vers -300, vous voyez qu'il nous faut des nombres négatifs !). La preuve se fait par l'absurde, un concept très important en mathématique. Nous allons donc supposer *par l'absurde* que le résultat est faux. La démonstration sera terminée lorsque nous arriverons à une contradiction, ce qui prouvera donc que l'hypothèse ne pouvait être vraie. Nous avons vu en exercices que l'implication $A \Rightarrow B$ est équivalente à $non(B) \Rightarrow non(A)$. Autrement dit, si B est fausse, alors A ne peut être vraie.

THÉORÈME 5.6. *Il existe une infinité de nombres premiers.*

Cette démonstration est en fait celle d'Euclide.

Chapitre 3

Les nombres entiers relatifs

Notre but théorique est d'ajouter des nombres négatifs aux nombre naturels pour pouvoir parler de soustraction sans devoir faire d'hypothèse. Il y a bien sûr aussi un but pratique puisque les nombres négatifs apparaissent dans la nature. Ne dit-on pas "trois kilomètres derrière nous", "il y a deux heures",'un découvert de 3000 CHF sur mon compte en banque", "à $-10'000$ m dans la fosse des Mariannes" ou encore "il fait $-40°C$ en hiver au Canada" ?

1. Construction des entiers relatifs

Nous allons maintenant étendre l'ensemble des naturels et leurs opérations d'addition et de multiplication de sorte que la soustraction soit toujours définie. Pour cela nous devons ajouter des inverses additifs aux nombres naturels non nuls. Ainsi, pour chaque $n \in \mathbb{N}$, $n \neq 0$, nous ajouterons un nombre, noté $-n$ (pour 0, on pose $-0 = 0$) et étendrons l'addition de $\mathbb{N}$ de sorte que $n + (-n) = 0$. Par conséquent la soustraction sera toujours définie.

Définition 1.1. Un *nombre entier (relatif) a* consiste en la donnée d'un nombre naturel n, sa *valeur absolue*, et d'un symbole $+$ ou $-$, son *signe*. On note

$$a = (+n) \text{ ou } a = (-n)$$

et on dit qu'un nombre entier est *positif* si son signe est $+$, *négatif* sinon. On pose $(+0) = (-0)$ qu'on note simplement 0. L'ensemble des entiers, noté $\mathbb{Z}$, est donc

$$\mathbb{Z} = \{\ldots, (-4), (-3), (-2), (-1), 0, (+1), (+2), (+3), (+4), \ldots\}$$

Nous allégerons bientôt la notation en enlevant les parenthèses, mais pour l'instant nous voulons bien distinguer un nombre entier d'un nombre naturel.

2. L'addition

Nous voulons maintenant étendre la somme de $\mathbb{N}$ à $\mathbb{Z}$, c'est-à-dire construire une somme dans $\mathbb{Z}$ de sorte que la somme de deux nombres entiers relatifs positifs coïncide avec la somme des entiers naturels correspondants que nous connaissons.

Plus précisément nous verrons qu'il existe une unique manière de définir une opération + sur $\mathbb{Z}$ de sorte que :

- elle se restreigne à l'addition de $\mathbb{N}$ sur les positifs,
- elle soit associative,
- $(+m) + (-m) = 0$ pour tout $m \in \mathbb{N}$.

Pour la définir nous devons expliquer comment calculer la somme de deux entiers, chacun d'entre eux pouvant être positif ou négatif. Il y a donc quatre cas à prendre en considération.

Définition 2.1. Soient $m, n \in \mathbb{N}$.

(1)

$$(+m) + (+n) = (+(m+n)).$$

(2)

$$(+m) + (-n) = \begin{cases} (+(m-n)) & \text{si } m \geq n, \\ (-(n-m)) & \text{si } n > m. \end{cases}$$

(3)

$$(-m) + (+n) = \begin{cases} (+(n-m)) & \text{si } n \geq m, \\ (-(m-n)) & \text{si } m > n. \end{cases}$$

(4)

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

Le point (1) nous assure que cette addition étend celle de $\mathbb{N}$.

Cette définition est la bonne puisque toutes les belles propriétés de l'addition des entiers naturels sont préservées. Au lieu d'expliquer comme dans l'exemple précédent pourquoi nous sommes obligés de définir l'addition comme nous le faisons, nous travaillons maintenant avec cette définition, que nous acceptons, et nous en déduisons les propriétés souhaitées.

Proposition 2.2. *L'addition dans $\mathbb{Z}$ a les propriétés suivantes :*

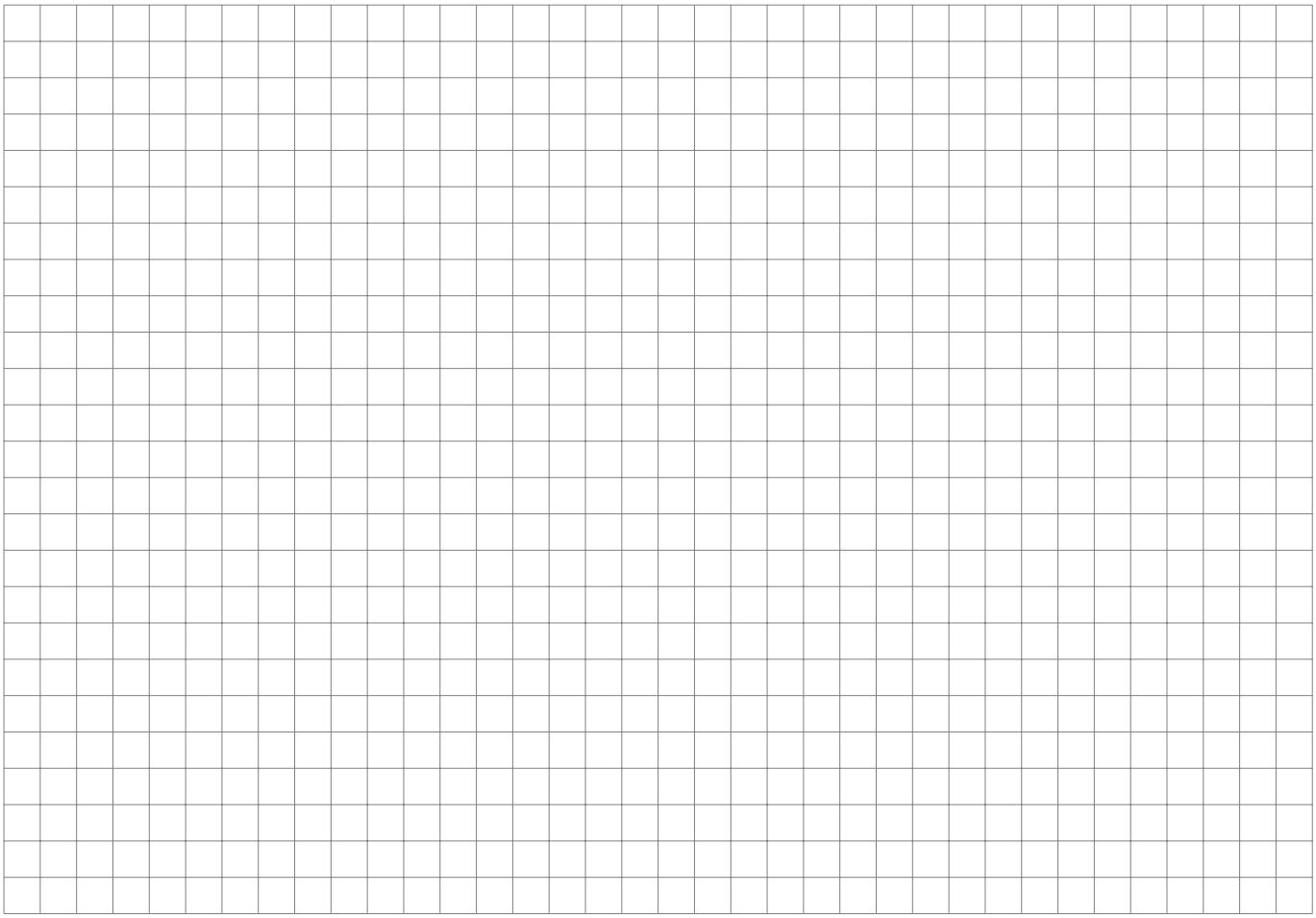
(1) Associativité : pour tous $a, b, c \in \mathbb{Z}$, on a $(a + b) + c = a + (b + c)$.

(2) Elément neutre 0 : pour tout $a \in \mathbb{Z}$, $a + 0 = a = 0 + a$.

(3) Commutativité : pour tous $a, b \in \mathbb{Z}$, on a $a + b = b + a$.

(4) Existence de l'opposé : pour tout entier a, il existe un unique entier noté $-a$, appelé l'opposé de a, tel que $a + (-a) = 0$.

Démonstration. Aucun point n'est compliqué, mais tous sont un peu laborieux. Pour l'associativité par exemple il faudrait vérifier les huit cas possibles selon que a, b et c sont des entiers positifs ou négatifs. Et lorsque deux entiers relatifs n'ont pas le même signe, on doit encore distinguer plusieurs sous-cas selon laquelle des valeurs absolues est la plus grande.



