2024-04-27T14:15

Introduction rapide à l'arithmétique élémentaire

Série pour lycée / L0 / bac + 0

Alexey Muranov

27 avril 2024

2024-04-27T14:15

Table des matières

I. Nombres naturels

I.1. Qu'est-ce que c'est, un nombre naturel ?

Les *nombres naturels* sont les nombres utilisés à compter et à énumérer des objets. Par exemple : *un*, *deux*, *trois*, *quatre*.

Il y a un cas spécial où on tente de compter des objets alors qu'il n'y en a pas. On peut admettre que dans ce cas le nombre d'objets est *zéro*.

Pour énumérer des objet, on commence d'habitude avec *un*. Cependant, en mathématique et en informatique, on trouve souvent plus pratique de commencer avec *zéro*.

Faut-il donc traiter *zéro* comme un *nombre naturel* ?

En France on admet que *zéro* est un nombre naturel, mais dans certains autres pays les nombres naturels commencent avec *un*. Ici on va suivre la tradition française. Ainsi, on admet que les *nombres naturels* sont : *zéro*, *un*, *deux*, et ainsi de suite à l'infinie.

Dans le *système de numération* romain classique, il n'y a pas de symbole pour le nombre *zéro*, mais à une certaine époque certains auteurs écrivaient « N » pour *zéro*. Le nombre *un* y est noté « I » (la lettre « i » au majuscule, mais « i » minuscule est parfois utilisée aussi).

Dans le système de numération arabe occidental, le nombre *zéro* est noté « 0 » et le nombre *un* est noté « 1 ».

Si on aura besoin de parler de l'*ensemble* des nombres naturels, cet ensemble sera noté « $\mathbf{N}$ ».

I.2. Successeurs et prédécesseurs

Tout nombre naturel possède un unique *successeur* : le nombre naturel suivant. Tout nombre naturel à l'exception de *zéro* est le successeur de son unique *prédécesseur*.

Par exemple, *trois* est le successeur de *deux* et le prédécesseur de *quatre*.

Si a est un nombre naturel, son successeur peut être noté « sa » ou « $s(a)$ » ou « $(s)a$ » (où les parenthèses superflues servent à souligner la différence des rôles de s et de a) ; on lit une telle expression comme « le successeur de a » ou comme « s de a ». Ici on va adopter la notation « sa ».

Ainsi on a défini l'*opération successeur* s qui à chaque nombre naturel associe son successeur. Si on *applique* l'opération s à un nombre naturel a, le résultat sa est le successeur de a.

Par exemple, si 0 est *zéro*, alors $s0$ est *un*, $s(s0)$ est *deux*, $s(s(s0))$ est *trois*, et ainsi de suite.

Voici une propriété importante :

> si $sa = sb$, alors $a = b$.

Ainsi, l'opération successeur est « réversible » : on peut déterminer a si on connaît sa.

I.3. Relations d'ordre usuelles

Tous deux nombres naturels a et b peuvent être *comparés* : soit a est *strictement plus grand* que b (et b est *strictement plus petit* que a), soit b est *strictement plus grand* que a (et a est *strictement plus petit* que b), soit ils sont égaux (donc b est a et a est b). En symboles, on exprime cela ainsi : soit $a > b$ (et $b < a$), soit $b > a$ (et $a < b$), soit $a = b$.

Au lieu d'écrire « $a < b$ ou $a = b$ », on peut écrire « $a \leqslant b$ », et au lieu d'écrire « $a > b$ ou $a = b$ », on peut écrire « $a \geqslant b$ ».

Le sens de ces relations est le suivant : si a est le nombre d'objets dans une collection finie A (dans un ensemble fini A) et b est le nombre d'objets dans une partie B de A, alors $a \geqslant b$. Si en plus il existe un objet dans A qui n'est pas dans B, alors $a > b$.

Voici les trois propriétés de la relation $(<)$ les plus importantes :

(1) si $a < b$ et $b < c$, alors $a < c$,

(2) si $a < b$, alors $a \neq b$,

(3) si $a \neq b$, alors $a < b$ ou $b < a$.

Ajoutons à cette liste une quatrième propriété qui fait lien avec l'opération successeur :

(4) $a < sa$.

I.4. Addition

Si a est le nombre d'objet dans une collection finie (dans un ensemble fini), b est le nombre d'objets dans une deuxième collection finie (dans un deuxième ensemble fini), et que les deux collections n'ont pas d'objets en commun (on dit dans ce cas qu'elles sont *disjointes*), alors si on réunit les deux collections, le nombre d'objets dans la collection réunie est a *plus* b, autrement dit la *somme* de a et b. La somme de a et b ne dépend que de a et de b (la nature des objets et les collections en question sont sans importance).

Par exemple, on peut observer que la somme de *deux* et *trois* est *cinq* en utilisant cinq n'importe quels objets, par exemple cinq pommes, en séparant deux objets des trois autres.

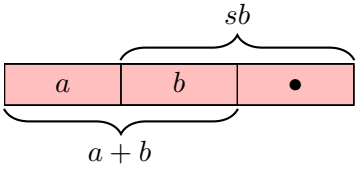
Si a et b sont deux nombres naturels, on note « $a + b$ » leur somme.

Ainsi on a défini l'*opération d'addition* $(+)$ qui à deux nombres naturels associe leur somme.

L'addition $(+)$ de nombres naturels peut aussi être définie par les deux règles suivantes, en utilisant uniquement l'opération successeur s et le nombre *zéro* 0 :

(1) $a + 0 = a$, (2) $a + sb = s(a + b)$.

Le schéma suivant montre que la règle (2) est en accord avec la notion de l'addition introduite précédemment :



Exercice. En utilisant uniquement les deux règles données ci-dessus, montrer que

$$s(s0) + s(s(s0)) = s(s(s(s(s0)))).$$

Voici les trois identités les plus importantes satisfaites par l'opération d'addition (pour les nombres naturels) :

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

(2) $a + 0 = a = 0 + a$,

(3) $b + a = a + b$.

Exercice. Démontrer ces identités (au moins d'une manière informelle).

Voici une propriété importante :

si $a + c = b + c$, alors $a = b$.

Ainsi, pour tout nombre naturel a, l'opération d'addition de a (à un autre nombre naturel) est « réversible » : on peut déterminer b si on connaît $b + a$ et a.

Cette dernière propriété s'écrit autrement ainsi :

si $a \neq b$, alors $a + c \neq b + c$.

On peut observer une propriété plus précise :

si $a < b$, alors $a + c < b + c$.

Définition des relations d'ordre à l'aide de l'addition

L'opération d'addition $(+)$ peut servir à définir les relations $(\leqslant)$ et $(<)$ par les règles suivantes :

(1) $a \leqslant b$ si et seulement si il existe c tel que $b = a + c$,

(2) $a < b$ si et seulement si il existe c différent de *zéro* tel que $b = a + c$.

Attention : ces règles ne concernent que les nombres naturels.

I.5. Soustraction

La définition de l'opération de *soustraction* repose sur la propriété suivante des nombres naturels :

si $b + a = c + a$, alors $b = c$.

Rappelons nous aussi que

$a \leqslant b$ si et seulement si il existe c tel que $c + a = b$.

Soient a et b deux nombre naturel. On peut tenter de chercher un nombre naturel c tel que $c + a = b$. Si $a > b$, on n'en trouvera aucun, et si $a \leqslant b$, on en trouvera un, et un seul. Dans le second cas, l'unique nombre c tel que $c + a = b$ est noté « $b - a$ » et est dit b *moins* a, ou encore la *différence* de b et a. Si $a > b$, alors la valeur de « $b - a$ », en tant qu'un nombre naturel, n'est pas définie. (Mais on pourra définir la valeur de « $b - a$ » comme un *entier relatif*.)

Par exemple, *trois* moins *un* est *deux*, mais aucun nombre naturel n'est *zéro* moins *un*.

Ainsi on a défini l'*opération de soustraction* $(-)$ qui à deux nombres naturels associe leur différence, tant que leur différence est définie.

La définition de l'opération de soustraction $(-)$ donnée ci-dessus peut être exprimée par l'équivalence suivante :

$$b - a = c \quad \Leftrightarrow \quad b = c + a.$$

L'opération de soustraction $(-)$ de nombres naturels peut aussi être définie par les trois propriétés suivantes, à la condition que l'opération d'addition $(+)$ est déjà définie :

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

(2) $(a - b) + b = a$ si $b \leqslant a$,

(3) la valeur de « $a - b$ » n'est définie (comme un nombre naturel) que si $b \leqslant a$.

En fait, la deuxième propriété résulte de la première, et la première résulte de la deuxième, donc il suffit de garder une seule parmi les deux.[1]

Voici quelques identités remarquables satisfaites par l'opération de soustraction (pour les nombres naturels) :

(1) $a + (b - c) = (a + b) - c$ si $c \leqslant b$,

(2) $a - (b + c) = (a - c) - b$ si $b + c \leqslant a$,

[1] Supposons que l'opération $(-)$ est définie de telle façon que $(a+b)-b = a$ pour tous les nombres naturels a et b. Soient a et b deux nombres naturels arbitraires mais tels que $b \leqslant a$. Alors il existe un nombre naturel c tel que $a = c + b$. Or, si $a = c + b$, alors $(a - b) + b = ((c + b) - b) + b = c + b = a$, car $(c + b) - b = c$.
Supposons maintenant que l'opération $(-)$ est définie de telle façon que $(a - b) + b = a$ pour tous les nombres naturels a et b tels que $b \leqslant a$. Soient a et b deux nombres naturels arbitraires et posons $c = a+b$. Alors $\underbrace{((a + b) - b)}_{\sqcup} + b = (c - b) + b = c = \underset{\sqcup}{a} + b$, et donc $(a + b) - b = a$.

(3) $a-(b-c)=(a+c)-b$ si $c\leqslant b\leqslant a+c$,

(4) $(a-b)+(b-c)=a-c$ si $c\leqslant b\leqslant a$,

(5) $(a+c)-(b+c)=a-b$ si $b\leqslant a$,

(6) $(a-b)+c=(a+c)-b$ si $b\leqslant a$,

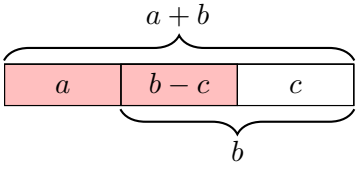
(7) $(a-b)-c=(a-c)-b$ si $b+c\leqslant a$,

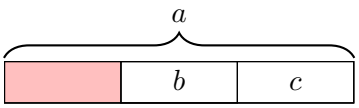
(8) $a-(a-b)=b$ si $b\leqslant a$,

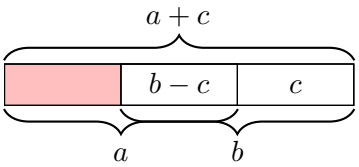
(9) $a-0=a$,

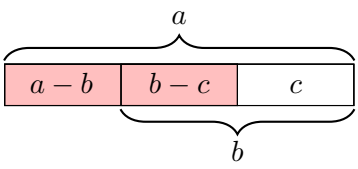
(10) $a-a=0$.

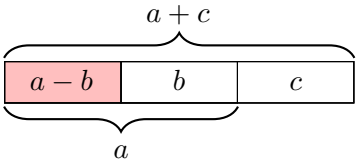
Les schémas suivants peuvent être éclairants :

(1)


(2)


(3)


(4)


(5)


Exercice. Démontrer ces identités (au moins d'une manière informelle).

Exercice. Déduire ces identités algébriquement à partir des propriétés algébriques de l'addition présentées précédemment.

I.6. Systèmes de numération

Pour pouvoir utiliser des nombres naturels individuels, il faut pouvoir les appeler et les écrire. Or, il y a une infinité des nombres naturels, donc on ne peut pas les considérer un par un et donner à chacun un nom et un symbole.

En principe, il suffit d'avoir un symbole pour *zéro*, par exemple « $*$ », et un symbol pour l'opération successeur, par exemple « s », pour pouvoir écrire un n'importe quel nombre naturel : $s*$ est *un*, $s(s*)$ est *deux*, $s(s(s*))$ est *trois*, et ainsi de suite.

On peut aussi écrire un n'importe quel nombre naturel non nul en utilisant un symbole pour le nombre *un* et un symbole pour l'opération d'addition. Par exemple, si « I » est un symbole pour *un*, et « + » est un symbole pour l'addition, alors I est *un*, I + I est *deux*, (I + I) + I est *trois*, et ainsi de suite.

Cependant, écrire les nombres naturels comme des longues expressions arithmétiques n'est pas toujours pratique. Ainsi, souvent on préfère d'utiliser un *systèmes de numération* plus ou moins « compact » pour « nommer » les nombres.

Le tableau I.1 contient quelques exemples de *systèmes de numération* qu'on pourrait envisager, et qui sont en effet utilisés.

	zéro	un	deux	trois	quatre	cinq	six	dix	onze	douze	seize	mille
`(a)`		|	||	|||	||||	|||||	||||||	|||||||||	||||||||||	||||||||||||	|···|
`(b)`		|	||	|||	||||	𝍸	𝍸|	𝍸𝍸	𝍸𝍸|	𝍸𝍸||	𝍸𝍸𝍸|	𝍸 ··· 𝍸
`(c)`		I	II	III	IV	V	VI	X	XI	XII	XVI	M
`(d)`	0	1	10	11	100	101	110	1010	1011	1100	10000	1111101000
`(e)`	0	1	2	10	11	12	20	101	102	110	121	1101001
`(f)`	0	1	2	3	4	5	6	10	11	12	16	1000
`(g)`	0	1	2	3	4	5	6	A	B	C	10	3E8

TAB. I.1. : Exemples de systèmes de numération

Le système `(c)` est le système romain classique. Le système `(f)` est le système arabe occidental.