L'élément neutre est $(+0)$ que nous notons donc 0 dès maintenant. La commutativité est plus simple à vérifier que l'associativité, elle découle de la commutativité de l'addition dans $\mathbb{N}$ lorsque a et b ont le même signe et de la comparaison des formules (2) et (3) lorsqu'ils ont des signes opposés. Quant à l'opposé il est donné, pour tout $m \in \mathbb{N}$, par $-0 = 0$, $-(+m) = (-m)$ et $-(-m) = (+m)$. En effet $0 + 0 = 0$ ce qui force -0 à être égal à 0, et par exemple $(+11) + (-11) = (+0) = 0$ ce qui implique $-(+11) = (-11)$. □

Un ensemble X muni d'une opération vérifiant les propriétés (i) à (iv) s'appelle un *groupe abélien*. Nous en verrons sans cesse en mathématiques, aussi bien en algèbre qu'en géométrie !

Remarque 2.3. Soit $a \in \mathbb{Z}$. Quand on regarde la valeur absolue de a comme un entier (positif), on la note $|a|$. Donc, pour tout $m \in \mathbb{N}$, $|(+m)| = (+m)$ et

$|(-m)| = (+m)$. Autrement dit,

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

Par exemple $|(+11)| = (+11)$ et $|(-11)| = (+11)$.

3. La soustraction

Tout le travail que nous avons effectué avait un but : La soustraction existe toujours dans $\mathbb{Z}$.

Proposition 3.1. *Pour tous $a, b \in \mathbb{Z}$, il existe un unique $c \in \mathbb{Z}$ tel que $a = b + c$.*

Ce nombre, noté $a - b$, est appelé la *différence* de a et b. Il est donné par $a - b = a + (-b)$. Pour démontrer la proposition il suffit de vérifier que ce nombre vérifie bien l'égalité souhaitée :

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

Voici le slogan dont il faut se souvenir :

Dans $\mathbb{Z}$, *soustraire c'est additionner l'opposé.*

Définition 3.2. Soient a et b des nombres relatifs. On dit que a est *plus petit (ou égal)* à b, ce qui se note $a \leq b$, s'il existe un nombre entier *positif* c tel que $b = a + c$.

En d'autres termes $a \leq b$ si et seulement si $b - a$, qui existe toujours, est positif.

Exemple 3.3. Un nombre entier relatif a est positif si et seulement $a \geq 0$.

4. Multiplication et division

Pour définir le produit de deux nombres entiers, nous devons à nouveau considérer quatre cas, selon le signe de chacun des deux nombres. Par exemple, si le premier est positif et le second est négatif, on pose $(+m) \cdot (-n) = (-(m \cdot n))$. Le produit de deux nombres négatifs est positif, par exemple $(-11) \cdot (-12) = (+132)$.

Il existe une unique manière de définir une multiplication sur $\mathbb{Z}$ qui étende celle de $\mathbb{N}$ et qui soit distributive sur l'addition.

Définition 4.1. Soient $m, n \in \mathbb{N}$.

(1) $(+m) \cdot (+n) = +(m \cdot n)$

(2) $(-m) \cdot (+n) = -(m \cdot n)$

(3) $(+m) \cdot (-n) = -(m \cdot n)$

(4) $(-m) \cdot (-n) = +(m \cdot n)$

Proposition 4.2. Propriétés de la multiplication. *La multiplication dans $\mathbb{Z}$ a les propriétés suivantes :*

(1) Associativité : $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ pour tous $a, b, c \in \mathbb{Z}$.

(2) Commutativité : $a \cdot b = b \cdot a$ pour tous $a, b \in \mathbb{Z}$.

(3) $(+1)$ est l'élément neutre : $a \cdot (+1) = a$ pour tout $a \in \mathbb{Z}$.

(4) Distributivité sur l'addition : $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ pour tous $a, b, c \in \mathbb{Z}$.

Remarque 4.3. Un ensemble X muni de deux opérations $+$ et $\cdot$ vérifiant les quatre propriétés d'addition vue la semaine passée et les quatre propriétés de multiplication ci-dessus s'appelle un *anneau commutatif*.

Notons qu'un anneau commutatif est toujours un semi-anneau commutatif. On demande plus à un anneau qu'à un semi-anneau (l'existence d'opposés), et la seule propriété exigée pour un semi-anneau qui n'apparaît pas dans la définition d'anneau est le fait que le zéro de l'addition est absorbant. Ceci est automatique (preuve en exercice). Pour tous $a, b \in \mathbb{Z}$, ($a = 0$ ou $b = 0$) $\Rightarrow a \cdot b = 0$ puisque 0 est absorbant. Il s'avère que la réciproque est aussi vraie :

Proposition 4.4. *L'anneau des entiers relatifs $\mathbb{Z}$ est* intègre*, c'est-à-dire que pour tous $a, b \in \mathbb{Z}$, $a \cdot b = 0 \Rightarrow a = 0$ ou $b = 0$.*

DÉMONSTRATION. On se base sur le fait que c'est vrai dans $\mathbb{N}$: pour tous $m, n \in \mathbb{N}$, si $m \cdot n = 0$, alors soit $m = 0$, soit $n = 0$. Soient maintenant $a, b \in \mathbb{Z}$ et supposons que $a \cdot b = 0$. Quels que soient les signes de a et b, la valeur absolue de $a \cdot b$ est le produit des valeurs absolues de a et de b par définition de la multiplication dans $\mathbb{Z}$. Par la propriété de $\mathbb{N}$ qu'on vient de rappeler, il faut donc que la valeur absolue de a ou la valeur absolue de b soit nulle. Mais ceci implique que a ou b est nul. □

Définition 4.5. Soient $a, b \in \mathbb{Z}$. On dit que a *divise* b (ou a est un *diviseur* de b, ou encore b est *divisible* par a) s'il existe un nombre entier c tel que $b = a \cdot c$. On note $a \mid b$ cette affirmation.

Corollaire 4.6. *Si $a \mid b$ et $a \neq 0$, alors il existe un* unique *c tel que $b = a \cdot c$.*

Définition 4.7. Soient $a, b \in \mathbb{Z}$. Si $a \mid b$ et $a \neq 0$, alors l'unique nombre entier c tel que $b = a \cdot c$, noté $b : a$, est appelé le *quotient* de b par a.

Proposition 4.8. Propriétés de la division. *Pour tous $a, b \in \mathbb{Z}$, b est divisible par a si et seulement si $|b|$ est divisible par $|a|$. De plus, si $m, n \in \mathbb{N}$ et $n \mid m$, alors*

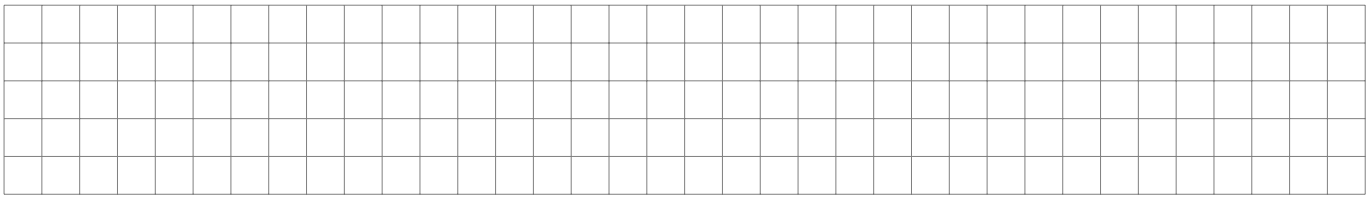
(1) $(+m) : (+n) = [+(m : n)]$

(2) $(-m) : (+n) = [-(m : n)]$

(3) $(+m) : (-n) = [-(m : n)]$

(4) $(-m) : (-n) = [+(m : n)]$

DÉMONSTRATION. Montrons (4) par exemple : $(-m) : (-n) = [+(m : n)]$.



Pour montrer (2), c'est-à-dire que $(-m) : (+n) = [-(m : n)]$ il suffit de vérifier que $[-(m : n)] \cdot (+n) = (-m)$. Calculons donc !

$$[-(m : n)] \cdot (+n) = [-((m : n) \cdot n)] = (-m)$$

par définition de la division dans $\mathbb{N}$. □

La division des entiers relatifs a donc les mêmes propriétés que celles des nombres naturels.

5. Retour à la soustraction

Pour terminer nous regardons les propriétés de la valeur absolue et revenons encore à la soustraction. La proposition suivante dit que "le produit des valeurs absolues est égal à la valeur absolue du produit".

Proposition 5.1. Propriétés de la valeur absolue. *Soient* $a, b \in \mathbb{Z}$. *Alors* $|a \cdot b| = |a| \cdot |b|$. *Lorsque* b *est divisible par* a, *alors* $|b : a| = |b| : |a|$.

Les propriétés de la soustraction que nous énonçons maintenant se déduisent directement des propriétés adéquates de l'addition et la définition de la soustraction. Saurais-tu les démontrer ?

Proposition 5.2. Propriétés de la soustraction. *La soustraction dans* $\mathbb{Z}$ *a les propriétés suivantes : pour tous* $a, b, c \in \mathbb{Z}$,

(1) $a - (b + c) = (a - b) - c$,

(2) $a - (b - c) = (a - b) + c$,

(3) $a + (b - c) = (a + b) - c$,

(4) $a \cdot (b - c) = (a \cdot b) - (a \cdot c)$,

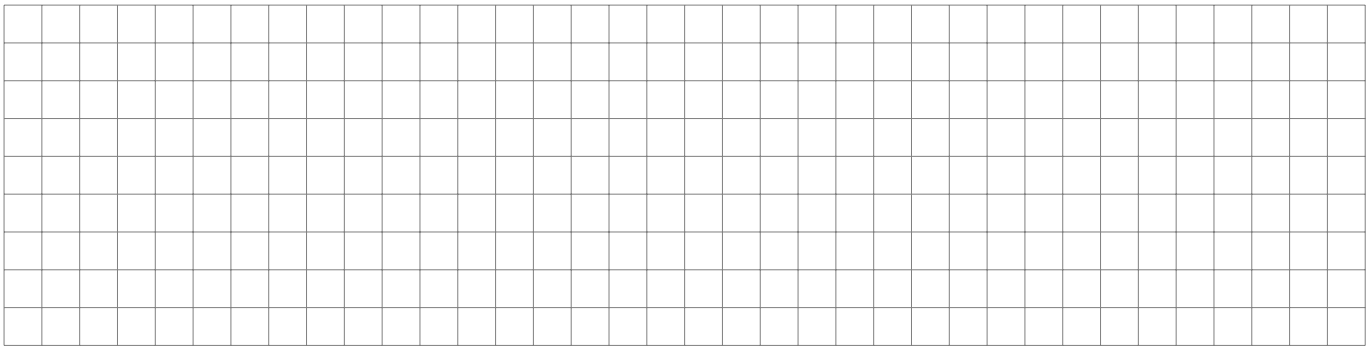
(5) $a - 0 = a$ *et* $a - a = 0$.

DÉMONSTRATION. Montrons par exemple la quatrième propriété, les autres sont du même style. Nous devons démontrer que $a \cdot (b - c) = (a \cdot b) - (a \cdot c)$, c'est-à-dire que la multiplication se distribue par rapport à la soustraction. Nous ne savons pas encore que cela est vrai, mais nous savons néanmoins que la distributivité par rapport à l'addition est vérifiée par la Proposition 4.2 (4). En observant l'égalité à prouver on constate que le terme de droite est une différence et c'est là la nouveauté de cette section.

Par définition la différence $(a \cdot b) - (a \cdot c)$ est le seul nombre entier relatif x tel que $x + (a \cdot c) = a \cdot b$. Pour montrer que $a \cdot (b - c) = x$ aussi, il faut donc démontrer que $a \cdot (b - c) + (a \cdot c) = a \cdot b$. C'est maintenant que nous avons traduit le problème que nous sommes en fait presque arrivés au bout de la preuve. Il ne reste en effet plus qu'à utiliser la distributivité :

$$a \cdot (b - c) + (a \cdot c) = a \cdot [(b - c) + c] = a \cdot b \text{ par définition de la soustraction.}$$

Nous sommes arrivés au bout de la preuve ! □



Exemple 5.3.

$$\begin{aligned}(-3) - [(+5) - (-8)] &= (-3) - [(+5) + (+8)] \\ &= (-3) - (+13) \\ &= (-3) + (-13) \\ &= (-16)\end{aligned}$$

$$\begin{aligned}[(-3) - (+5)] + (-8) &= [(-3) + (-5)] + (-8) \\ &= (-8) + (-8) \\ &= (-16)\end{aligned}$$

6. Priorité des opérations

Nous terminons le cours sur les entiers relatifs en parlant du point importantissime de la priorité des opérations et de la nécessité d'une bonne utilisation des parenthèses.

Les parenthèses sont utiles principalement pour deux raisons. Elles permettent d'une part d'indiquer et de distinguer les *signes* des opérations. D'autre part elles permettent d'indiquer dans quel *ordre* effectuer les opérations. S'il y a plusieurs parenthèse imbriquées, pour des raisons de lisibilité, on les différencie en utilisant des crochet $[\dots]$ et des accolades $\{\dots\}$. Le troisième exemple nous apprend que les barres verticales de la valeur absolue s'utilisent également comme des parenthèses (et les remplacent pour ne pas surcharger la notation).

Exemple 6.1. (1) **Signe des opérations.** On écrit $(+3)-(-2)$ et non $+3--2$. De même, on écrit $(+3)+(-2)$, $(+3)\cdot(-2)$ et $(-15):(-5)$.

(2) **Notation de l'opposé.** On écrit $-(-3)$ et $-(+5)$ et non $--3$ ni $-+5$.

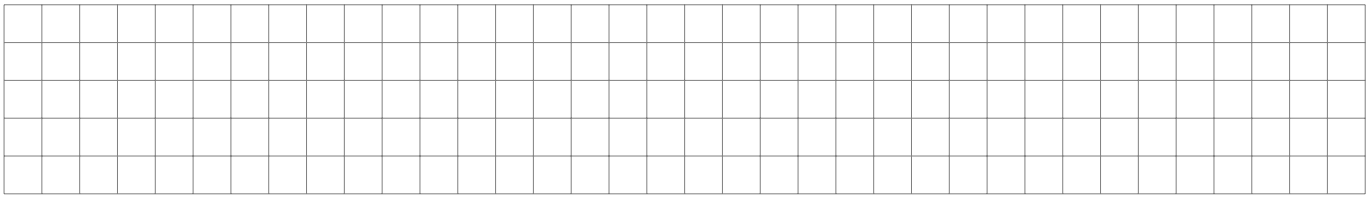
(3) **Signe et valeur absolue.** On écrit $|-8|$ et $|+7|$, mais $|(-9)-(+1)|$.

(4) **Niveau de parenthèses.** $(+3)-|\,[\{(+5)\cdot(-6)\}-(-10)]\,|=$

Dans le dernier exemple, nous effectuons, dans une expression avec parenthèses, d'abord les opérations entre parenthèses, de l'intérieur vers l'extérieur. On peut aussi déplacer les parenthèses avant de faire le calcul en utilisant les propriétés des opérations. Par exemple $[(+6)\cdot(-3)]-[(+4)\cdot(-6)]$ par commutativité de la multiplication s'écrit aussi

Certaines parenthèses ne sont pas utiles car l'ordre dans lequel on fait le calcul ne change pas le résultat. Ceci provient des propriétés particulières des opérations. Dans ce cas, on n'écrit pas les parenthèses, car le lecteur peut choisir la priorité. On dit que ces parenthèses sont *superflues*. L'associativité de l'addition et de la multiplication permettent d'introduire la règle de simplification suivante :

Règle de simplification (Associativité généralisée) : dans une expression ne contenant que des additions ou que des multiplications, aucune parenthèse n'est nécessaire.



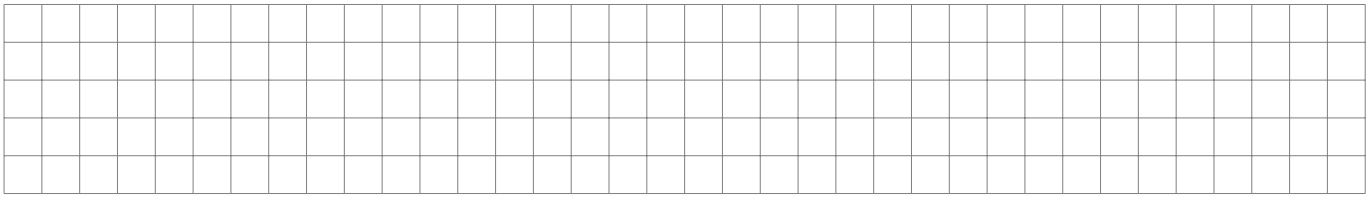
Il y a aussi d'autres règles mélangeant les quatre opérations qui découlent des propriétés de la soustraction et de la division.

Exemple 6.2. Soient $a, b, c \in \mathbb{Z}$, l'une des propriétés de la soustraction que nous avons vues est que $(a + b) - c = a + (b - c)$. On note donc $a + b - c$. Par contre, $(a - b) + c \neq a - (b + c)$ en général.

De même pour la division $(a \cdot b) : c = a \cdot (b : c)$ lorsque $c|b$. On note donc $a \cdot b : c$.

L'idée de la règle suivante est que, pour différencier les positifs des négatifs, il suffit de distinguer les négatifs. De cette façon on économise beaucoup de parenthèses dans l'écriture !

Règle de signe. Un nombre entier sans signe est un nombre entier positif. De plus, on n'entoure plus les nombres entiers positifs de parenthèses si on les écrit sans signe et on n'entoure les négatifs que lorsqu'ils sont précédés d'une opération.



De cette façon les entiers naturels $\mathbb{N}$ forment un sous-ensemble de $\mathbb{Z}$, du point de vue de l'écriture aussi ! On simplifie enfin l'écriture des parenthèses de priorité en utilisant les règles conventionnelles suivantes :

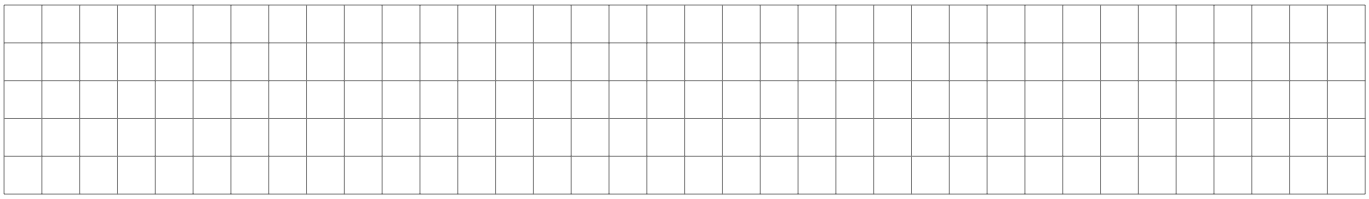
Règles de priorité.