Les systèmes `(d)`, `(e)`, `(f)` et `(g)` sont tous construits sur le même principe. La seule différence entre ces systèmes est le nombre des *chiffres* utilisés :

- le système `(d)` utilise les deux chiffres « 0 » et « 1 »,
- le système `(e)` utilise les trois chiffres « 0 », « 1 » et « 2 »,
- le système `(f)` utilise les dix chiffres « 0 », « 1 », « 2 », « 3 », « 4 », « 5 », « 6 », « 7 », « 8 », « 9 »,
- le système `(g)` utilise seize chiffres : les dix de « 0 » à « 9 », et encore les six de « A » à « F » (ou de « a » à « f »).

Ces systèmes font partie des systèmes de numération dits *positionnels*, car la « valeur » de chaque chiffre qui apparaît dans l'écriture d'un nombre dépend de la *position* de cette chiffre dans l'écriture. Ces systèmes parfois sont dits *n-aires*, où *n* est le nombre des chiffres utilisés. Pour décrire ces systèmes, on utilise aussi des adjectifs d'origine latine, ou grecque, ou latin et grecque, comme : *binaire*, *ternaire*, *quaternaire*. Ainsi, le système `(d)` est dit *binaire* (ou *deux-aire*), le système `(e)` est dit *ternaire* (ou *trois-aire*), le système `(f)` est dit *décimal* (ou *dix-aire*), et le système `(g)` est dit *hexadécimal* (ou *seize-aire*).

Pour un système positionnel n-aire, le nombre n (le nombre des chiffre) est dit la *base* du système. Ainsi, la base du système `(d)` est *deux*, la base du système `(e)` est *trois*, la base du système `(f)` est *dix*, et la base du système `(g)` est *seize*.

Dans ce cours, la plupart du temps on va utiliser le système arabe occidental (le système `(f)`). Ainsi, par défaut, « 10 » veut dire *dix*, « 100 » veut dire *cent*, et ainsi de suite.

Si on souhaite utiliser un système positionnel n-aire avec n différent de *dix* sans avertissement, on peut convenir à préciser la base en indice, écrit en système décimal. Ainsi, « 10_2 » veut dire *deux*, « 100_3 » veut dire *neuf*, et « 34_5 » veut dire *dix-neuf* :

$$34_5 = 30_5 + 4_5 = 10_5 + 10_5 + 10_5 + 4_5 = 5 + 5 + 5 + 4 = 10 + 9 = 19.$$

En fait, rien n'empêche d'écrire la base en n'importe quel système. Par exemple, comme « 12_3 » veut dire *cinq*, « 34_{12_3} » veut dire *dix-neuf*.

Exercice. Écrire le nombre *vingt-cinq* en binaire, puis en ternaire, puis en décimal, puis en hexadécimal (les systèmes `(d)`, `(e)`, `(f)` et `(g)`).

Exercice. Dresser les tables d'addition pour les systèmes binaire et quinaire (les bases *deux* et *cinq*). Pour chaque système, toutes les valeurs dans sa table doivent être écrites en ce système.

I.7. Multiplication

Étant données a collectons d'objets, où chaque collection contient b objets et où aucunes deux d'entre elles n'ont d'objets en commun (toutes deux collections sont disjointes), le nombre d'objets que ces a collections contiennent ensemble est a *fois* b :

$$\underbrace{b + b + \cdots + b}_{a \text{ fois}}.$$

Cette définition peut paraître inadaptée si a est *un* ou *zéro*, mais il suffit de préciser que *une fois* b est b et que *zéro fois* b est *zéro*. On peut aussi définir a *fois* b comme

$$0 \underbrace{+ b + b + \cdots + b}_{a \text{ fois}}.$$

Le nombre a fois b est aussi dit b *multiplié* par a.

Adoptons les notations « $a \ltimes b$ » et « $b \rtimes a$ » pour écrire a fois b, quand a et b sont deux nombres naturels. Ainsi, pour a et b naturels :

$$a \ltimes b \overset{\text{déf}}{=} 0 \underbrace{+ b + b + \cdots + b}_{a \text{ fois}},$$

$$a \rtimes b \overset{\text{déf}}{=} 0 \underbrace{+ a + a + \cdots + a}_{b \text{ fois}}.$$

Exercice. Calculer $2 \ltimes 2$, $2 \rtimes 2$, $2 \ltimes 3$, $2 \rtimes 3$, $2 \ltimes (3 \ltimes 4)$, $(2 \ltimes 3) \ltimes 4$.

Exercice. Supposons qu'il y a a conteneurs sur une plate-forme, que chaque conteneur contient b cartons, et que chaque carton contient c canettes.

(1) Montrer que le nombre total des canettes sur la plate-forme est $a \ltimes (b \ltimes c)$.

(2) Montrer que le nombre total des canettes sur la plate-forme est $(a \ltimes b) \ltimes c$.

Exercice. Démontrer (au moins d'une manière informelle) que pour tous nombres naturels a, b et c, $a \rtimes (b \rtimes c) = (a \rtimes b) \rtimes c$.

Évidemment, pour tous a et b naturels, $b \rtimes a = a \ltimes b$ (par définition). Cependant, on peut être surpris de remarquer que

$$4 \ltimes 3 = \underbrace{3 + 3 + 3 + 3}_{4 \text{ fois}} = 12 = \underbrace{4 + 4 + 4}_{3 \text{ fois}} = 3 \ltimes 4.$$

Est-ce une coïncidence ?

Exercice. Déterminer s'il existe deux nombres naturels a et b plus petits que 5 tels que $b \ltimes a \neq a \ltimes b$.

Exercice. Démontrer (au moins d'une manière informelle) que pour tous nombres naturels a et b, $b \ltimes a = a \ltimes b$.

On peut montrer que pour tous nombres naturels a et b, b fois a est le même nombre que a fois b : $b \ltimes a = a \ltimes b$, ou, écrit autrement,

$$a \rtimes b = a \ltimes b.$$

Le *produit* de nombres naturels a et b est défini, indifféremment, comme a fois b ou comme b fois a, et est traditionnellement noté « $a \times b$ », ou « $a \cdot b$ », ou tout simplement « ab ».

Ainsi on a défini l'*opération de multiplication* ($\times$) (aussi notée « $(\cdot)$ ») qui à deux nombres naturels a et b associe leur produit $ab = a \cdot b = a \times b = a \ltimes b = a \rtimes b$.

Exercice. (1) Calculer le produit $a \times b$ pour tous les nombres naturels a et b de 1 à 9 (dresser la table de multiplication).

(2) Dresser les tables de multiplication pour les bases 2 et 5. Pour chaque base, toutes les valeurs dans sa table doivent être écrites en cette base.

La multiplication ($\times$) de nombres naturels peut aussi être définie par les deux règles suivantes, en utilisant uniquement l'opération d'addition ($+$), l'opération successeur s, et le nombre *zéro* 0 :

(1) $a \times 0 = 0$, (2) $a \times sb = a \times b + a$.

Voici les six identités les plus importantes satisfaites par l'opération de multiplication (pour les nombres naturels) :

(1) $a \times (b \times c) = (a \times b) \times c$,

(2) $a \times 1 = a = 1 \times a$,

(3) $b \times a = a \times b$,

(4) $a \times (b + c) = a \times b + a \times c$,

(5) $a \times (b - c) = a \times b - a \times c$ si $c \leqslant b$,

(6) $a \times 0 = 0$.

Exercice. Démontrer ces identités (au moins d'une manière informelle).

Voici deux propriétés importantes :

(1) si $a \neq 0$ et $b \neq 0$, alors $a \times b \neq 0$,

(2) si $a \times c = b \times c$ et que $c \neq 0$, alors $a = b$.

Ainsi, pour tout nombre naturel $a \neq 0$, l'opération de multiplication par a (d'un autre nombre naturel) est « réversible » : on peut déterminer b si on connaît $b \times a$ et a.

La dernière propriété s'écrit autrement ainsi :

si $a \neq b$ et $c \neq 0$, alors $a \times c \neq b \times c$.

On peut observer une propriété plus précise :

si $a < b$ et $c > 0$, alors $a \times c < b \times c$.

I.8. Divisibilité

On dit qu'un nombre naturel a *divise* un nombre naturel b si et seulement si il existe un nombre naturel c tel que $b = a \times c$.

Par exemple, 2, 3 et 4 divisent 12, mais 5 ne le divise pas. Tout nombre naturel divise 0. Le nombre 0 ne divise que lui-même. Le nombre 1 divise tout.

On utilise la notation « $a \mid b$ » pour dire « a divise b », par exemple : $3 \mid 12$, $5 \nmid 12$, $5 \mid 0$, $0 \mid 0$, $0 \nmid 5$, $1 \mid 5$.

Ainsi on a défini la *relation de divisibilité* ($\mid$) entre nombres naturels.

Au lieu de dire que a divise b, on peut dire que b *se factorise* par a, ou encore que a est un *diviseur* de b, ou que b est un *multiple* de a. Voici donc quatre façons différentes d'exprimer une même relation entre a et b, notée « $a \mid b$ » :

(1) a divise b,

(2) b se factorise par a,

(3) a est diviseur de b,

(4) b est multiple de a.

Par exemple, 3 est diviseur de 12, et 12 est multiple de 3.

Les nombres naturels qui sont multiples de 2 sont dits *pairs*, et les autres sont dits *impairs*.

Proposition. *Si un nombre naturel a divise un nombre naturel $b \neq 0$, alors $1 \leqslant a \leqslant b$.*

Exercice. Prouver cette proposition.

Voici les trois propriétés les plus importantes de la relation de divisibilité ($|$) de nombres naturels :

(1) si $a \mid b$ et $b \mid c$, alors $a \mid c$,

(2) $a \mid a$,

(3) si $a \mid b$ et $b \mid a$, alors $a = b$.

Exercice. Démontrer les trois propriétés.

Remarque. Si on définit la relation de divisibilité pour les *entiers relatifs* de la manière analogique, la propriété (3) pour la divisibilité des entiers relatifs ne sera pas satisfaite.

Remarque. Les relations d'ordre ($\leqslant$) et ($\geqslant$) sur les nombres naturels (ainsi que sur les entiers relatifs, ou sur les réels) satisfont les mêmes trois propriétés que celles données ci-dessus pour la divisibilité des nombres naturels.

Définition. Un nombre naturel d est dit *diviseur commun* (ou *commun diviseur*) de plusieurs nombres naturels donnés si et seulement si d est diviseur de chacun de ces nombres.

Exemple. Les nombres naturels 1, 2, 6 sont diviseurs communs de 12 et 18. Les nombres naturels 10 et 15 sont diviseurs communs de 0, 30 et 60.

Définition. Deux nombres naturels sont dits *premiers entre eux* si et seulement si le nombre 1 est leur seul diviseur commun (naturel). Au lieu de dire que a et b sont premiers entre eux, on peut aussi dire que a est *premier avec* b.

Exemple. Les nombres naturels 10 et 21 sont premiers entre eux, mais 10 et 15 ne le sont pas (5 est un diviseur commun de 10 et 15).

Définition. Un nombre naturel m est dit *multiple commun* (ou *commun multiple*) de plusieurs nombres naturels donnés si et seulement si m est multiple de chacun de ces nombres.

Exemple. Les nombres naturels 0, 30, 60 sont multiples communs de 10 et 15. Les nombres naturels 12 et 18 sont multiples communs de 1, 2 et 6.

Proposition. *Soient a, b, c trois nombres naturels tels que c divise a et b. Alors c divise $a + b$. Si, en plus, $a \geqslant b$, alors c divise $a - b$.*

Exercice. Prouver cette proposition.

Exercice. (1) Montrer qu'un nombre naturel est multiple de 3 si et seulement si la somme des chiffres de son écriture décimale est multiple de 3.

(2) Prouver l'énoncé analogique pour la divisibilité par 9.

(3) Montrer qu'un nombre naturel est multiple de 5 si et seulement si la somme des chiffres de son écriture hexadécimale est multiple de 5.

I.9. Division

La définition de l'opération de *division* repose sur la propriété suivante des nombres naturels :

si $b \times a = c \times a$ et $a \neq 0$, alors $b = c$.

Soient a et b deux nombres naturels. On peut tenter de chercher un nombre naturel c tel que $c \times a = b$. Si $a \nmid b$, il n'y en a pas. Si $a = b = 0$, alors tout nombre naturel c convient. Si $a \neq 0$ et que $a \mid b$, alors il y a un et un seul nombre naturel c tel que $a \times c = c \times a = b$. Dans ce dernier cas, l'unique nombre c tel que $c \times a = b$ est dit le *quotient* de b par a et est noté « $b \div a$ », ou « $b : a$ », ou « b/a », ou « $a \backslash b$ », ou « $\frac{b}{a}$ ». Dans les autres cas, aucun nombre naturel n'est dit « quotient de b par a ». (Mais on pourra définir le quotient de b par a comme un nombre *rationnel* tant que $a \neq 0$.)

Par exemple, $12 \div 3 = 4$, mais on n'a pas défini la valeur de l'expression « $12 \div 5$ », ni la valeur de l'expression « $12 \div 0$ », ni la valeur de l'expression « $0 \div 0$ », comme un nombre naturel.

Ainsi on a défini l'*opération de division* ($\div$) (aussi notée « $(/)$ » ou parfois « $(:)$ ») qui à deux nombres naturels associe leur quotient, tant que leur quotient est défini.

La définition de l'opération de division donnée ci-dessus peut être exprimée par l'équivalence suivante :

$$b \div a = c \quad \Leftrightarrow \quad \begin{cases} b = c \times a \\ a \neq 0 \end{cases}.$$

L'opération de division ($\div$) de nombres naturels peut aussi être définie par les trois propriétés suivantes, à la condition que l'opération de multiplication ($\times$) est déjà définie :

(1) $(a \times b) \div b = a$ si $b \neq 0$,

(2) $(a \div b) \times b = a$ si $b \mid a$ et $b \neq 0$,

(3) la valeur de « $a \div b$ » n'est définie (comme un nombre naturel) que si $b \mid a$ et $b \neq 0$.