(1) Priorité des puissances et des racines sur les autres opérations.

(2) Priorité de la multiplication, de la division et de l'opposé sur l'addition et la soustraction.

(3) Pour des expressions contenant des opérations de même niveau de priorité, on effectue de gauche à droite.

Pour illustrer la première règle de priorité, on écrit donc $3+8^2$ au lieu de $3+(8^2)$ et $3\cdot 8^2$ au lieu de $3\cdot(8^2)$. En particulier $-(5^2)=-5^2\neq(-5)^2$.



Remarque 6.3. L'opposé a le même niveau de priorité que la multiplication et la division car il peut être vu comme une multiplication ou une division : Pour tout $a\in\mathbb{Z}$,

$$-a=(-1)\cdot a=a:(-1)$$

En particulier, on peut simplifier les parenthèses superflues dans les situations suivantes : Pour tous $a,b,c\in\mathbb{Z}$,

(1) $-(a\cdot b)=(-a)\cdot b=a\cdot(-b)$ se note donc $-a\cdot b$,

(2) Si $a:b$ est défini, alors $-(a:b)=(-a):b=a:(-b)$ se note donc $-a:b$.

La valeur absolue a la même priorité que les parenthèses, soit la première.

Exemple 6.4.

$$\begin{array}{rcccl} -[(-7)\cdot(-8)] & = & -(+56) & = & -56 \\ [-(-7)]\cdot(-8) & = & (+7)\cdot(-8) & = & -56 \\ (-7)\cdot[-(-8)] & = & (-7)\cdot(+8) & = & -56 \end{array}$$

Par contre,

$$\begin{array}{rcccl} -[(-3)+(+8)] & = & -(-3+8) & = & -5 \\ -(-3)+(+8) & = & +3+8 & = & +11 \\ (-3)+[-(+8)] & = & (-3)+(-8) & = & -11 \end{array}$$

Enfin, $-|-(-8)-6|^3=-|8-6|^3=-|(+2)|^3=-(+2)^3=-(+8)=-8$.

Chapitre 4

Les nombres rationnels

Nous construisons maintenant les nombres rationnels. L'idée est analogue à celle appliquée pour construire $\mathbb{Z}$ à partir de $\mathbb{N}$ pour rendre la soustraction toujours possible. Ici nous étendons $\mathbb{Z}$ afin de rendre la *division* toujours possible. La motivation vient des besoins de la vie courante. On utilise des fractions lorsqu'on dit trois-quarts d'heure, 10% de rabais, un demi-kilo de pain, le cinquième de la distance, un huitième de gâteau, la mi-temps du match, le Tiers-Monde, une chance sur un million de gagner au loto, un quartier de pomme, ...

1. Construction des nombres rationnels

Le mot « rationnel »vient du latin *ratio* qui signifie rapport, proportion. L'idée mathématique derrière la construction de l'ensemble $\mathbb{Q}$ des nombres rationnels – avec son addition et sa multiplication – est de former la "plus petite" extension de $\mathbb{Z}$ qui résout l'un des problèmes équivalents suivants (et donc tous) :

- Pouvoir effectuer toutes les divisions par un entier non nul.
- Avoir un inverse multiplicatif pour tout nombre non nul, i.e. pour tout $a \in \mathbb{Z}$, $a \neq 0$, avoir un nombre c tel que $a \cdot c = 1$.
- Avoir une solution à toutes les équations du type $a \cdot x = b$, avec $a, b \in \mathbb{Z}$, $a \neq 0$.

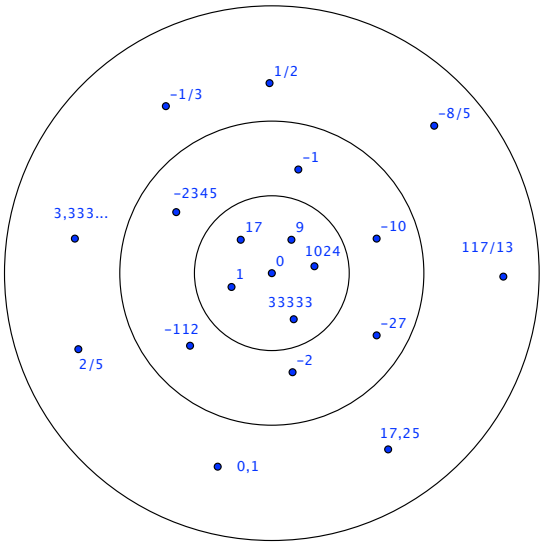
On construit l'ensemble $\mathbb{Q}$ à partir de l'ensemble $\mathbb{Z}$. Dans $\mathbb{Q}$, on aimerait avoir tous (et seulement) les quotients $a : b$ où $a, b \in \mathbb{Z}$, $b \neq 0$ (y compris les quotients du type $a : 1$, soit tous les entiers).

Pour chaque paire d'entiers a et b, avec $b \neq 0$, on introduit le *symbole*

$$\frac{a}{b}$$

appelé *fraction*, qui devrait jouer le rôle du quotient de a par b et qui manque en général dans $\mathbb{Z}$ (si b ne divise pas a).

Sous forme de diagramme de Venn, voici comment se représenter la situation. Ajoutons les étiquettes !



Le problème c'est que des symboles différents représentent alors le même quotient.

En cherchant un critère qui nous dit quand deux fractions doivent représenter le même nombre, nous remarquons que si $a, b, c, d \in \mathbb{Z}$ sont tels que $b \mid a$ et $d \mid c$, alors

$$a : b = c : d \iff a \cdot d = b \cdot c$$

en multipliant de part et d'autre de l'égalité par b et par d. Ceci conduit à poser :

Définition 1.1. Deux fractions $\frac{a}{b}$ et $\frac{c}{d}$ sont *équivalentes* si $a \cdot d = b \cdot c$ dans $\mathbb{Z}$. On note $\frac{a}{b} \sim \frac{c}{d}$.

Par exemple $\frac{12}{60} \sim \frac{1}{5}$ puisque $12 \cdot 5 = 60 \cdot 1$, un calcul que l'on est amené à faire si l'on veut savoir quelle fraction d'une heure représentent 12 minutes.

Cette relation a de bonnes propriétés, comme le montre le lemme suivant.

Lemme 1.2. *La relation $\sim$ introduite ci-dessus est une* relation d'équivalence *sur l'ensemble des fractions, c'est-à-dire qu'elle est*

(1) **réflexive :** $\frac{a}{b} \sim \frac{a}{b}$, *pour toute fraction* $\frac{a}{b}$.

(2) **symétrique :** *Si* $\frac{a}{b} \sim \frac{c}{d}$, *alors* $\frac{c}{d} \sim \frac{a}{b}$, *pour toutes fractions* $\frac{a}{b}$ *et* $\frac{c}{d}$.

(3) **transitive :** *Si* $\frac{a}{b} \sim \frac{c}{d}$ *et* $\frac{c}{d} \sim \frac{e}{f}$, *alors* $\frac{a}{b} \sim \frac{e}{f}$, *pour tous* $\frac{a}{b}$, $\frac{c}{d}$ *et* $\frac{e}{f}$.

DÉMONSTRATION. La plus dure est la dernière, les autres sont en exercice.

□

Définition 1.3. L'ensemble $\mathbb{Q}$ des nombres *rationnels* est l'ensemble

$$\{\frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0 \text{ et } \frac{a}{b} = \frac{c}{d} \iff \frac{a}{b} \text{ est équivalente à } \frac{c}{d}\}$$

Le nombre a s'appelle le *numérateur* et b le *dénominateur*. La barre horizontale s'appelle la barre de fraction.

Autrement dit, deux nombres rationnels sont égaux si et seulement s'ils peuvent être représentés par des fractions équivalentes. Formellement un nombre rationnel n'est donc pas une fraction, mais toute une *classe d'équivalence* de fractions (équivalentes). On utilisera la plupart du temps $\frac{1}{2}$ pour le nombre "une demi", mais c'est le même nombre que $\frac{13}{26}$ par exemple.

De fait, à partir de maintenant, lorsqu'on écrit une fraction, on entend le nombre rationnel qu'elle représente et non plus simplement le symbole de fraction. C'est pourquoi on écrit des égalités de fractions même lorsque les symboles de fractions sont seulement équivalents. Par exemple $\frac{1}{2} = \frac{13}{26}$. C'est ce qu'on appelle en mathématiques un *abus de notation* !

Remarque 1.4. L'origine des termes numérateur et dénominateur est latine : *numerator* et *denominator*. Le premier terme indique combien de parts on va partager, le second par combien on va effectuer ce partage.

Voici différents cas d'équivalence des fractions importants dans la pratique. On lit ces égalités de gauche à droite, comme toujours en français, ce qui explique les noms de ces règles.

Proposition 1.5. *Soient $a, b, c \in \mathbb{Z}$ avec $b, c \neq 0$.*

(1) ***Amplification.*** $\dfrac{a}{b} = \dfrac{a \cdot c}{b \cdot c}$.

(2) ***Simplification.*** *Si c est un diviseur commun de a et b, alors* $\dfrac{a}{b} = \dfrac{a : c}{b : c}$

Démonstration. Pour l'amplification il suffit d'utiliser la commutativité de la multiplication

$$a \cdot b \cdot c = a \cdot c \cdot b = b \cdot a \cdot c$$

Pour la simplification, on peut alors utiliser l'amplification par c :

$$\frac{a : c}{b : c} = \frac{(a : c) \cdot c}{(b : c) \cdot c} = \frac{a}{b}$$

□

Exemple 1.6. On nous apprend qu'aujourd'hui une heure de promenade avec des chiens est facturée 28 francs, alors qu'en 1980 il n'était pas rare de rendre ce service pour 16 francs. Quel rapport en pour cents cela représente-t-il ?

Définition 1.7. Une fraction $\dfrac{a}{b}$ est *irréductible* si $\mathrm{pgdc}(a, b) = 1$. On dit que les nombres a et b sont *premiers entre eux*.

Remarque 1.8. Par simplification, toute fraction est équivalente à une unique fraction irréductible. La fraction irréductible de $\dfrac{a}{b}$ est la fraction

$$\frac{a : \mathrm{pgdc}(a, b)}{b : \mathrm{pgdc}(a, b)}.$$

Exemple 1.9. La fraction $\frac{54}{60}$ n'est pas irréductible, mais elle est égale à $\frac{9}{10}$, qui est irréductible puisque 9 et 10 sont premiers entre eux.

Proposition 1.10. *Deux fractions sont équivalentes si et seulement si elles ont la même fraction irréductible.*

Avant de passer aux opérations de somme et de produit j'aimerais mettre en évidence un fait que vous avez vu en exercices. La règle de simplification permet de réduire des fractions lorsque numérateur et dénominateur ont un facteur commun, c'est-à-dire qu'ils s'écrivent comme multiples d'un nombre c. On NE PEUT PAS simplifier lorsqu'ils s'écrivent tous deux comme somme ! En général

$$\frac{a+c}{b+c} \neq \frac{a}{b}$$

En effet $(a+c)\cdot b \neq (b+c)\cdot a$ à moins que $c\cdot b = c\cdot a$. Un exemple frappant est donné par

$$2 = \frac{4}{2} = \frac{3+1}{1+1} \neq \frac{3}{1} = 3$$

On illustre ici le fait qu'un contre-exemple donne une preuve qu'une certaine affirmation est fausse. Plutôt que de dire que quelque chose n'est pas toujours vrai, il vaut mieux convaincre en donnant un exemple explicite et irréfutable.

2. La multiplication dans $\mathbb{Q}$

Nous verrons dans les sections suivantes que $\mathbb{Z}$ est contenu dans $\mathbb{Q}$ et que les opérations de somme et de produit que nous connaissons s'étendent aux nombres rationnels.

Remarque 2.1. La fraction $\frac{a}{1}$ représente le quotient $a : 1$, soit le nombre entier a. On écrit donc a pour le nombre rationnel représenté par la fraction $\frac{a}{1}$. De cette manière, $\mathbb{Z} \subset \mathbb{Q}$.

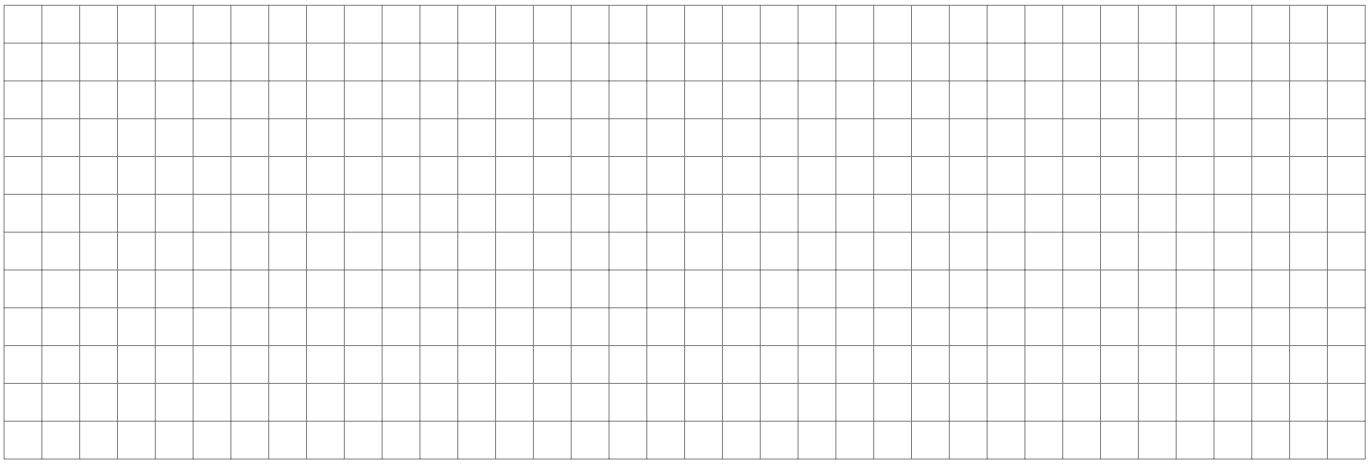
On veut définir une multiplication sur $\mathbb{Q}$ qui étende celle de $\mathbb{Z}$ et telle que $\frac{a}{b}$ soit le quotient dans $\mathbb{Q}$ de $\frac{a}{1} = a$ par $\frac{b}{1} = b$. Soient $a, b, c, d \in \mathbb{Z}$, $b, d \neq 0$. Si les quotients $a : b$ et $c : d$ existent dans $\mathbb{Z}$, alors on a dans $\mathbb{Z}$:

$$(a : b) \cdot (c : d) = (a \cdot c) : (b \cdot d)$$

Ceci conduit à définir :

Définition 2.2. Soient r, s des nombres rationnels. Soient $\frac{a}{b}$ et $\frac{c}{d}$ des fractions qui représentent r et s respectivement. Le *produit* de r et s, noté $r \cdot s$, est défini par

$$r \cdot s = \frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d}$$



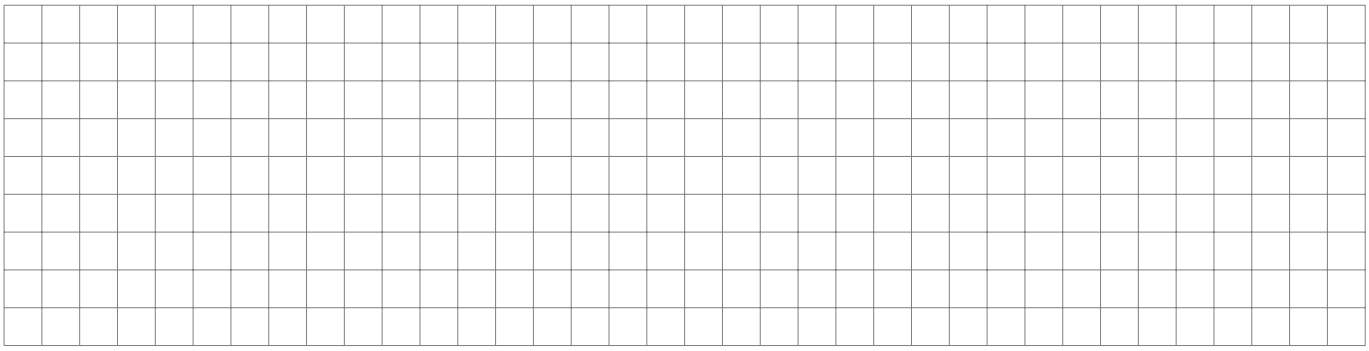
Vérifions maintenant que ce produit a bien les propriétés souhaitées. En particulier il résout le problème de la division dans $\mathbb{Z}$.

Proposition 2.3. *La multiplication de $\mathbb{Q}$ étend celle de $\mathbb{Z}$. Dans $\mathbb{Q}$, la fraction $\frac{a}{b}$ est le quotient de a par b. De plus la fraction $\frac{1}{a}$ est l'inverse du nombre entier non nul a.*

DÉMONSTRATION. Soient $a, b \in \mathbb{Z}$. Alors le produit de a et b dans $\mathbb{Q}$ se calcule comme suit

$$\frac{a}{1} \cdot \frac{b}{1} = \frac{a \cdot b}{1} = a \cdot b$$

C'est bien le produit dans $\mathbb{Z}$! Pour montrer ensuite que $\frac{a}{b}$ est le quotient de a par b,



La dernière vérification est du même tonneau (en exercice). □

Les propriétés des opérations dans $\mathbb{Z}$ que nous avons démontrées précédemment permettent de comprendre les propriétés des opérations que nous avons étendues dans $\mathbb{Q}$.