En fait, la deuxième propriété résulte de la première, et la première résulte de la deuxième, donc il suffit de garder une seule parmi les deux.[2]

Voici quelques identités remarquables satisfaites par l'opération de division (pour les nombres naturels) :

(1) $a \times (b \div c) = (a \times b) \div c$ si $c \mid b$ et $c \neq 0$,

[2] Supposons que l'opération ($\div$) est définie de telle façon que $(a \times b) \div b = a$ pour tous les nombres naturels a et b tels que $b \neq 0$. Soient a et b deux nombres naturels arbitraires mais tels que $b \mid a$ et $b \neq 0$. Alors il existe un nombre naturel c tel que $a = c \times b$. Or, si $a = c \times b$, alors $(a \div b) \times b = ((c \times b) \div b) \times b = c \times b = a$, car $(c \times b) \div b = c$.
Supposons maintenant que l'opération ($\div$) est définie de telle façon que $(a \div b) \times b = a$ pour tous les nombres naturels a et b tels que $b \mid a$ et $b \neq 0$. Soient a et b deux nombres naturels arbitraires et posons $c = a \times b$. Alors $\underbrace{((a \times b) \div b)} \times b = (c \div b) \times b = c = \underline{a} \times b$, et donc $(a \times b) \div b = a$.

(2) $a \div (b \times c) = (a \div c) \div b$ si $b \times c \mid a$ et $b \times c \neq 0$,

(3) $a \div (b \div c) = (a \times c) \div b$ si $c \mid b \mid a \times c$ et $b \neq 0$,

(4) $(a \div b) \times (b \div c) = a \div c$ si $c \mid b \mid a$ et $b \neq 0$,

(5) $(a \times c) \div (b \times c) = a \div b$ si $b \mid a$ et $b \times c \neq 0$,

(6) $(a \div b) \times c = (a \times c) \div b$ si $b \mid a$ et $b \neq 0$,

(7) $(a \div b) \div c = (a \div c) \div b$ si $b \times c \mid a$ et $b \times c \neq 0$,

(8) $a \div (a \div b) = b$ si $b \mid a$ et $a \neq 0$,

(9) $a \div 1 = a$,

(10) $a \div a = 1$ si $a \neq 0$,

(11) $(a + b) \div c = a \div c + b \div c$ si $c \mid a$, $c \mid b$ et $c \neq 0$,

(12) $(a - b) \div c = a \div c - b \div c$ si $c \mid a$, $c \mid b$, $c \neq 0$ et $b \leqslant a$,

(13) $0 \div a = 0$ si $a \neq 0$.

Exercice. Démontrer ces identités (au moins d'une manière informelle).

Exercice. Déduire ces identités algébriquement à partir des propriétés algébriques de la multiplication présentées précédemment.

I.10. Exponentiation, puissances

Si a et b sont deux nombres naturels, alors la b-ième *puissance* de a, ou a *élevé à la* b*-ième puissance*, ou a *puissance* b, est le nombre noté « a^b » et défini ainsi :

$$a^b \overset{\text{déf}}{=} 1 \underbrace{\times a \times a \times \cdots \times a}_{b \text{ fois}}.$$

Par exemple : $a^0 = 1$, $a^1 = a$, $a^2 = a \times a$, $a^3 = a \times a \times a$.

Dans une expression de la forme « a^b », la valeur de « a » est dit la *base*, et la valeur de « b » est dit l'*exposant*.

Le nombre a^b est aussi dit a *exposant* b, ainsi que l'*exponentielle* de b en *base* a.

Ainsi on a défini l'*opération puissance*, ou l'*opération d'exponentiation*, qui à deux nombres naturels a et b associe le nombre a^b (la b-ième puissance de a, l'exponentielle de b en base a).

Si a est un nombre naturel, alors le *carré* de a, ou a *au carré*, est le nombre $a^2 = a \times a$ (a puissance 2), et le *cube* de a, ou a *au cube*, est le nombre $a^3 = a \times a \times a$ (a puissance 3).

L'exponentiation de nombres naturels peut aussi être définie par les deux règles suivantes, en utilisant uniquement l'opération de multiplication, l'opération successeur s, et les nombres *zéro* 0 et *un* 1 :

(1) $a^0 = 1$, (2) $a^{sb} = a^b \times a$.

Remarque. Il n'y a pas de consensus général sur le sens de « 0^0 ». D'après la définition donnée ici, $0^0 = 1$. Cependant, en *analyse mathématique*, parfois on décide que l'expression « 0^0 » n'ait pas de sens ou que sa valeur ne soit pas définie (comme pour « $0 \div 0$ »).

Exercice. Supposons qu'on a n jours pour réviser m matières, et qu'on veut chaque jour réviser une et une seule matière. En revanche, on peut passer plusieurs jours à réviser une même matière, on peut alterner entre différentes matières, et ne pas réviser certaines parmi elles. Il reste à décider quel jour on revise quelle matière. Montrer qu'on a exactement m^n possibilités.

Voici quelques identités remarquables satisfaites par l'opération d'exponentiation (pour les nombres naturels) :

(1) $a^{b\times c} = (a^b)^c$,

(2) $a^1 = a$,

(3) $a^{b+c} = a^b \times a^c$,

(4) $a^{b-c} = a^b \div a^c$ si $a \neq 0$ et $c \leqslant b$,

(5) $a^0 = 1$,

(6) $(a \times b)^c = a^c \times b^c$,

(7) $(a \div b)^c = a^c \div b^c$ si $b \neq 0$ et $b \mid a$,

(8) $1^c = 1$.

Exercice. Démontrer ces identités (au moins d'une manière informelle).

Voici deux propriétés importantes :

(1) si $a^c = b^c$ et que $c \neq 0$, alors $a = b$,

(2) si $c^a = c^b$ et que $c \neq 0$ et $c \neq 1$, alors $a = b$.

Ainsi,

(1) pour tout nombre naturel $a \neq 0$, l'opération qui à tout nombre naturel b associe b^a est « réversible », et

(2) pour tout nombre naturel $a > 1$, l'opération qui à tout nombre naturel b associe a^b est « réversible ».

Ces deux propriétés s'écrivent autrement ainsi :

(1) si $a \neq b$ et $c \neq 0$, alors $a^c \neq b^c$, (2) si $a \neq b$, $c \neq 0$ et $c \neq 1$, alors $c^a \neq c^b$.

On peut observer deux propriétés plus précises :

(1) si $a < b$ et $c > 0$, alors $a^c < b^c$, (2) si $a < b$ et $c > 1$, alors $c^a < c^b$.

I.11. Exponentiations itérées, notation de Knuth

Donald Knuth a proposé d'utiliser une notation avec des flèches pour l'opération d'exponentiation, ainsi que pour les *exponentiations (ré-)itérées.*[3]

Avec la notation de Knuth, « $a \uparrow b$ » veut dire a^b :

$$a \uparrow b \overset{\text{déf}}{=} a^b = \underbrace{a \times (\cdots \times (a \times}_{b \text{ fois}} 1) \cdots).$$

Les opérations ($\uparrow\uparrow$), ($\uparrow\uparrow\uparrow$), et ainsi de suite, sont définies par récurrence :

$$a \uparrow\uparrow b \overset{\text{déf}}{=} \underbrace{a \uparrow (\cdots \uparrow (a \uparrow}_{b \text{ fois}} 1) \cdots),$$
$$a \uparrow\uparrow\uparrow b \overset{\text{déf}}{=} \underbrace{a \uparrow\uparrow (\cdots \uparrow\uparrow (a \uparrow\uparrow}_{b \text{ fois}} 1) \cdots),$$

et ainsi de suite.

Par example :

$$\begin{aligned} 2 \uparrow 3 &= 2 \times (2 \times (2 \times 1)) = 2 \times 2 \times 2 = 8, \\ 3 \uparrow 2 &= 3 \times (3 \times 1) = 3 \times 3 = 9, \\ 2 \uparrow\uparrow 3 &= 2 \uparrow (2 \uparrow (2 \uparrow 1)) = 2 \uparrow (2 \uparrow 2) = 2 \uparrow 4 = 16, \\ 3 \uparrow\uparrow 2 &= 3 \uparrow (3 \uparrow 1) = 3 \uparrow 3 = 27. \end{aligned}$$

Les opérations ($\uparrow$), ($\uparrow\uparrow$), ($\uparrow\uparrow\uparrow$), et ainsi de suite, peuvent aussi être définies à l'aide de l'opération successeur s :

$$\begin{aligned} a \uparrow 0 &= 1, & a \uparrow sb &= a \times (a \uparrow b), \\ a \uparrow\uparrow 0 &= 1, & a \uparrow\uparrow sb &= a \uparrow (a \uparrow\uparrow b), \\ a \uparrow\uparrow\uparrow 0 &= 1, & a \uparrow\uparrow\uparrow sb &= a \uparrow\uparrow (a \uparrow\uparrow\uparrow b), \\ &\cdots \end{aligned}$$

Exercice. Calculer $2 \uparrow\uparrow\uparrow 3$ et $3 \uparrow\uparrow\uparrow 2$.

Observons que pour tout nombre naturel a,

$$a = a + 0 = a \times 1 = a \uparrow 1 = a \uparrow\uparrow 1 = a \uparrow\uparrow\uparrow 1 = \cdots .$$

Une autre observation curieuse :

$$4 = 2 + 2 = 2 \times 2 = 2 \uparrow 2 = 2 \uparrow\uparrow 2 = 2 \uparrow\uparrow\uparrow 2 = \cdots .$$

[3] Le terme « puissances itérées » à la place d'« exponentiations itérées » est courant. Cependant, ce n'est pas une *fonction puissance* qui est itérée dans « $a \uparrow\uparrow b$ », mais une *fonction exponentielle*. On pourrait dire que pour calculer $2 \uparrow 2$ on effectue une exponentiation, pour calculer $2 \uparrow\uparrow 2$ on effectue une exponentiation itérée, pour calculer $2 \uparrow\uparrow\uparrow 2$ on effectue une exponentiation itérée itérée, et ainsi de suite.

I.12. Factorielle

Considérons l'opération qui à tout nombre naturel a associe un nombre naturel noté « $a!$ », définie par les deux règles suivantes :

(1) $0! \overset{\text{déf}}{=} 1$, (2) $(sa)! \overset{\text{déf}}{=} a! \times sa$.

Si a est un nombre naturel, alors le nombre $a!$ défini ci-dessus est dit la *factorielle* de a, ou *a-factorielle*.

Exemple. La factorielle de 1 est 1, la factorielle de 2 est 2, la factorielle de 3 est 6.

Exercice. Calculer 4!, 5!, 6!.

Exercice. Supposons qu'on a n jours pour réviser n matières, et qu'on veut réviser chaque matière en un jour, et qu'on veut chaque jour ne reviser qu'une seule matière. Il reste à décider quel jour on revise quelle matière. Montrer qu'on a exactement $n!$ possibilités.

I.13. Division entière (division euclidienne)

Proposition. *Soient a et b deux nombres naturels tels que $b \neq 0$. Alors il existe un unique couple de nombres naturels q et r tel que* :

$$a = b \times q + r \quad \textit{et} \quad r < b.$$

Exercice. Prouver cette proposition.

Définition. Si a, b, q, r sont quatre nombres naturels tels que $b \neq 0$ et que

$$a = b \times q + r \quad \text{et} \quad r < b,$$

alors le nombre q est dit le *quotient* de la *division entière* de a par b, et le nombre r est dit le *reste* de la division entière de a par b. On dit aussi *division euclidienne* au lieu de *division entière*.

Exemple. Le quotient et le reste de la division entière de 100 par 7 sont 14 et 2, car $100 = 7 \times 14 + 2$ et $2 < 7$.

Le système de numération décimal usuel, ainsi que les systèmes de numération analogues de toutes les autres bases, permet d'effectuer la division entière par un algorithme plus ou moins efficace. Par exemple, trouvons le quotient et le reste de la division entière de 2222 par 33. Commençons par observer que $33 \times 100 = 3300 > 2222$. Ensuite, effectuons la division entière de 2222 par $33 \times 10 = 330$:

$$\begin{aligned} 2222 &= 330 \times 1 + 1892 \\ &= 330 \times 2 + 1562 \\ &= 330 \times 3 + 1232 \\ &= 330 \times 4 + 902 \\ &= 330 \times 5 + 572 \\ &= 330 \times 6 + 242 \qquad (330 \times 6 = 1980). \end{aligned}$$

Donc, le quotient de la division entière de 2222 par 330 est 6, et le reste est 242. Maintenant, effectuons la division entière de 242 par 33 :

$$\begin{aligned}
242 &= 33 \times 1 + 209 \\
&= 33 \times 2 + 176 \\
&= 33 \times 3 + 143 \\
&= 33 \times 4 + 110 \\
&= 33 \times 5 + 77 \\
&= 33 \times 6 + 44 \\
&= 33 \times 7 + 11 \qquad (33 \times 7 = 231).
\end{aligned}$$

En conclusion :

$$2222 = 330 \times 6 + 33 \times 7 + 11 = 33 \times 60 + 33 \times 7 + 11 = 33 \times 67 + 11.$$

On peut effectuer la division entière de 2222 par 33 d'une manière un peu plus efficace, voici comment. Commençons par noter que

$$\begin{aligned}
&33 \times 1 = 33, \\
&33 \times 2 = 33 + 33 = 66, \\
&33 \times 3 = 66 + 33 = 99, \\
&33 \times 4 = 99 + 33 = 132, \\
&33 \times 5 = 132 + 33 = 165, \\
&33 \times 6 = 165 + 33 = 198, \\
&33 \times 7 = 198 + 33 = 231, \\
&33 \times 8 = 231 + 33 = 264, \\
&33 \times 9 = 264 + 33 = 297.
\end{aligned}$$

Ensuite, on remarque que

$$33 \times 6 \times 10 = 1980 \leqslant 2222 < 2310 = 33 \times 7 \times 10,$$

et que

$$2222 = 1980 + 242 = 33 \times 6 \times 10 + 242 = 33 \times 60 + 242.$$

Puis, on remarque que

$$33 \times 7 = 231 \leqslant 242 < 264 = 33 \times 8,$$

et que

$$242 = 231 + 11 = 33 \times 7 + 11.$$

En conclusion :

$$2222 = 33 \times 60 + 33 \times 7 + 11 = 33 \times 67 + 11.$$

Ce dernier calcul peut être présenté schématiquement ainsi :

$$\begin{array}{r|l} 2222 & 33 \\ \hline -1980 & 60 \\ \hline 242 & \\ -231 & 7 \\ \hline 11 & 67 \end{array} \quad \text{ou} \quad \begin{array}{r|l} 2222 & 33 \\ \hline -1980 & 67 \\ \hline 242 & \\ -231 & \\ \hline 11 & \end{array} \quad \text{ou} \quad \begin{array}{r|l} 2222 & 33 \\ \hline -198 & 67 \\ \hline 242 & \\ -231 & \\ \hline 11 & \end{array}$$

Exercice. Effectuer la division entière de trois cent douze par dix-huit en présentant tout le calcul, ainsi que les résultats, en base cinq.

I.14. PGCD et PPCM

Définition. Un nombre naturel d est dit un *plus grand commun diviseur* (*PGCD*) de nombres naturels a et b si et seulement si

(1) d est diviseur commun de a et b, et

(2) d est multiple de tout diviseur commun de a et b.

Autrement dit, un PGCD de a et b est un tel diviseur commun de a et b qu'il se factorise par tous les autres.

Observons que 1 est le PGCD de deux nombres naturels si et seulement si ces nombres sont premiers entre eux.

Exercice. Montrer que si a et b sont deux nombres naturels, et que c et d sont deux plus grands communs diviseurs de a et b, alors $c = d$.

Exemple. On peut montrer que 6 est le plus grand commun diviseur de 12 et 18. En effet, il n'y a que 4 diviseurs communs de 12 et 18 : 1, 2, 3 et 6, et 6 est multiple de chacun des autres.

Exercice. Trouver le PGCD de 0 et 0 (s'il existe).

Observons que pour tout nombre naturel a, le plus grand commun diviseur de a et 0 est a.

Définition. Un nombre naturel m est dit un *plus petit commun multiple* (*PPCM*) de nombres naturels a et b si et seulement si

(1) m est multiple commun de a et b, et

(2) m est diviseur de tout multiple commun de a et b.

Autrement dit, un PPCM de a et b est un tel multiple commun de a et b qu'il divise tous les autres.

Exercice. Montrer que si a et b sont deux nombres naturels, et que m et n sont deux plus petits communs multiples de a et b, alors $m = n$.

Exemple. On peut montrer que 30 est le plus petit commun multiple de 10 et 15.

Observons que pour tout nombre naturel a, le plus petit commun multiple de a et 1 est a.

Notation. Pour deux nombres naturels a et b, on va noter « $\mathrm{pgcd}(a, b)$ » l'unique plus grand commun diviseur de a et b (s'il existe), et « $\mathrm{ppcm}(a, b)$ » l'unique plus petit commun multiple de a et b (s'il existe).

Voici une propriété remarquable :

$$\mathrm{pgcd}(a, b) = a \quad \Leftrightarrow \quad a \mid b \quad \Leftrightarrow \quad \mathrm{ppcm}(a, b) = b.$$

En particulier, comme déjà observé, $\mathrm{pgcd}(a, 0) = a = \mathrm{ppcm}(1, a)$, car $1 \mid a \mid 0$.

Exercice. Soient a et b deux nombres naturels. Prouver que $\mathrm{pgcd}(a, \mathrm{ppcm}(a, b)) = a$ et que $\mathrm{ppcm}(a, \mathrm{pgcd}(a, b)) = a$.

Exercice. Soient a et b deux nombres naturels et d un diviseur commun de a et b. Prouver que $\mathrm{ppcm}(a, b) \times d \mid a \times b$. Indication : on peut écrire $a = d \times p$ et $b = d \times q$.

Remarque. Si a et b sont deux nombres naturels différents de 0, alors le plus petit commun multiple de a et b n'est pas leur *plus petit* commun multiple au sens usuel : comme 0 est multiple de tout nombre naturel, c'est 0 qui est le *plus petit* commun multiple de a et b au sens usuel. Pareil, le plus grand commun diviseur de deux nombres naturels n'est pas toujours le *plus grand* au sens usuel, car le plus grand commun diviseur de 0 et 0 est 0, mais tout nombre naturel est diviseur de 0, donc il n'y en a pas du *plus grand* au sens usuel.

Étudions les rapports entre le PGCD et l'ordre usuel ($\leqslant$) sur les diviseurs communs et entre le PPCM et l'ordre usuel sur les multiples communs.

Lemme. *Si un nombre naturel a divise un nombre naturel $b \neq 0$, alors $1 \leqslant a \leqslant b$.*

Démonstration. Soit q un nombre naturel tel que $a \times q = b$. Comme $b \neq 0$, on a que $a \neq 0$ et $q \neq 0$. Donc, $a \geqslant 1$ et $q \geqslant 1$, et $b \geqslant a \times 1 = a$. □

Corollaire. *Si a et b sont deux nombres naturels, c est un diviseur commun de a et b, d est le PGCD de a et b, et que $d \neq 0$, alors $d \geqslant c \geqslant 1$.*

Corollaire. *Si a et b sont deux nombres naturels, n est un multiple commun de a et b, m est le PPCM de a et b, et que $n \neq 0$, alors $1 \leqslant m \leqslant n$.*

On n'a pas encore répondu à la question suivante :

Question. Est-ce que tout couple de nombres naturels possède le PGCD et le PPCM ?

On verra que la réponse est affirmative. Le lemme suivant va nous aider traiter le cas du PGCD, et il sera aussi utilisé pour justifier un algorithme de calcul du PGCD.

Lemme. *Si a, b, c, q sont quatre nombres naturels tels que $a = b \times q + c$, alors*

(1) *tout diviseur commun de b et c est diviseur de a,*

(2) *tout diviseur commun de a et b est diviseur de c,*

(3) *en particulier,* $\operatorname{pgcd}(a, b) = \operatorname{pgcd}(b, c)$ *si* $\operatorname{pgcd}(a, b)$ *ou* $\operatorname{pgcd}(b, c)$ *existe.*

Exercice. Prouver ce lemme.

Ce lemme peut être utilisé pour calculer le PGCD de deux nombres naturels. Par exemple, utilisons le pour trouver le PGCD de 123 et 456 (et ainsi montrer qu'il existe). Pour cela, effectuons les divisions entières suivantes :

$$\begin{aligned} 456 &= 123 \times 3 + 87, \\ 123 &= 87 \times 1 + 36, \\ 87 &= 36 \times 2 + 15, \\ 36 &= 15 \times 2 + 6, \\ 15 &= 6 \times 2 + 3, \\ 6 &= 3 \times 2 \quad (+0). \end{aligned}$$

Comme 3 est le PGCD de 3 et 0 (ainsi que de 6 et 3), d'après le dernier lemme on obtient que

$$\begin{aligned} \operatorname{pgcd}(456, 123) = \operatorname{pgcd}(123, 87) = \operatorname{pgcd}(87, 36) = \operatorname{pgcd}(36, 15) = \operatorname{pgcd}(15, 6) \\ = \operatorname{pgcd}(6, 3) = 3. \end{aligned}$$

Cette méthode du calcul du PGCD s'appelle l'*algorithme d'Euclide*.

Exercice. Trouver le PGCD de 2222 et 333, s'il existe.

Il paraît clair que grâce au dernier lemme et à l'algorithme d'Euclide, on peut déterminer le PGCD de n'importe quels deux nombres naturels, et qu'en particulier, donc, n'importe quels deux nombres naturels admettent le PGCD. On peut prouver l'existence du PGCD rigoureusement et sans évoquer l'algorithme d'Euclide.

Théorème. *Quels que soient deux nombres naturels, leur PGCD existe.*

Démonstration. Démontrons ce théorème par un raisonnent *par l'absurde* : supposons qu'il existe deux nombres naturels qui n'ont pas du PGCD, et en déduisons une absurdité.

Supposons qu'il existe deux nombres naturels qui n'ont pas du PGCD. Dans ce cas, il existe deux nombres naturels qui n'ont pas du PGCD et dont la somme est la plus petite parmi les somme de tous les couples de nombres naturels qui n'ont pas du PGCD.

Soient donc a et b deux nombres naturels qui n'ont pas du PGCD et dont la somme est la plus petite parmi les sommes de tous les couples de nombres naturels qui n'ont pas du PGCD. Sans perte de généralité, supposons en plus que $a \geqslant b$. (Sinon on peut échanger les rôles de a et b).

Dans ce cas, $b \neq 0$, car $\operatorname{pgcd}(a, 0) = a$. D'où, $(a - b) + b = a < a + b$, et donc il existe le PGCD de $a - b$ et b (d'après le choix de a et b). Or, d'après le dernier lemme, si le PGCD de $a - b$ et b existe, alors le PGCD de a et b existe aussi (et, en plus, $\operatorname{pgcd}(a, b) = \operatorname{pgcd}(a - b, b)$). Cela contredit le choix de a et b. □

On peut maintenant utiliser le théorème précédent d'existence du PGCD pour démontrer le théorème suivant d'existence du PPCM.

Théorème. *Quels que soient deux nombres naturels, leur PPCM existe.*

Pour démontrer ce théorème, les deux lemmes suivants seront utiles.

Lemme. *Si a, b, m, n sont quatre nombres naturels tels que m et n sont multiples communs de a et b, alors* $\operatorname{pgcd}(m, n)$ *est également un multiple commun de a et b.*

Démonstration. Comme a et b sont diviseurs communs de m et n, ils divisent le PGCD de m et n. □

Lemme. *Si A est un ensemble non vide de nombres naturels, alors il existe un élément de A tel qu'aucun autre élément de A ne le divise.*

Démonstration. S'il n'y a qu'un seul nombre dans A, alors évidemment aucun autre élément de A ne le divise (car il n'y en a pas).

S'il y a au moins deux nombres dans A, alors au moins un nombre dans A est différent de 0. Soit a le plus petit nombre naturel non nul dans A. Alors aucun élément de A autre que a ne divise a.

Dans les deux cas, il y a un élément de A tel qu'aucun autre élément de A de le divise. □

Démonstration du théorème d'existence du PPCM. Soient a et b deux nombres naturels arbitraires. Évidemment, 0 est un de leurs multiples communs. (D'ailleurs, $a \times b$ l'est aussi.) Soit m un multiple commun de a et b tel qu'aucun autre multiple commun de a et b ne le divise. (Un tel m existe d'après le lemme précédent.) Montrons que $\operatorname{ppcm}(a, b) = m$. Pour cela il ne reste qu'à prouver que m divise tout multiple commun de a et b.

Soit n un multiple commun arbitraire de a et b. D'après un lemme, $\operatorname{pgcd}(m, n)$ est un multiple commun de a et b. (C'est grâce au théorème précédent qu'on sait que $\operatorname{pgcd}(m, n)$ existe.) Cependant, $\operatorname{pgcd}(m, n)$ divise m. Or, d'après le choix de m, aucun multiple commun de a et b different de m ne divise m. D'où, $\operatorname{pgcd}(m, n) = m$, et donc m divise n. □

Grâce à ce théorème, pour montrer qu'un nombre naturel m est le PPCM de deux nombres naturels a et b, il suffit de vérifier que :

(1) m est un multiple commun de a et b, et que

(2) aucun autre multiple commun de a et b ne divise m.

Exemple. Clairement, 30 est un multiple commun de 10 et 15. Donc, le PPCM de 10 et 15 (qui existe, d'après le théorème) est diviseur de 30 et multiple de 10 et de 15. Les seuls multiples de 15 qui divisent 30 sont 15 et 30, et parmi ces deux, seulement 30 est multiple de 10. Donc, 30 est le PPCM de 10 et 15.

Il existe cependant une méthode plus directe pour calculer efficacement le PPCM de deux nombres naturels, la voici. On peut prouver[4] que si a et b sont deux nombres naturels premiers entre eux, alors $\text{ppcm}(a,b) = a \times b$. Il en résulte que pour tous nombres naturels a et b,

$$\text{ppcm}(a,b) \times \text{pgcd}(a,b) = a \times b.$$

I.15. Algorithme d'Euclide

Pour trouver le PGCD de deux nombres naturels, on peut utiliser l'*algorithme d'Euclide*, qui utilise la division entière (division euclidienne).

Soient a et b deux nombres naturels dont on cherche le PGCD. Posons

$$r_0 = a, \qquad r_1 = b.$$

Si $r_1 = b = 0$, alors $\text{pgcd}(a,b) = r_0 = a$. Sinon, posons q_2 et r_2 le quotient et le reste de la division entière de $r_0 = a$ par $r_1 = b$:

$$a = b \times q_2 + r_2, \qquad r_2 < b.$$

Ainsi,

$$r_0 = r_1 \times q_2 + r_2, \qquad r_2 < r_1.$$

Si $r_2 \neq 0$, on calcule le quotient q_3 et le reste r_3 de la division entière de $r_1 = b$ par r_2 :

$$r_1 = b = r_2 \times q_3 + r_3, \qquad r_3 < r_2.$$

On continue ainsi et détermine les quotients q_{k+2} et les restes r_{k+2} *par récurrence* :

$$r_k = r_{k+1} \times q_{k+2} + r_{k+2}, \qquad r_{k+2} < r_{k+1}.$$

On finira par trouver n tel que $r_{n+2} = 0$ et donc r_{n+1} divise r_n :

$$r_n = r_{n+1} \times q_{n+2}, \qquad r_{n+2} = 0.$$

Alors $\text{pgcd}(a,b) = r_{n+1}$. En effet, d'après un lemme précédent,

$$\begin{aligned}\text{pgcd}(a,b) = \text{pgcd}(r_0,r_1) = \text{pgcd}(r_1,r_2) = \cdots \\ = \text{pgcd}(r_n,r_{n+1}) = \text{pgcd}(r_{n+1},0) = r_{n+1}.\end{aligned}$$

[4] Une preuve habituelle passe par le *lemme de Bézout*.