Proposition 2.4. Propriétés de la multiplication. *On a*

(1) Associativité : pour tous $r, s, t \in \mathbb{Q}$,

$$(r \cdot s) \cdot t = r \cdot (s \cdot t).$$

(2) Elément neutre 1 : pour tout $r \in \mathbb{Q}$,

$$r \cdot 1 = 1 \cdot r = r.$$

(3) Commutativité : pour tous $r, s \in \mathbb{Q}$,

$$r \cdot s = s \cdot r.$$

(4) Existence d'un inverse : tout nombre rationnel non nul admet un inverse multiplicatif, i.e. pour tout $r \in \mathbb{Q}$, $r \neq 0$, il existe un unique nombre rationnel, noté r^{-1}, appelé l'inverse de r, tel que

$$r \cdot r^{-1} = 1.$$

Il est donné par

$$\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}.$$

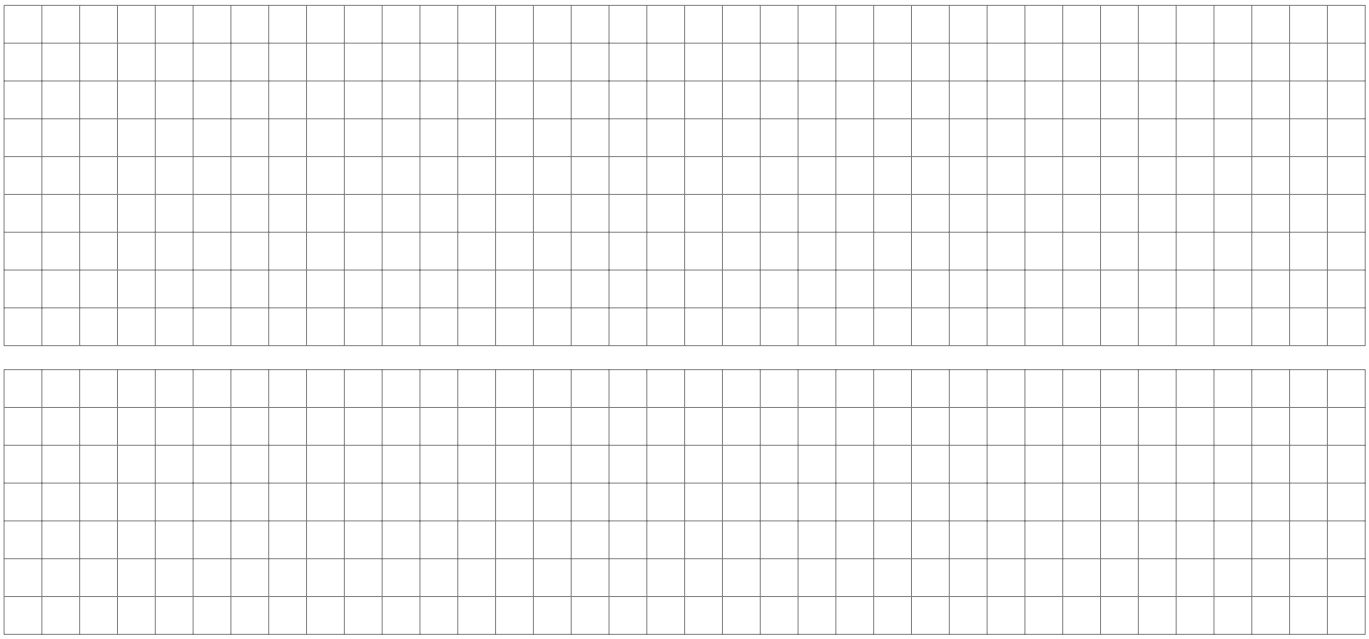
La preuve est facile ! Par exemple le dernier point se vérifie par un simple calcul :

$$\frac{a}{b} \cdot \frac{b}{a} = \frac{a \cdot b}{b \cdot a} = \frac{1}{1} = 1$$

Grâce à tout ce travail, le problème de la division est résolu dans $\mathbb{Q}$.

Proposition 2.5. *Pour tous $r, s \in \mathbb{Q}$ avec $s \neq 0$, il existe un unique nombre rationnel, noté $r : s$, appelé le quotient de r par s tel que*

$$r = (r : s) \cdot s.$$



Autrement dit : Dans $\mathbb{Q}$, diviser, c'est multiplier par l'inverse.

Exemple 2.6. L'inverse de $\frac{7}{4}$ est $\frac{4}{7}$ et $\left(\frac{-5}{3}\right)^{-1} = \frac{-3}{5}$. Ainsi pour diviser par $\frac{-5}{3}$, on multipliera par $\frac{-3}{5}$:

$$\frac{7}{4} : \frac{-5}{3} = \frac{7}{4} \cdot \frac{-3}{5} = \frac{-21}{20}$$

On remarque pour terminer que lors d'une multiplication on peut effectuer des simplifications “croisées". La méthode de calcul pour un produit de fractions est donc en général de réduire chacune des fractions pour les rendre irréductibles, d'effectuer les simplifications croisées possibles, puis finalement de calculer le produit et de le réduire. Par exemple

3. L'addition dans $\mathbb{Q}$

La multiplication a été simple à définir car nous avons utilisé les propriétés du produit dans $\mathbb{Z}$ pour construire $\mathbb{Q}$. Pour la somme ce sera un peu plus compliqué. On veut définir une addition sur l'ensemble $\mathbb{Q}$ telle que :

- La multiplication se distribue sur l'addition,
- L'addition sur $\mathbb{Q}$ étend celle de $\mathbb{Z}$, c'est-à-dire que la somme $\frac{a}{1} + \frac{b}{1}$ doit être égale à $a + b$ pour $a, b \in \mathbb{Z}$.

Donc si une telle addition existe et que $\frac{a}{b}, \frac{c}{b}$ sont deux fractions ayant le même dénominateur, alors

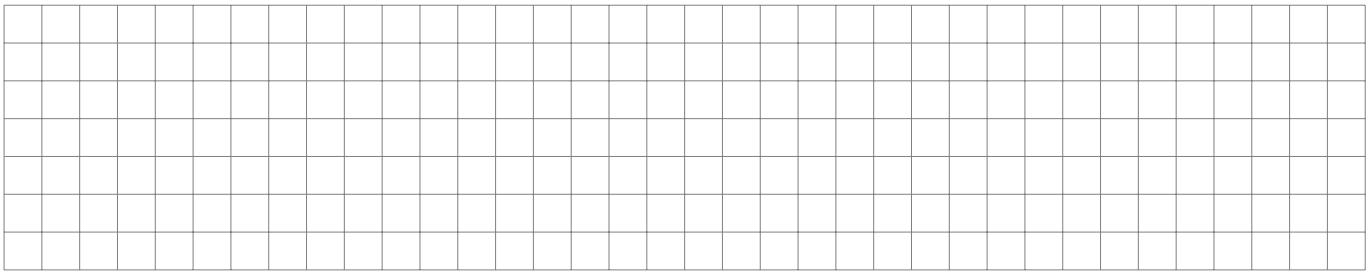
$$\frac{a}{b} + \frac{c}{b} = \frac{a+c}{b}$$

Pour additionner deux fractions, il suffira donc de prendre deux fractions équivalentes qui ont le même dénominateur, puis sommer les numérateurs et garder ce dénominateur commun.

Définition 3.1. Soient $\frac{a}{b}$ et $\frac{c}{d}$ deux fractions. Alors la *somme* de ces deux fractions est égale à

$$\frac{a}{b} + \frac{c}{d} = \frac{a \cdot d}{b \cdot d} + \frac{c \cdot b}{b \cdot d} = \frac{a \cdot d + b \cdot c}{b \cdot d}$$

Exemple 3.2. On calcule



Le dénominateur de la somme est un multiple commun des dénominateurs, par exemple leur produit, mais leur ppmc est le choix le plus économique ! Comme dans le cas de la multiplication on économise de l'énergie si on rend d'abord les fractions irréductibles avant de les additionner :

$$\frac{56}{49} + \frac{-6}{8} = \frac{8}{7} + \frac{-3}{4} = \frac{32-21}{28} = \frac{11}{28}$$

Attention : on ne peut pas simplifier en diagonale ! C'est tentant, bien sûr, mais très, très faux. Par exemple

$$\frac{10}{3} = \frac{3}{1} + \frac{1}{3} \neq \frac{1}{1} + \frac{1}{1} = 2$$

Remarque 3.3. L'addition de deux nombres rationnels r et s est bien définie : elle ne dépend pas du choix des fractions qui représentent r et s. On peut montrer que si $\frac{a}{b}$ et $\frac{a'}{b'}$ sont équivalentes, et $\frac{c}{d}$ et $\frac{c'}{d'}$ sont équivalentes, alors leur somme $\frac{a}{b} + \frac{c}{d}$ et $\frac{a'}{b'} + \frac{c'}{d'}$ sont aussi équivalentes. Saurais-tu le démontrer ?

Proposition 3.4. Propriétés de l'addition. *L'addition dans $\mathbb{Q}$ a les propriétés suivantes :*

(1) Associativité : pour tous $r, s, t \in \mathbb{Q}$, on a $(r + s) + t = r + (s + t)$.

(2) Commutativité : pour tous $r, s \in \mathbb{Q}$, on a $r + s = s + r$.

(3) Elément neutre 0 : pour tout $r \in \mathbb{Q}$, on a $r + 0 = r = 0 + r$.

*(4) Existence de l'opposé : pour tout rationnel r, il existe un unique rationnel noté $-r$, appelé l'*opposé *de r, tel que $r + (-r) = 0$.*

(5) Distributivité de la multiplication sur l'addition : pour tous $r, s, t \in \mathbb{Q}$, on a $r \cdot (s + t) = (r \cdot s) + (r \cdot t)$.

Démonstration. Montrons l'associativité, l'une des propriétés les plus embêtantes parce qu'elle concerne trois nombres. On considère trois nombres rationnels r, s, t.