I.16. PGCD et PPCM de familles arbitraires

En général, on définit le PGCD et le PPCM d'une n'importe quelle famille de nombres naturels de la même manière que dans le cas des couples :

- le PGCD d'une famille est le diviseur commun de cette famille qui est multiple de tout diviseur commun de cette famille,
- le PPCM d'une famille est le multiple commun de cette famille qui est diviseur de tout multiple commun de cette famille.

Par exemple :

$$\operatorname{pgcd}(36, 60, 90) = 6, \quad \operatorname{ppcm}(36, 60, 90) = 180.$$

Pour une famille (a) réduite à un seul nombre naturel a, on a :

$$\operatorname{pgcd}(a) = a = \operatorname{ppcm}(a).$$

Pour la *famille vide* $()$ on a :

$$\operatorname{pgcd}() = 0, \quad \operatorname{ppcm}() = 1.$$

Les définitions du PGCD et du PPCM dans la section I.14 ont été données pour des couples de nombres naturels pour des raison pédagogiques, car à première vue une définition et un traitement plus généraux peuvent paraître plus complexes.

I.17. Nombres premiers et factorisation

Tout nombre naturel divise *zéro*, mais *zéro* ne divise que lui-même.

Le nombre *un* divise tous les nombres naturels, mais le seul nombre naturel qui le divise est *un* lui-même.

Ainsi, en ce qui concerne la relation de divisibilité pour les nombres naturels, les nombres *zéro* et *un* sont « les plus singuliers ».[5]

Cependant, certains autres nombres naturels, qui s'appellent les nombres *premiers*, se distinguent bien par rapport à la relation de divisibilité.

Définition. Un nombre naturel a est dit *premier*[6] si et seulement si

(1) a ne divise pas 1, et

(2) les seuls nombres naturels qui divisent a sont 1 et a.

[5] La relation de divisibilité ($|$) sur les nombres naturels est une *relation d'ordre*. Par rapport à cette relation d'ordre, 0 est le plus grand nombre, et 1 est le plus petit.

Définition. Les nombres naturels différents de 0 et de 1 qui ne sont pas premiers sont dits *composés*.

Exemple. Les nombres 2, 3 et 5 sont premiers, alors que les nombres 4 et 6 sont composés.

On peut séparer les nombres naturels strictement plus grands que 1 en premiers et en composés par le *crible d'Ératosthène*.

Proposition. *Tout nombre naturel composé peut être écrit comme un produit de nombres premiers.*

Exercice. Prouver cette proposition.

On peut prouver que si un nombre naturel est décomposé en un produit de nombres premiers de deux façons différentes, les deux décompositions ne diffèrent que par l'ordre des facteurs. Par exemple,

$$60 = 2 \times 2 \times 3 \times 5 \quad \text{et} \quad 60 = 3 \times 2 \times 5 \times 2.$$

Ce fait s'appelle le *théorème fondamental de l'arithmétique*, on l'énonce ici sans démonstration.[7]

Théorème (Théorème fondamental de l'arithmétique)**.** *Tout nombre naturel composé peut être écrit comme un produit de nombres premiers d'une unique façon, à l'ordre près des facteurs.*

Voici un exemple d'un problème non résolu (jusqu'en 2024) en arithmétique :

Conjecture (*Conjecture de Goldbach*)**.** *Tout nombre naturel pair strictement supérieur à 2 s'écrit comme la somme de deux nombres premiers.*

Question. La conjecture de Goldbach, est-elle vraie ou fausse ?

[6] Si on voulait suivre de près la terminologie de l'algèbre moderne, on devrait appeler ces nombres *irréductibles*, plutôt que premiers, et on devrait appeler *premiers* les nombres p différents de 0 et de 1 tels que pour tout produit $a \times b$ qui est divisible par p, a ou b est divisible par p. Cependant, d'après le *lemme d'Euclide*, une telle définition moderne des nombres premiers serait en fait équivalente à la définition donnée ici. Autrement dit, lorsqu'il s'agit des nombres naturels, on peut montrer qu'il n'y a pas de différence entre les éléments irréductibles et les éléments premiers au sens de l'algèbre moderne.

[7] Une preuve habituelle passe par le *lemme de Bézout*.

II. Nombres entiers relatifs

II.1. Qu'est-ce que c'est, un nombre entier relatif ?

Rappelons nous que l'opération de soustraction de nombres naturels peut être appliquée à deux nombres naturels a et b à la condition que $b \leqslant a$, et que dans ce cas le résultat de cette opération est la *différence* entre a et b, notée « $a - b$ ». La valeur de la différence « $a - b$ » n'est définie comme un nombre naturel que si $b \leqslant a$.

Exercice. Essayer de compléter les tableaux suivants :

3	5	1	4	7	4
8	10	10	13	16	13
100	?	?	100	100	?

La différence entre deux nombres exprime un certain rapport entre ces nombres, qu'on pourrait appeler leur « rapport additif ». Par exemple, le « rapport additif » entre 5 et 3 est le même qu'entre 10 et 8, et le même qu'entre 102 et 100, mais différent de celui entre 7 et 4. En effet :

$$5 - 3 = 10 - 8 = 102 - 100 = 2 \neq 3 = 7 - 4.$$

Cependant, il paraît clair que le « rapport additif » entre 3 et 5 doit être le même qu'entre 8 et 10. Or, aucun nombre naturel n'exprime, dans le sens précédent, le « rapport additif » entre 3 et 5, ni entre 8 et 10, car les valeurs des différences « $3-5$ » et « $8-10$ » ne sont pas définies comme nombres naturels.

Avant de tenter de régler cette situation embarrassante, essayons de clarifier l'idée du « rapport additif ».

Notons $(\underset{+}{\simeq})$ la relation entre couples de nombres naturels dont le sens sera le suivant :

> « $(a, b) \underset{+}{\simeq} (c, d)$ » veut dire que le « rapport additif » entre b et a est le même qu'entre d et c.

Essayons de donner une définition précise de la relation $(\underset{+}{\simeq})$ en accord avec l'idée intuitive du « rapport additif ». On souhaite, en particulier, que

$$(3, 5) \underset{+}{\simeq} (8, 10) \underset{+}{\simeq} (100, 102) \underset{+}{\not\simeq} (4, 7),$$

mais aussi que

$$(5,3) \mathrel{\underset{+}{\simeq}} (10,8) \mathrel{\underset{+}{\simeq}} (102,100) \mathrel{\underset{+}{\not\simeq}} (3,5).$$

Dans le cas où $a \leqslant b$ et $c \leqslant d$, on souhaite que l'équivalence suivante soit satisfaite :

$$(a,b) \mathrel{\underset{+}{\simeq}} (c,d) \quad \Leftrightarrow \quad b-a = d-c.$$

Cependant, l'équation « $b-a=d-c$ » ne peut servir comme la définition du sens de « $(a,b) \mathrel{\underset{+}{\simeq}} (c,d)$ » que si $a \leqslant b$ et $c \leqslant d$, car sinon, les valeurs des différences « $b-a$ » et « $d-c$ » ne sont pas toutes les deux définies (comme nombres naturels). Le problème est dans l'opération de soustraction.

Comment peut-on vérifier si $b-a=d-c$ sans utiliser l'opération de soustraction ? Une solution est évidente : il suffit de vérifier si $b+c=d+a$, car

$$b-a=d-c \quad \Leftrightarrow \quad b+c=d+a$$

dans le cas où $a \leqslant b$ et $c \leqslant d$.

Les valeurs des deux membres de l'équation « $b+c=d+a$ » (de ses parties gauche et droite) sont définies pour tous nombres naturels a, b, c, d. On va utiliser cette équation pour définir la relation $(\mathrel{\underset{+}{\simeq}})$, qui est censée traduire l'idée intuitive du « rapport additif ».

Définition. Définissons la relation $(\mathrel{\underset{+}{\simeq}})$ par l'équivalence suivante :

$$(a,b) \mathrel{\underset{+}{\simeq}} (c,d) \quad \Leftrightarrow \quad b+c=d+a,$$

où a, b, c, d sont quatre nombres naturels arbitraires.

Notons que, d'après cette définition,

$$\begin{aligned}(a,b) \mathrel{\underset{+}{\simeq}} (c,d) \quad &\Leftrightarrow \quad (b,a) \mathrel{\underset{+}{\simeq}} (d,c) \\ &\Leftrightarrow \quad (a,c) \mathrel{\underset{+}{\simeq}} (b,d) \quad \Leftrightarrow \quad (c,a) \mathrel{\underset{+}{\simeq}} (d,b).\end{aligned}$$

Exercice. Vérifier sur des exemples si la définition donnée ci-dessus de la relation $(\mathrel{\underset{+}{\simeq}})$ est en accord avec l'idée intuitive du « rapport additif ».

Exercice. Soient a, b, c, d quatre nombres naturels. Montrer que $(a,b) \mathrel{\underset{+}{\simeq}} (c,d)$ si et seulement si il existe deux nombres naturels e et f tels que $e+a=f+c$ et $e+b=f+d$.

Exercice. Trouver des nombres naturels a, b, c, d tels que

$$(5,8) \mathrel{\underset{+}{\simeq}} (a,11), \qquad (5,8) \mathrel{\underset{+}{\simeq}} (11,b), \qquad (8,5) \mathrel{\underset{+}{\simeq}} (c,11), \qquad (8,5) \mathrel{\underset{+}{\simeq}} (11,d),$$

s'ils existent. Combien des choix y a-t-il pour les valeurs de a, de b, de c et de d ?

Exercice. Trouver des nombres naturels a, b, c, d tels que

$$(5,8) \underset{+}{\simeq} (a,2), \qquad (5,8) \underset{+}{\simeq} (2,b), \qquad (8,5) \underset{+}{\simeq} (c,2), \qquad (8,5) \underset{+}{\simeq} (2,d).$$

s'ils existent. Combien des choix y a-t-il pour les valeurs de a, de b, de c et de d ?

Les trois propriétés suivantes de la relation $(\underset{+}{\simeq})$ sont d'une importance particulière pour la définition des entiers relatifs :

(1) si $(a,b) \underset{+}{\simeq} (c,d)$ et $(c,d) \underset{+}{\simeq} (e,f)$, alors $(a,b) \underset{+}{\simeq} (e,f)$,

(2) $(a,b) \underset{+}{\simeq} (a,b)$,

(3) si $(a,b) \underset{+}{\simeq} (c,d)$, alors $(c,d) \underset{+}{\simeq} (a,b)$.

Exercice. Démontrer ces propriétés.

Prenons en plus note des deux lemmes suivants.

Lemme. *Pour tous nombres naturels* a, b, c, $(a,b) \underset{+}{\simeq} (a+c,\ b+c)$.

Lemme. (1) *Si* a, b, c *sont trois nombres naturels tels que* $(a,b) \underset{+}{\simeq} (a,c)$, *alors* $b = c$.

(2) *Si* a, b, c *sont trois nombres naturels tels que* $(a,c) \underset{+}{\simeq} (b,c)$, *alors* $a = b$.

Exercice. Prouver ces lemmes.

Ainsi on a défini le sens de la phrase « le rapport additif entre b et a est le même qu'entre d et c » : cela veut dire que $b + c = d + a$. En plus, si $a \leqslant b$ et $c \leqslant d$, les « rapports additifs » entre b et a et entre d et c sont exprimés par les nombres naturels $b-a$ et $d-c$, et pour voir si les deux « rapports additifs » sont les mêmes, il suffit de voir si $b - a = d - c$. Mais, comme déjà mentionné, aucun nombre naturel n'exprime, dans ce sens, le « rapport additif » entre 3 et 5, ni entre 8 et 10, car les valeurs des différences « $3 - 5$ » et « $8 - 10$ » ne sont pas définies comme nombres naturels.

Une issue de cette situation est d'inventer de nouveaux nombres pour exprimer les différences entre n'importe quels nombres naturels.

Définition. Définissons les nombres *entiers*, aussi dits *entiers relatifs*, ainsi :

(1) tout nombre naturel est *entier* ;

(2) si a et b sont deux nombres naturels tels que la valeur de la différence « $b - a$ » n'est pas définie comme un nombre naturel (car $a > b$), on admet que la différence $b - a$ est un *entier* ;

(3) si a, b, c, d sont quatre nombres naturels, on admet que l'*entier* $d - c$ est le même que l'*entier* $b - a$ si et seulement si $(c,d) \underset{+}{\simeq} (a,b)$:

$$d - c = b - a \quad \Leftrightarrow \quad (c,d) \underset{+}{\simeq} (a,b) \quad \Leftrightarrow \quad b + c = d + a \ ;$$

(4) tout *entier* est la différence de deux nombres naturels.

Notation. L'ensemble des entiers relatifs sera noté « $\mathbf{Z}$ ».

Notons qu'on n'a pas besoin d'un nouveau système de numération pour écrire les nombres entiers relatifs car tout entier relatif peut être écrit comme la différence de deux nombres naturels. En plus, tout entier relatif qui n'est pas nombre naturel peut être écrit sous la forme « $0 - a$ », où a est un nombre naturel.

Notation. On adopte une écriture abrégée pour les différences de la forme « $0 - a$ » : on n'écrira pas le premier « 0 ». Ainsi, au lieu de « $0 - a$ », on peut écrire « $-a$ » tout court.

Exemple. L'expression « -42 » veut dire $0 - 42$.

II.2. Relations d'ordre usuelles

Définition. Définissons les relations $(\leqslant)$, $(\geqslant)$, $(<)$, $(>)$ entre des entiers par les équivalences suivantes, où a, b, c sont des nombres naturels arbitraires :

$$b - a \leqslant c - a \quad \Leftrightarrow \quad b \leqslant c, \qquad b - a \geqslant c - a \quad \Leftrightarrow \quad b \geqslant c,$$
$$b - a < c - a \quad \Leftrightarrow \quad b < c, \qquad b - a > c - a \quad \Leftrightarrow \quad b > c.$$

Il reste à vérifier que ces définitions sont toutes correctes et complètes.

Proposition. *La définition donnée ci-dessus de la relation $(\leqslant)$ est correcte. C'est-à-dire, quels que soient six nombres naturels a_1, a_2, b_1, b_2, c_1, c_2, si $b_1 - a_1 = b_2 - a_2$ et $c_1 - a_1 = c_2 - a_2$, alors*

$$b_1 \leqslant c_1 \quad \Leftrightarrow \quad b_2 \leqslant c_2.$$

Démonstration. Soient a_1, a_2, b_1, b_2, c_1, c_2 six nombres naturels tels que $b_1 - a_1 = b_2 - a_2$ et $c_1 - a_1 = c_2 - a_2$. Alors,

$$(a_1, b_1) \mathrel{\dot{+}} (a_2, b_2) \quad \text{et} \quad (a_1, c_1) \mathrel{\dot{+}} (a_2, c_2)$$

(voir la définition des *entiers relatifs*), c'est-à-dire, $b_1 + a_2 = b_2 + a_1$ et $c_1 + a_2 = c_2 + a_1$.

D'après les propriétés des nombres naturels déjà établies,

$$b_1 \leqslant c_1 \quad \Leftrightarrow \quad b_1 + a_2 \leqslant c_1 + a_2 \quad \Leftrightarrow \quad b_2 + a_1 \leqslant c_2 + a_1 \quad \Leftrightarrow \quad b_2 \leqslant c_2. \qquad \square$$

Exercice. Vérifier si les définitions des relations $(\geqslant)$, $(<)$, $(>)$ sont correctes elles aussi.

Proposition. *Les définitions données ci-dessus des relations $(\leqslant)$, $(\geqslant)$, $(<)$, $(>)$ sont toutes complètes. C'est-à-dire, quels que soient deux entiers x et y, il existe trois nombres naturels a, b, c tels que $x = b - a$ et $y = c - a$.*

Démonstration. Soient x et y deux nombres entiers arbitraires. Soient a, b, c, d nombres naturels tels que $x = a - b$ et $y = c - d$. Alors

$$x = (a + d) - (b + d) \quad \text{et} \quad y = (c + b) - (d + b) = (c + b) - (b + d). \qquad \square$$

Exercice. Essayons de définir une relation (Δ) entre des nombres naturels par l'équivalence suivante :

$$a+b\,\Delta\,c+d \quad\Leftrightarrow\quad b+c=d+a.$$

Est-ce que cette tentative définition est correcte ?

Proposition. *Quels que soient les nombres naturels a, b, c, d, les équivalences suivantes sont satisfaites* :

$$\begin{aligned} a-b\leqslant c-d &\quad\Leftrightarrow\quad a+d\leqslant c+b, & a-b\geqslant c-d &\quad\Leftrightarrow\quad a+d\geqslant c+b,\\ a-b<c-d &\quad\Leftrightarrow\quad a+d<c+b, & a-b>c-d &\quad\Leftrightarrow\quad a+d>c+b. \end{aligned}$$

Démonstration. Comme $a-b=(a+d)-(b+d)$ et $c-d=(c+b)-(d+b)$, on a :

$$a-b\leqslant c-d \quad\Leftrightarrow\quad (a+d)-(b+d)\leqslant(c+b)-(d+b) \quad\Leftrightarrow\quad a+d\leqslant c+b.$$

On vérifie de la même manière les cas de $(\geqslant)$, de $(<)$ et de $(>)$. □

Les relations $(\leqslant)$, $(\geqslant)$, $(<)$, $(>)$ sont reliées par les équivalences suivantes :

(1) $x\leqslant y$ si et seulement si $y\geqslant x$,

(2) $x<y$ si et seulement si $y>x$,

(3) $x\leqslant y$ si et seulement si $x<y$ ou $x=y$,

(4) $x<y$ si et seulement si $x\leqslant y$ et $x\neq y$.

Exercice. Vérifier ces équivalences.

Les quatre propriétés suivantes de la relation $(\leqslant)$ entre des nombres entiers sont les mêmes que pour la relation $(\leqslant)$ entre des nombres naturels :

(1) si $x\leqslant y$ et $y\leqslant z$, alors $x\leqslant z$,

(2) $x\leqslant x$,

(3) si $x\leqslant y$ et $y\leqslant x$, alors $x=y$,

(4) $x\leqslant y$ ou $y\leqslant x$.

Exercice. Démontrer ces propriétés.

Les trois propriétés suivantes de la relation $(<)$ entre des nombres entiers sont les mêmes que pour la relation $(<)$ entre des nombres naturels :

(1) si $x<y$ et $y<z$, alors $x<z$,

(2) si $x<y$, alors $x\neq y$,

(3) si $x\neq y$, alors $x<y$ ou $y<x$.

Exercice. Démontrer ces propriétés.

Notation. Si x et y sont deux entiers, on va noter « $\max(x,y)$ » le plus grand entre x et y et « $\min(x,y)$ » le plus petit entre x et y :

$$\max(x,y)\overset{\text{déf}}{=}\begin{cases} x & \text{si}\quad x\geqslant y,\\ y & \text{si}\quad x\leqslant y; \end{cases} \qquad \min(x,y)\overset{\text{déf}}{=}\begin{cases} x & \text{si}\quad x\leqslant y,\\ y & \text{si}\quad x\geqslant y. \end{cases}$$

Entiers positifs et négatifs

Définition. Soient a et b deux nombres naturels. Le nombre entier $b - a$ est dit :

(1) *positif* (au sens large) si et seulement si $a \leqslant b$,

(2) *négatif* (au sens large) si et seulement si $a \geqslant b$,

(3) *strictement positif* si et seulement si $a < b$,

(4) *strictement négatif* si et seulement si $a > b$.

Autrement dit,

(1) x est *positif* (au sens large) si et seulement si $x \geqslant 0$,

(2) x est *négatif* (au sens large) si et seulement si $x \leqslant 0$,

(3) x est *strictement positif* si et seulement si $x > 0$,

(4) x est *strictement négatif* si et seulement si $x < 0$.

Ainsi, les entiers positifs (au sens large) sont les nombres naturels, et tout entier négatif peut être écrit sous la forme « $-a$ », où a est un nombre naturel.

II.3. « Translation additive » d'un nombre naturel par un entier relatif

En introduisant les nombres entiers relatifs, on a *prolongé* l'opération de soustraction des nombres naturels pour que la valeur de la différence « $a - b$ » soit définie quels que soient les nombres naturels a et b (même quand $a < b$), et on a défini les nombres entiers comme les valeurs de toutes les différences entre des nombres naturels. Cependant, pour l'instant, les opérations d'addition, de soustraction, de multiplication et de division ne sont définies que pour les nombres naturels.

Dans la section suivante on va chercher une façon convenable de prolonger l'opération d'addition des nombres naturels en une opération définies pour n'importe quels entiers relatifs, qu'on va toujours appeler l'*addition* et noter « $+$ ».

Pour commencer, on va adopter la définition suivante, qui paraît tout à fait naturelle.

Définition. Si a et b sont deux nombres naturels, et que $x = b - a$, alors la *somme* de a et de l'entier x, notée « $a + x$ », est b :

$$a + (b - a) \overset{\text{déf}}{=} b.$$

Cette définition est clairement en accord avec la définition de l'addition des nombres naturels, car si a, b et $b - a$ sont tous nombres naturels, alors la somme de a et $b - a$ est b, au sens de l'addition des nombres naturels. Ainsi, cette définition, pourvu qu'elle soit correcte, *prolonge* l'opération d'addition des nombres naturels.

Il est facile de montrer que cette définition est correcte, c'est-à-dire, que si a est un nombre naturel et x est un entier relatif tels que la définition s'applique pour donner une valeur de « $a + x$ », alors elle ne donnera qu'une valeur unique. En effet : si b_1 et b_2 sont deux nombres naturels tels que $x = b_1 - a = b_2 - a$, alors $b_1 = b_2$, d'après un lemme précédent.

Exemple. $5 + (-3) = 5 + (0 - 3) = 5 + (2 - 5) = 2$.

Exercice. Calculer et simplifier : $1 + (-1)$.

Cependant, la valeur de « $3 + (0 - 5)$ » n'est pas encore définie.

Soit x un entier. Si a et b sont deux nombres naturels tels que $x = b - a$, alors on va, de manière informelle, appeler $b = a + x$ le *« translaté additif »* de a par x. On peut parler de l'opération de *« translation additive »* par x, qui a certains nombres naturels associe leurs translatés additifs par x.

II.4. Addition

D'après la définition de la « translation additive », quels que soient trois nombres naturels a, b, c, on a :

$$a + (b - a) + (c - b) = b + (c - b) = c = a + (c - a).$$

Cette observation suggère qu'il est naturel de définir l'opération d'*addition* $(+)$ des entiers relatifs de telle manière que pour tous nombres naturels a, b, c, on ait l'égalité :

$$(b - a) + (c - b) = c - a.$$

Pour voir si on peut imposer cette identité comme la définition de l'addition d'entiers, il suffit de vérifier si pour tous nombres naturels a_1, a_2, b_1, b_2, c_1, c_2 tels que $b_1 - a_1 = b_2 - a_2$ et $c_1 - b_1 = c_2 - b_2$, on a $c_1 - a_1 = c_2 - a_2$. D'après le lemme suivant, c'est le cas.

Lemme. *Soient six nombres naturels* a_1, a_2, b_1, b_2, c_1, c_2 *tels que* $(a_1, b_1) \underset{+}{\frown} (a_2, b_2)$ *et* $(b_1, c_1) \underset{+}{\frown} (b_2, c_2)$. *Alors* $(a_1, c_1) \underset{+}{\frown} (a_2, c_2)$.

Démonstration. Comme $(a_1, b_1) \underset{+}{\frown} (a_2, b_2)$, on en déduit que $(a_1, a_2) \underset{+}{\frown} (b_1, b_2)$. Comme $(b_1, c_1) \underset{+}{\frown} (b_2, c_2)$, on en déduit que $(b_1, b_2) \underset{+}{\frown} (c_1, c_2)$. Ainsi, $(a_1, a_2) \underset{+}{\frown} (c_1, c_2)$. D'où, $(a_1, c_1) \underset{+}{\frown} (a_2, c_2)$. □

Définition. Si a, b, c sont trois nombres naturels, $x = b - a$ et $y = c - b$, alors la *somme* des entiers x et y, notée « $x + y$ », est $c - a$:

$$(b - a) + (c - b) \overset{\text{déf}}{=} c - a.$$

Exercice. Montrer, en utilisant le dernier lemme, que cette définition est correcte. Vérifier en plus qu'elle est complète, c'est-à-dire, qu'elle définit la somme de deux n'importe quels entiers.

Ainsi on a défini l'opération d'*addition* $(+)$ qui à deux n'importe quels entiers associe leur somme.

Exemples.

$$(3-1)+(9-4)=(3-1)+(8-3)=8-1=7,$$
$$(3-1)+(4-9)=(9-7)+(4-9)=4-7=0-3=-3,$$
$$(1-3)+(9-4)=(1-3)+(6-1)=6-3=3,$$
$$(1-3)+(4-9)=(5-7)+(0-5)=0-7=-7.$$

Exercice. Calculer et simplifier : $(-1)+1$, $1+(-1)$, $(-1)+(-1)$.

En général, pour tous nombres naturels a, b, c, d,

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

Exercice. Essayons de définir une opération (Δ) sur des nombres naturels par l'identité suivante :

$$(a+b)\,\Delta\,(c+d)\overset{\text{déf}}{=}ab+cd.$$

Est-ce que cette tentative définition est correcte ?

Les trois identités suivantes satisfaites par l'opération d'addition de nombres entiers sont les mêmes que pour l'opération d'addition de nombres naturels :

(1) $x+(y+z)=(x+y)+z$,

(2) $x+0=x=0+x$,

(3) $y+x=x+y$.

Exercice. Démontrer ces identités.

Notation. On adopte une écriture abrégée pour les sommes de la forme « $0+x$ » : au lieu de « $0+x$ », on peut écrire « $+x$ ».

Exemple. L'expression « $+(+(+42))$ » veut dire $0+(0+(0+42))$.

Lemme. *Soit x un entier arbitraire. Soient a et b deux nombres naturels tels que $x=b-a$. Posons $y=a-b$. Alors $x+y=0=y+x$.*

Exercice. Prouver ce lemme.

Proposition. *Pour tous entiers x et y, il existe un unique entier z tel que $z+y=x$.*

Démonstration. Soient x et y deux entiers arbitraires, et soit v un entier tel que $y+v = v+y = 0$ (il existe d'après le lemme précédent). Alors

$$(x+v)+y = x+(v+y) = x+0 = x.$$

On a montré l'existence, il reste à montrer l'unicité : que si z est un entier tel que $z+y = x$, alors $z = x+v$.

Soit z un entier tel que $z+y = x$. Alors

$$z = z+0 = z+(y+v) = (z+y)+v = x+v. \qquad \square$$

Définition. Deux entiers x et y sont dits *opposés* l'un de l'autre si et seulement si $x+y = 0$.

Rapport aux relations d'ordre usuelles

Proposition. *Pour tous entiers x, y, z, si $x < y$, alors $x+z < y+z$.*

Exercice. Prouver cette proposition.

Corollaire. *Pour tous entiers x, y, z, les équivalences suivantes sont satisfaites* :

$$x < y \quad \Leftrightarrow \quad x+z < y+z, \qquad\qquad x \leqslant y \quad \Leftrightarrow \quad x+z \leqslant y+z.$$

Exercice. Prouver ce corollaire.

II.5. Soustraction

La définition de l'opération de *soustraction* repose sur les propriétés suivantes des nombres entiers :

(1) si $y+x = z+x$, alors $y = z$,

(2) quels que soient x et y, il existe z tel que $z+x = y$.

Soient x et y deux entiers. On peut tenter de chercher un entier z tel que $z+x = y$. Comme montré précédemment, il y en a un, et un seul.

Définition. Si x et y sont deux entiers, alors l'unique entier z tel que $z+x = y$ est dit la *différence* de y et x et est noté « $y-x$ ».