Pour montrer l'existence de l'opposé, il suffit de constater que l'opposé de la fraction $\frac{a}{b}$ est donné par $-\frac{a}{b} = \frac{-a}{b} = \frac{a}{-b}$. □

Remarque 3.5. L'addition de $\mathbb{Q}$ a les mêmes propriétés (1)-(4) que celle de $\mathbb{Z}$. Les nombres rationnels, munis de l'addition, forment un groupe abélien. Ajoutons maintenant la multiplication. Elle aussi a les mêmes propriétés que celle de $\mathbb{Z}$ si bien qu'en ajoutant la distributivité (5), on constate que $\mathbb{Q}$, avec sa somme et son produit, forme un anneau commutatif. Il y a mieux encore ! La nouveauté de la multiplication dans $\mathbb{Q}$ par rapport à celle de $\mathbb{Z}$ est que tout nombre non nul possède un inverse. Un anneau commutatif qui a cette propriété supplémentaire s'appelle un *corps*.

Remarquons encore que la soustraction dans $\mathbb{Q}$ a les mêmes propriétés que celle de $\mathbb{Z}$. En particulier, la soustraction est toujours possible et soustraire c'est additionner l'opposé. Pour tous rationnels r, s, on a $r - s = r + (-s)$.

Avant de se lancer tête baissée dans les calculs, on se demandera toujours s'il y a des simplifications de fractions à effectuer auparavant, éventuellement des simplifications "croisées" pour des produits.

Chapitre 5

Un premier aperçu des nombres réels

Après les nombres rationnels, nous abordons de manière superficielle les nombres réels par leur représentation sous forme de “nombre à virgule”. Notre but est de comprendre quelle est l'écriture décimale des nombres rationnels et comment on les distingue des nombres réels qui ne sont pas rationnels.

1. Notation et exemples

Lorsqu'on parle d'écriture décimale cela signifie que l'on écrit les nombres avec le système positionnel en base 10. Rappelons que tout nombre entier a admet une unique écriture décimale. Si $a = \pm n$, $n \in \mathbb{N}$, n peut s'écrire comme une unique suite de $k+1$ chiffres

$$a_k a_{k-1} \dots a_1 a_0$$

où $k \in \mathbb{N}$, $a_i \in \{0, 1, \dots, 9\}$ pour tout $0 \leq i \leq k$ et $a_k \neq 0$ si $k \neq 0$. Cela signifie que

$$n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \dots + a_1 \cdot 10^1 + a_0 \cdot 10^0.$$

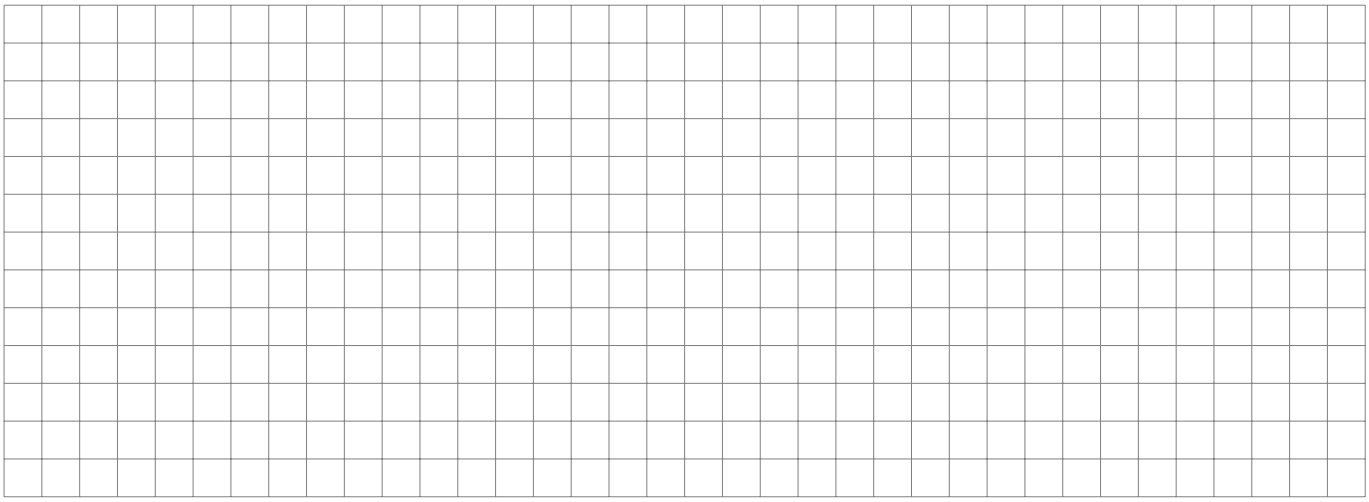
Par exemple, l'écriture décimale 3708 signifie $3 \cdot 10^3 + 7 \cdot 10^2 + 0 \cdot 10^1 + 8 \cdot 10^0$.

Une telle somme doit toujours avoir un nombre fini de facteurs sinon elle “diverge", i.e. elle a une valeur infinie. Autrement dit, un nombre entier a toujours un nombre fini de chiffres en écriture décimale.

La convention que l'on a utilisé ci-dessus est que les chiffres représentent le nombre de certaines puissances de 10, de plus en plus grandes lorsqu'on se déplace de droite à gauche. La convention que nous adoptons donc lorsque nous voulons écrire des nombres qui ne sont pas entiers est de continuer le développement décimal en indiquant ceci par une virgule et les chiffres après la virgule donnent le nombre de puissances de $10^{-1} = \dfrac{1}{10}$. Ainsi, le nombre $4762,23458$ s'écrit

$$4 \cdot (10)^3 + 7 \cdot (10)^2 + 6 \cdot 10 + 2 \cdot 1 + 2 \cdot \frac{1}{10} + 3 \cdot \frac{1}{10^2} + 4 \cdot \frac{1}{10^3} + 5 \cdot \frac{1}{10^4} + 8 \cdot \frac{1}{10^5}$$

Exemple 1.1. Le nombre $\dfrac{3}{4}$, “trois quarts", s'écrit aussi $0,75$.



Dans les exemples étudiés il y a un nombre fini de chiffres après la virgule. Mais on peut se poser la question de savoir si cela a un sens d'écrire une infinité de chiffres après la virgule ? Est-ce que cela peut donner une valeur finie ? Si l'écriture décimale est infinie, le nombre correspond à une somme infinie de fractions. En effet

$$0, a_1 a_2 a_3 \cdots = \frac{a_1}{10} + \frac{a_2}{100} + \frac{a_3}{1000} + \dots$$

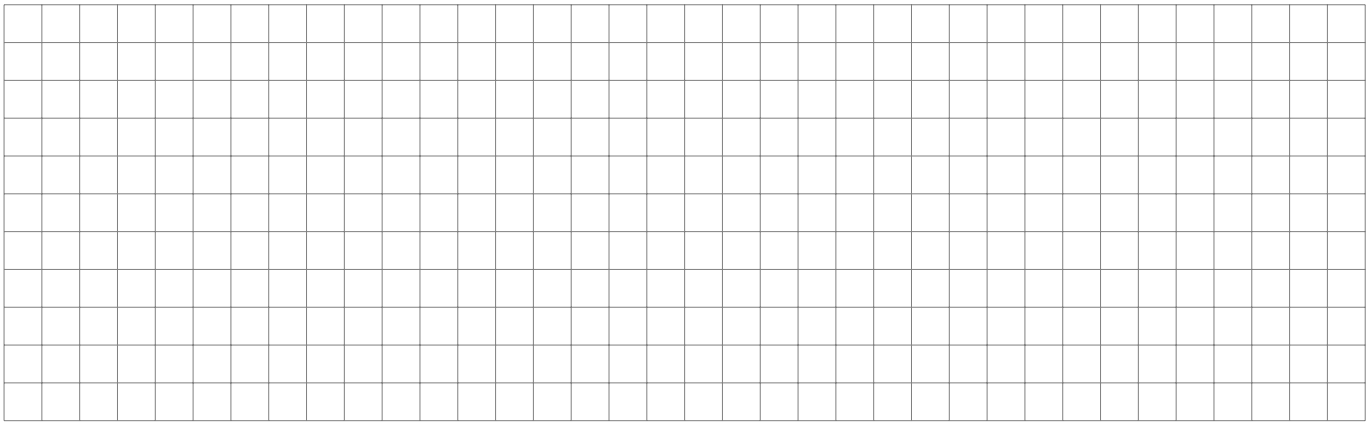
On peut montrer qu'une telle somme est toujours finie, mais seulement certaines de ces sommes sont des nombres rationnels. Les autres sont des nombres réels *irrationnels* (que nous n'avons pas défini pour l'instant).

Un exemple est donné par la fraction "un tiers". J'affirme que $\frac{1}{3} = 0,333\ldots =: 0,\bar{3}$. On dit "zéro virgule trois *périodique*". Comment se peut-il qu'il y ait un nombre de chiffres infini après la virgule alors que c'était impossible pour les chiffres avant la virgule ? Ici

$$0,\bar{3} = \frac{3}{10} + \frac{3}{100} + \frac{3}{1000} + \cdots = \frac{333}{1000} + \cdots = \frac{3333}{10000} + \cdots$$

Le dénominateur est presque égal au triple du numérateur, mais il faudra ajouter un nombre infini de puissances de plus en plus grandes de $\frac{1}{10}$ (des nombres rationnels de plus en plus petits !) pour y arriver.

Proposition 1.2. *Les nombres* $0{,}\bar{3}$ *et* $\dfrac{1}{3}$ *sont égaux.*



Saurais-tu démontrer que 1 et $0{,}\bar{9}$ sont égaux ?