Ainsi on a défini l'opération de *soustraction* $(-)$ qui à deux n'importe quels entiers associe leur différence.

Exercice. Calculer et simplifier : $(-1)-1$, $1-(-1)$, $(-1)-(-1)$.

La définition de l'opération de soustraction $(-)$ donnée ci-dessus peut être exprimée par l'équivalence suivante :

$$y - x = z \quad \Leftrightarrow \quad y = z + x.$$

L'opération de soustraction $(-)$ d'entiers peut aussi être définie par les deux identités suivantes, à la condition que l'opération d'addition $(+)$ est déjà définie :

(1) $(x + y) - y = x$, (2) $(x - y) + y = x$.

En fait, n'importe quelle de ces deux identités suffit toute seule pour définir l'opération de soustraction d'entiers.

Exercice. Montrer que n'importe quelle de ces deux identités suffit toute seule pour définir l'opération de soustraction d'entiers.

Exercice. Soient a, b, c, d quatre nombres naturels. Montrer que

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

Les identités suivantes sont satisfaites (pour tous x, y, z entiers) :

(1) $x + (y - z) = (x + y) - z$,
(2) $x - (y + z) = (x - z) - y$,
(3) $x - (y - z) = (x + z) - y$,
(4) $(x - y) + (y - z) = x - z$,
(5) $(x + z) - (y + z) = x - y$,
(6) $(x - y) + z = (x + z) - y$,
(7) $(x - y) - z = (x - z) - y$,
(8) $x - (x - y) = y$,
(9) $x - 0 = x$,
(10) $x - x = 0$.

Exercice. Démontrer ces identités.

Notation. On adopte une écriture abrégée pour les différences de la forme « $0 - x$ » : au lieu de « $0 - x$ », on peut écrire « $-x$ ».

Exemple. L'expression « $-(-(-42))$ » veut dire $0 - (0 - (0 - 42))$.

Observons que :

(1) $-(-x) = 0 - (0 - x) = x$,

(2) $x + (-y) = x + (0 - y) = (x + 0) - y = x - y$.

Rapport aux relations d'ordre usuelles

Proposition. *Pour tous entiers x, y, z, si $x < y$, alors $z - x > z - y$.*

Exercice. Prouver cette proposition.

Corollaire. *Pour tous entiers x, y, z, les équivalences suivantes sont satisfaites* :

$$x < y \quad \Leftrightarrow \quad z - x > z - y, \qquad\qquad x \leqslant y \quad \Leftrightarrow \quad z - x \geqslant z - y.$$

En particulier :

(1) x est strictement positif si et seulement si $-x$ est strictement négatif,

(2) x est strictement négatif si et seulement si $-x$ est strictement positif,

(3) x est positif (au sens large) si et seulement si $-x$ est négatif (au sens large),

(4) x est négatif (au sens large) si et seulement si $-x$ est positif (au sens large).

Exercice. Prouver le dernier corollaire.

II.6. Multiplication

Définition. Si a est un nombre naturel et x est un entier, alors le *produit* de x et a, noté « $x \times a$ », « $x \cdot a$ », ou « xa », est défini par la règle :

$$xa \overset{\text{déf}}{=} 0 \underbrace{+ x + x + \cdots + x}_{a \text{ fois}}.$$

Lemme. *Pour tous a, b, c naturels, $(a - b)c = ac - bc$.*

L'identité $(a - b)c = ac - bc$ est déjà établie dans le cas où tous les nombres qui interviennent dans le calcul sont naturels, c'est-à-dire, dans le cas où $b \leqslant a$. Il reste à vérifier le cas général.

Démonstration du lemme. D'après les propriétés de l'addition et de la soustraction déjà établies,

$$\begin{aligned}
(a-b)c &= 0 \underbrace{+ (a-b) + (a-b) + \cdots + (a-b)}_{c \text{ fois}} \\
&= 0 \underbrace{+ (a + (-b)) + (a + (-b)) + \cdots + (a + (-b))}_{c \text{ fois}} \\
&= 0 \underbrace{+ a + a + \cdots + a}_{c \text{ fois}} \underbrace{+ (-b) + (-b) + \cdots + (-b)}_{c \text{ fois}} \\
&= 0 \underbrace{+ a + a + \cdots + a}_{c \text{ fois}} - (0 \underbrace{+ b + b + \cdots + b}_{c \text{ fois}}) \\
&= ac - bc.
\end{aligned}$$

□

Définition. Si a et b sont deux nombres naturels, x est un entier, et $y = b - a$, alors le *produit* de x et y, noté « $x \times y$ », « $x \cdot y$ », ou « xy », est défini par la règle :

$$\begin{aligned} x(b-a) &\overset{\text{déf}}{=} 0 \underbrace{+x+x+\cdots+x}_{b \text{ fois}} \underbrace{-x-x-\cdots-x}_{a \text{ fois}} \\ &= 0 \underbrace{+x+x+\cdots+x}_{b \text{ fois}} - (0 \underbrace{+x+x+\cdots+x}_{a \text{ fois}}) = xb - xa. \end{aligned}$$

Exercice. Vérifier si cette définition est correcte.

Ainsi on a défini l'opération de *multiplication* $(\cdot)$ (aussi notée « $(\times)$ ») qui à deux n'importe quels entiers associe leur produit.

Exercice. Calculer $(-1)1$, $1(-1)$ et $(-1)(-1)$.

Proposition. *Pour tous entiers x et y, $yx = xy$.*

Démonstration. Soient x et y deux entiers arbitraires. Soient a, b, c, d quatre nombres naturels tels que $a - b = x$ et $c - d = y$. Alors, en appliquant le dernier lemme et d'autres propriétés déjà établies, on trouve :

$$\begin{aligned} xy &= x(c-d) = xc - xd = (a-b)c - (a-b)d = (ac - bc) - (ad - bd) \\ &= ac - bc + bd - ad = ca - cb + db - da = ca - da + db - cb \\ &= (ca - da) - (cb - db) = (c-d)a - (c-d)b = ya - yb = y(a-b) = yx. \end{aligned}$$ □

Les identités suivantes sont satisfaites :

(1) $x(yz) = (xy)z$,

(2) $x \cdot 1 = x = 1 \cdot x$,

(3) $yx = xy$,

(4) $x(y+z) = xy + xz$,

(5) $x(y-z) = xy - xz$,

(6) $x \cdot 0 = 0$.

Exercice. Démontrer ces identités.

Proposition. *Si x et y sont deux entiers tels que $x \neq 0$ et $y \neq 0$, alors $xy \neq 0$.*

Démonstration. On sait que si a et b sont deux nombres naturels non nuls, alors ab est non nul aussi.

Si x est un entier non nul qui n'est pas un nombre naturel, alors $x < 0$, $-x > 0$, et donc $-x$ est un nombre naturel non nul.

Soient x et y deux entiers arbitraires mais différents de 0. Supposons que $xy = 0$. Alors $(-x)y = 0$, $x(-y) = 0$, et $(-x)(-y) = 0$. Or, parmi les nombres x et $-x$, ainsi que parmi les nombres y et $-y$, il y en a un qui est naturel (et non nul). Soient a le nombre naturel tel que $a = x$ ou $a = -x$, et b le nombre naturel tel que $b = y$ ou $b = -y$. Alors $a \neq 0$, $b \neq 0$, mais $ab = 0$. On a obtenu une contradiction avec le fait que le produit de deux nombres naturels non nuls ne peut pas être nul. Donc, $xy \neq 0$. □

Corollaire. *Si x, y, z sont trois entiers tels que $xz = yz$ et que $z \neq 0$, alors $x = y$.*

Exercice. Prouver ce corollaire.

Exercice. Trouver tous les nombres entiers x tels que $xx + 5x + 4 = 0$. Indication : $xx + 5x + 4 = xx + x + 4x + 4 = (x+1)(x+4)$.

Rapport aux relations d'ordre usuelles

Proposition. *Pour tous entiers x, y, z,*

(1) *si $x < y$ et $z > 0$, alors $xz < yz$,* (2) *si $x < y$ et $z < 0$, alors $xz > yz$.*

Exercice. Prouver cette proposition.

Corollaire. *Pour tous entiers x, y, z,*

(1) *si $z > 0$, alors les équivalences suivantes sont satisfaites :*

$$x < y \quad \Leftrightarrow \quad xz < yz, \qquad\qquad x \leqslant y \quad \Leftrightarrow \quad xz \leqslant yz,$$

(2) *si $z < 0$, alors les équivalences suivantes sont satisfaites :*

$$x < y \quad \Leftrightarrow \quad xz > yz, \qquad\qquad x \leqslant y \quad \Leftrightarrow \quad xz \geqslant yz.$$

Exercice. Prouver ce corollaire.

Corollaire. *Pour tous entiers x et y,*

(1) *si $x > 0$ et $y > 0$, alors $xy > 0$,* (3) *si $x < 0$ et $y > 0$, alors $xy < 0$,*

(2) *si $x > 0$ et $y < 0$, alors $xy < 0$,* (4) *si $x < 0$ et $y < 0$, alors $xy > 0$.*

Exercice. Prouver ce corollaire.

Corollaire. *Pour tout entier x, $xx \geqslant 0$.*

Exercice. Prouver ce corollaire.

Exercice. Trouver tous les nombres entiers x tels que $xx + 5x + 4 < 0$. Indication : $xx + 5x + 4 = xx + x + 4x + 4 = (x + 1)(x + 4)$.

II.7. Valeur absolue

Définition. Si a et b sont deux nombres naturels, et que $x = b - a$, alors la *valeur absolue* de l'entier x, notée « $|x|$ », est définie ainsi :

$$|b - a| \overset{\text{déf}}{=} \begin{cases} b - a & \text{si} \quad a \leqslant b, \\ a - b & \text{si} \quad b \leqslant a. \end{cases}$$

Autrement dit, si x est un entier, alors

$$|x| \overset{\text{déf}}{=} \begin{cases} +x & \text{si} \quad x \geqslant 0, \\ -x & \text{si} \quad x \leqslant 0. \end{cases}$$

Ainsi, la valeur absolue de tout entier est positive (au sens large).

En utilisant la notation avec « max », on peut définir la valeur absolue d'un entier x par la formule :

$$|x| = \max(x, -x).$$

Une autre façon (équivalente) de définir la valeur absolue d'un entier x est par l'équivalence suivante :

$$|x| = y \quad \Leftrightarrow \quad \begin{cases} xx = yy \\ y \geqslant 0 \end{cases}.$$

Exercice. Montrer que la valeur absolue peut être définie par cette équivalence. Indication : si a et b sont deux nombres naturels tels que $aa = bb$, alors $a = b$, car, pour les nombres naturels a et b, si $a < b$, alors $aa < bb$.

Lemme. *Pour tous entiers x et y,*

$$|x| \leqslant y \quad \Leftrightarrow \quad -y \leqslant x \leqslant y \qquad \textit{et} \qquad |x| < y \quad \Leftrightarrow \quad -y < x < y.$$

Démonstration.

$$|x| \leqslant y \quad \Leftrightarrow \quad \max(x, -x) \leqslant y \quad \Leftrightarrow \quad \begin{cases} x \leqslant y \\ -x \leqslant y \end{cases}$$

$$\Leftrightarrow \quad \begin{cases} x \leqslant y \\ -y \leqslant x \end{cases} \quad \Leftrightarrow \quad -y \leqslant x \leqslant y,$$

$$|x| < y \quad \Leftrightarrow \quad \max(x, -x) < y \quad \Leftrightarrow \quad \begin{cases} x < y \\ -x < y \end{cases}$$

$$\Leftrightarrow \quad \begin{cases} x < y \\ -y < x \end{cases} \quad \Leftrightarrow \quad -y < x < y. \qquad \square$$

Proposition (Inégalité triangulaire)**.** *Pour tous entiers x et y,*

$$|x + y| \leqslant |x| + |y|\,.$$

Démonstration. Comme $|x| \leqslant |x|$ et $|y| \leqslant |y|$, d'après le lemme précédent on a :

$$-|x| \leqslant x \leqslant |x| \quad \text{et} \quad -|y| \leqslant y \leqslant |y|\,.$$

D'où,

$$-(|x| + |y|) \leqslant x + y \leqslant |x| + |y|\,,$$

et donc, encore d'après le lemme précédent,

$$|x + y| \leqslant |x| + |y|\,. \qquad \square$$

L'origine du nom « *inégalité triangulaire* » sera peut-être plus claire si l'on traduit cette inégalité sous la forme suivante :

$$|c - a| \leqslant |b - a| + |c - b|\,.$$

Proposition. *Pour tous entiers x et y,*

$$|xy| = |x|\,|y|\,.$$

Démonstration. Soient x et y deux entiers arbitraires. Alors

$$(xy)(xy) = (xx)(yy) = (|x|\,|x|)(|y|\,|y|) = (|x|\,|y|)(|x|\,|y|),$$

et $|x|\,|y| \geqslant 0$. D'où, $|xy| = |x|\,|y|$, d'après une des définitions équivalentes de la valeur absolue. □

II.8. Divisibilité

Définition. On dit qu'un entier x *divise* un entier y si et seulement si il existe un entier z tel que $y = xz$.

Exercice. Vu que l'ensemble des nombres naturels fait partie de l'ensemble des entiers, maintenant on a deux définitions de la divisibilité pour les nombres naturels. Selon l'ancienne, a divise b si et seulement si il existe un nombre naturel c tel que $b = ac$. Selon la nouvelle, a divise b si et seulement si il existe un entier z tel que $b = az$. Vérifier qu'il n'y a pas de contradiction entre les deux définitions.

Exemples. Les entiers 2, -3 et 4 divisent -12, mais 5 ne le divise pas. Tout entier divise 0. Le nombre 0 ne divise que lui-même. Les nombres 1 et -1 divisent tous les entiers.

Notation. On utilise toujours la notation « $x \mid y$ » pour dire « x divise y ».

Ainsi on a défini la *relation de divisibilité* ($\mid$) entre entiers.