2. L'écriture décimale

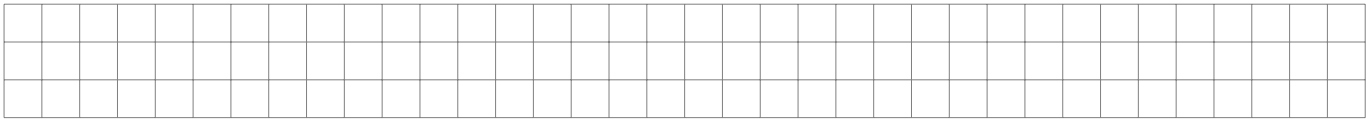
On considère maintenant un nombre dont l'écriture décimale est constituée des chiffres $a_1, a_2, \ldots$ après la virgule. Explicitement le nombre a_n indique la présence de a_n fois $\dfrac{1}{10^n}$.

Définition 2.1. L'écriture décimale d'un nombre est dite *périodique* s'il existe un nombre entier naturel k, la *période*, et un nombre entier naturel N, tel que $a_{n+k} = a_n$ pour tout $n \geq N$. Un tel nombre est dit *périodique*. L'écriture décimale d'un nombre est *finie* si elle admet un nombre fini de décimales non nulles. Un tel nombre est dit *décimal*.

Ainsi un nombre périodique à une écriture décimale formée d'une suite de chiffres qui se répètent à l'infini. Par exemple

$$35{,}943267267267\ldots = 35{,}943\overline{267}$$

est un nombre périodique. La période vaut 3 ici et à partir du quatrième chiffre après la virgule les chiffres 267 se répètent à l'infini. Par contre les nombres 261,1 ou 0,000012 ou encore 7,983 sont décimaux.



Voici le résultat principal de cette section. La preuve, dont on donne l'idée, décrit la méthode pour passer de l'écriture fractionnaire à l'écriture décimale et vice-versa.

Il ne faudra pas connaître la preuve par coeur, mais il est important de savoir écrire un nombre rationnel selon ces deux systèmes.

Proposition 2.2. *Tout nombre rationnel admet une écriture décimale finie ou périodique. Inversement, toute écriture décimale finie ou périodique est un nombre rationnel.*

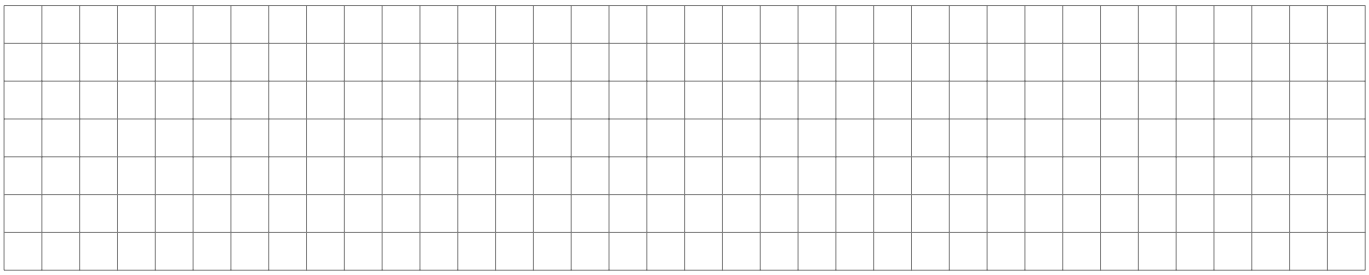
On commence par étudier le cas des nombres décimaux. On affirme que si le dénominateur b d'une fraction $\frac{a}{b}$ est un diviseur d'une puissance de 10, i.e. $b = 2^k \cdot 5^m$, $k, m \in \mathbb{N}$, alors l'écriture décimale est finie. Il suffit en effet de multiplier ce nombre rationnel par 10^M où M est le maximum de k et m pour trouver un nombre entier !

Exemple 2.3. Si le dénominateur vaut $8 = 2^3$, il faut multiplier le nombre par

Lorsque le dénominateur est une puissance de 10 (et pas seulement un diviseur comme ci-dessus), le procédé est plus transparent. Par exemple $\frac{37}{1000} = 0,037$.

Le sens inverse est bien plus simple ! Tout nombre décimal est un nombre rationnel dont la fraction irréductible a un dénominateur qui est un diviseur d'une puissance de 10. En effet si un nombre décimal a k chiffres après la virgule, il suffit de le multiplier par 10^k pour trouver un nombre entier.

Exemple 2.4. Comment transformer le nombre $-67,8326$ en une fraction irréductible ?



Corollaire 2.5. *Si le dénominateur de la fraction irréductible d'un nombre rationnel n'est pas un diviseur d'une puissance de 10, alors son écriture décimale est infinie.*

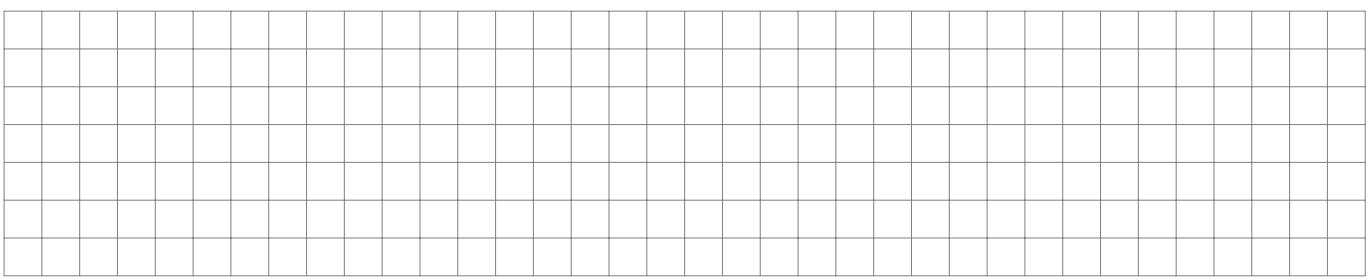
On va voir que cette écriture décimale est nécessairement périodique.

Considérons une fraction dont le dénominateur n'est pas diviseur d'une puissance de 10, alors la méthode précédente ne marche pas. On procède par division euclidienne. En général la division d'un nombre entier n par un nombre entier m donne un quotient q et un reste de la division r. Le reste est un nombre positif ou nul, mais strictement plus petit que m. On a donc

$$n = q \cdot m + r$$

Exemple 2.6. On cherche le développement décimal de $\frac{1}{7}$. On itère le procédé de division euclidienne. On a $1 : 7 = 0$ reste 1, et on dit que le quotient de la division de 1 par 7 vaut zéro et il reste 1. Il y a donc zéro unité dans un septième. Pour trouver le premier chiffre après la virgule, on multiplie alors le reste par 10 et on recommence :

$$10 = 1 \cdot 7 + 3 \quad \text{le quotient vaut 1 et il reste 3}$$



Par conséquent $\frac{1}{7} = 0,1428571428571\cdots = 0,\overline{142857}$. Nous avons choisi le cas le plus long puisque tous les restes possibles apparaissent !

Corollaire 2.7. *Si le dénominateur de la fraction irréductible d'un nombre rationnel n'est pas un diviseur d'une puissance de 10, alors son écriture décimale est périodique et la longueur de la période est strictement inférieure au dénominateur (de la fraction irréductible).*

Une écriture décimale infinie non périodique ne peut pas donc jamais provenir d'un nombre rationnel.

Pour terminer notre étude nous devons encore expliquer comment transformer un nombre périodique en une fraction. La méthode est basée sur l'astuce qui nous a permis de comprendre ci-dessus pourquoi $\frac{1}{3}$ est égal à $0,\overline{3}$.

Soit r un nombre périodique, sa période étant k. Par exemple $0,\overline{3}$ est de période 1, mais $173,1741574157415\cdots = 173,1\overline{7415}$ est de période 4. On procède pas à pas :

(1) On multiplie le nombre par 10^k. Pour l'exemple précédent on calcule donc

$$10^4 \cdot 173,1\overline{7415} = 1731741,5\overline{7415}$$

(2) Pour faire disparaître la partie périodique de ce nombre on le soustrait au résultat précédent. On calcule donc $10^k - 1$ fois r. Ici

$$9999 \cdot 173{,}1\overline{7415} = 1'731'741{,}5\overline{7415} - 173{,}1\overline{7415} = 1'731'568{,}4$$

(3) Si ce nombre n'est pas entier on le multiplie par une puissance de 10 pour le rendre entier. Ici

$$99'990 \cdot 173{,}1\overline{7415} = 17'315'684$$

(4) On isole le nombre qui nous intéresse dans cette égalité. On trouve ainsi une expression fractionnaire pour r dont le dénominateur est une puissance de 10 qui multiplie une autre puissance de 10 moins un. Le problème est alors de réduire cette fraction. Dans notre cas

$$173{,}1\overline{7415} = \frac{17'315'684}{99'990} = \frac{8'657'842}{49'995}$$

Remarque 2.8. En sommant un nombre infini de nombres rationnels, on peut obtenir un nombre réel fini irrationnel. Par exemple le nombre

$$0{,}12345678910111213141516171819202 1\ldots$$

n'est ni décimal, ni périodique. Il ne provient donc d'aucune fraction ! Il en va de même du nombre

$$0{,}10100100010000100000100000010000000\ldots$$

Il y a d'autres nombres célèbres et utiles en mathématiques qui ne sont pas rationnels. C'est le cas de π et e, que nous verrons dans une année, mais il est plus difficile de *démontrer* que leur écriture décimale n'est pas périodique...