Au lieu de dire que x divise y, on peut dire que y *se factorise* par x, ou encore que x est un *diviseur* de y, ou que y est un *multiple* de x. Voici donc quatre façons différentes d'exprimer une même relation entre x et y, notée « $x \mid y$ » :

(1) x divise y,

(2) y se factorise par x,

(3) x est diviseur de y,

(4) y est multiple de x.

Exemples. L'entier 3 est diviseur de -12, et -12 est multiple de 3.

Définition. Les entiers qui sont multiples de 2 sont dits *pairs*, et les autres sont dits *impairs*.

Lemme. *Pour tous entiers x et y, x divise y si et seulement si $|x|$ divise $|y|$.*

Exercice. Prouver le lemme.

Les deux propriétés suivantes de la relation (|) entre des nombres entiers sont les mêmes que pour la relation (|) entre des nombres naturels :

(1) si $x \mid y$ et $y \mid z$, alors $x \mid z$, (2) $x \mid x$.

Exercice. Démontrer les deux propriétés.

Cependant, il n'est pas vrai en général que si $x \mid y$ et $y \mid x$, alors $x = y$. Ce qui est vrai, en revanche, c'est que si $x \mid y$ et $y \mid x$, alors $|x| = |y|$.[1]

Définition. Deux entiers sont dits *premiers entre eux* si et seulement si tout leur diviseur commun divise 1. Au lieu de dire que a et b sont premiers entre eux, on peut aussi dire que a est *premier avec* b.

Autrement dit, deux entiers sont premiers entre eux si et seulement si ils n'ont pas de diviseurs communs autres que 1 et -1.

Exemples. Les entiers -10 et -21 sont premiers entre eux, mais -10 et 15 ne le sont pas.

Proposition. *Soient x, y, z trois entiers tels que z divise x et y. Alors z divise $x + y$, ainsi que $x - y$.*

Exercice. Prouver cette proposition.

II.9. Division

La définition de l'opération de *division* repose sur la propriété suivante des nombres entiers :

si $yx = zx$ et $x \neq 0$, alors $y = x$.

Soient x et y deux entiers. On peut tenter de chercher un entier z tel que $zx = y$. Si $x \nmid y$, il n'y en a pas. Si $x = y = 0$, alors tout valeur de « z » convient. Si $x \neq 0$ et que $x \mid y$, alors il y a un et un seul entier z tel que $zx = y$.

Définition. Si x est un entier non nul et y est un multiple de x, alors l'unique entier z tel que $zx = y$ est dit le *quotient* de y par x et est noté « $y \div x$ », ou « $y : x$ », ou « y/x », ou « $x\backslash y$ », ou « $\dfrac{y}{x}$ ». Dans les autres cas, aucun entier n'est dit « quotient de y par x ».

Ainsi on a défini l'opération de *division* (/) qui à deux entiers associe leur quotient, tant que leur quotient est défini.

[1] Parfois on utilise la définition suivante : deux entiers sont dits *associés* (entre eux) si et seulement chacun des deux divise l'autre. Ainsi, deux entiers x et y sont associés si et seulement si $x = y$ ou $x = -y$.

Exemples. $12/(-3) = -4$, mais on n'a pas défini la valeur de l'expression « $12/5$ », ni la valeur de l'expression « $12/0$ », ni la valeur de l'expression « $0/0$ », comme un entier.

Exercice. Calculer $(-1)/1$, $1/(-1)$ et $(-1)/(-1)$.

La définition de l'opération de division donnée ci-dessus peut être exprimée par l'équivalence suivante :

$$\frac{y}{x} = z \quad \Leftrightarrow \quad \begin{cases} y = zx \\ x \neq 0 \end{cases}.$$

L'opération de division $(/)$ d'entiers peut aussi être définie par les trois propriétés suivantes, à la condition que l'opération de multiplication $(\cdot)$ est déjà définie :

(1) $(xy)/y = x$ si $y \neq 0$,

(2) $(x/y)y = x$ si $y \neq 0$ et $y \mid x$,

(3) la valeur de « x/y » n'est définie (comme un nombre entier) que si $y \neq 0$ et $y \mid x$.

En fait, la deuxième propriété résulte de la première, et la première résulte de la deuxième, donc il suffit de garder une seule parmi les deux.

Exercice. Montrer que la deuxième propriété résulte de la première, et que la première résulte de la deuxième.

Voici quelques identités remarquables satisfaites par l'opération de division (pour les entiers) :

(1) $x(y/z) = (xy)/z$ si $z \mid y$ et $z \neq 0$,

(2) $x/(yz) = (x/z)/y$ si $yz \mid x$ et $yz \neq 0$,

(3) $x/(y/z) = (xz)/y$ si $z \mid y \mid xz$ et $y \neq 0$,

(4) $(x/y)(y/z) = x/z$ si $z \mid y \mid x$ et $y \neq 0$,

(5) $(xz)/(yz) = x/y$ si $y \mid x$ et $yz \neq 0$,

(6) $(x/y)z = (xz)/y$ si $y \mid x$ et $y \neq 0$,

(7) $(x/y)/z = (x/z)/y$ si $yz \mid x$ et $yz \neq 0$,

(8) $x/(x/y) = y$ si $y \mid x$ et $x \neq 0$,

(9) $x/1 = x$,

(10) $x/x = 1$ si $x \neq 0$,

(11) $(x + y)/z = x/z + y/z$ si $z \mid x$, $z \mid y$ et $z \neq 0$,

(12) $(x - y)/z = x/z - y/z$ si $z \mid x$, $z \mid y$ et $z \neq 0$,

(13) $0/x = 0$ si $x \neq 0$.

Exercice. Démontrer ces identités.

II.10. Exponentiation, puissances

Définition. Si a est un nombre naturel et x est un entier, alors x *puissance* a, ou la a-ième *puissance* de x, ou x *élevé à la* a*-ième puissance*, est le nombre noté « x^a » et défini par la règle :

$$x^a \overset{\text{déf}}{=} 1\underbrace{\cdot x \cdot x \cdot \cdots \cdot x}_{a \text{ fois}}.$$

Les identités suivantes sont satisfaites pour tous a et b naturels et pour tous x et y entiers :

(1) $x^{ab} = (x^a)^b$,

(2) $x^1 = x$,

(3) $x^{a+b} = x^a x^b$,

(4) $x^{a-b} = x^a/x^b$ si $x \neq 0$ et $b \leqslant a$,

(5) $x^0 = 1$,

(6) $(xy)^a = x^a y^a$,

(7) $(x/y)^a = x^a/y^a$ si $y \neq 0$ et $y \mid x$,

(8) $1^a = 1$.

Exercice. Démontrer ces identités.

Définition. Si a et b sont deux nombres naturels, u est un diviseur entier de 1 (autrement dit, $u = \pm 1$), et $x = b - a$, alors u *puissance* x est le nombre noté « u^x » et défini par la règle :

$$u^{b-a} \overset{\text{déf}}{=} 1\underbrace{\cdot u \cdot u \cdot \cdots \cdot u}_{b \text{ fois}}\underbrace{/u/u/\cdots/u}_{a \text{ fois}} = \frac{u^b}{u^a}.$$

Exercice. Vérifier si cette définition est correcte.

Exercice. Calculer 1^{-1} et $(-1)^{-1}$.

II.11. Racines

Définition. Une *racine carrée* d'un nombre x est un nombre y tel que $y^2 = x$. Une *racine cubique* d'un nombre x est un nombre y tel que $y^3 = x$. En général, si n est un nombre naturel non nul, une *racine* n*-ième* d'un nombre x est un nombre y tel que $y^n = x$.

Exemples. Le nombre -3 est une racine carré de 9, 2 est une racine cubique de 8, -1 est une racine 2023-ième de -1.

Exercice. Montrer que pour tout nombre naturel non nul n, 0 est l'unique racine n-ième de 0.

Exercice. Montrer que si n est un nombre naturel non nul pair et x est un entier strictement négatif, alors parmi les nombres entiers[2] il n'y a pas de racines n-ièmes de x.

[2] On peut montrer qu'il n'y en a pas parmi les *nombres réels* non plus. En revanche, parmi les *nombres complexes* il y en a n.

Proposition. (1) *Si u est une racine n-ième de x et v est une racine n-ième de y, alors uv est une racine n-ième de xy.*

(2) *Si x est une racine m-ième de y et y est une racine n-ième de z, alors x est une racine mn-ième de z.*

Exercice. Prouver cette propositions.

Proposition. (1) *Si x est une racine carrée de y, alors $-x$ l'est aussi.*

(2) *Si x et y sont deux racines carrées de z, alors $y = x$ ou $y = -x$.*

Exercice. Prouver cette propositions. Indication : pour la deuxième partie, considérer le produit $(x + y)(x - y)$.

Proposition. *Si n est un nombre naturel non nul et x et y sont deux entiers positifs tels que $x^n = y^n$, alors $x = y$.*

Exercice. Prouver cette propositions.

Proposition. *Si n est un nombre naturel impair et x et y sont deux entiers tels que $x^n = y^n$, alors $x = y$.*

Exercice. Prouver cette propositions.

Définition. Soient n un nombre naturel impair et x un entier qui est la n-ième puissance d'un entier y ($x = y^n$). Alors ***la*** racine n-ième de x est l'unique racine n-ième entière de x (donc y).

Définition. Soient n un nombre naturel non nul et x un entier positif ($x \geqslant 0$) qui est la n-ième puissance d'un entier y ($x = y^n$). Alors ***la*** racine n-ième de x est l'unique racine n-ième positive de x (donc $|y|$). Si x est strictement positif ($x > 0$), alors la racine n-ième positive de x est aussi dite la racine n-ième *principale* de x.

Notation. Si n est un nombre naturel non nul et x est un entier qui admet une racine n-ième entière[3], alors on note « $\sqrt[n]{x}$ » ou « $\sqrt[n]{x}$ » l'unique racine n-ième entière de x si n et impair, et on note « $\sqrt[n]{x}$ » ou « $\sqrt[n]{x}$ » l'unique racine n-ième positive de x si n est pair. Si n est pair et x est strictement négatif, alors la valeur de l'expression « $\sqrt[n]{x}$ » n'est pas définie (l'expression « $\sqrt[n]{x}$ » n'a pas de sens). Dans le cas où $n = 2$, on utilise aussi la notation « $\sqrt{x}$ » au lieu de « $\sqrt[2]{x}$ ».

Ainsi, si n est un nombre naturel *impair*, alors pour tous x et y entiers,

$$\sqrt[n]{x} = y \quad \Leftrightarrow \quad x = y^n,$$

et si n est un nombre naturel non nul *pair*, alors pour tous x et y entiers,

$$\sqrt[n]{x} = y \quad \Leftrightarrow \quad \begin{cases} x = y^n \\ y \geqslant 0 \end{cases}.$$

Pour n naturel *impair*, l'opération $\sqrt[n]{}$ sur les entiers peut aussi être définie par les trois propriétés suivantes :

[3] La même notation sera utilisée pour les racines *réelles*.

(1) $\sqrt[n]{x^n} = x$,

(2) $(\sqrt[n]{x})^n = x$ si x est la n-ième puissance d'un entier,

(3) la valeur de « $\sqrt[n]{x}$ » n'est définie (comme un nombre entier) que si x est la n-ième puissance d'un entier.

En fait, la deuxième propriété résulte de la première, et la première résulte de la deuxième, donc il suffit de garder une seule parmi les deux.

Pour n naturel non nul *pair*, l'opération $\sqrt[n]{}$ sur les entiers peut aussi être définie par les trois propriétés suivantes :

(1) $\sqrt[n]{x^n} = x$ si $x \geqslant 0$,

(2) $(\sqrt[n]{x})^n = x$ si x est la n-ième puissance d'un entier,

(3) la valeur de « $\sqrt[n]{x}$ » n'est définie (comme un nombre entier) que si x est la n-ième puissance d'un entier.

En fait, la deuxième propriété résulte de la première, et la première résulte de la deuxième, donc il suffit de garder une seule parmi les deux.

Exemples. $\sqrt{9} = 3$, $\sqrt[3]{-8} = -2$, $\sqrt[1000]{0} = 0$, $\sqrt[2023]{-1} = -1$, l'expression « $\sqrt{-1}$ » n'a pas de sens (sa valuer n'est pas définie).

Exercice. Calculer $\sqrt{64}$, $\sqrt[3]{64}$ et $\sqrt[3]{-64}$.

Voici quelques identités remarquables pour m et n naturels non nuls, a naturel, et x et y entiers, qui sont satisfaites *à la condition que les valeurs des deux membres* (des parties gauche et droite) *soient définies comme nombres entiers* :

(1) $\sqrt[n]{x^a} = \left(\sqrt[n]{x}\right)^a$,

(2) $\sqrt[n]{\sqrt[m]{x}} = \sqrt[nm]{x}$,

(3) $\sqrt[n]{xy} = \sqrt[n]{x}\,\sqrt[n]{y}$,

(4) $\sqrt[n]{x/y} = \sqrt[n]{x}/\sqrt[n]{y}$,

(5) $\sqrt[n]{1} = 1$, $\sqrt[n]{0} = 0$.

Exercice. Démontrer ces identités.

Observons que $\sqrt{(-1)(-1)} = 1$, alors que la valeur de l'expression « $\sqrt{-1}\sqrt{-1}$ » n'est pas définie (car déjà l'expression « $\sqrt{-1}$ » n'a pas de valeur définie).

II.12. Division euclidienne

Si x et y sont deux entiers avec $y \neq 0$, alors effectuer une *division euclidienne* de x par y veut dire trouver un entier q (le *quotient*) et un entier r (le *reste*) tels que :

(1) $x = yq + r$,

(2) r satisfait une certaine condition précisée d'avance, d'habitude sous forme d'une double inéquation, qui d'habitude assure que le couple (q, r) est unique.

Comme une condition sur le reste qui assure que le couple (q, r) est unique, on peut utiliser, par exemple, une des suivantes :

(1) $0 \leqslant r < |y|$,

(2) $-|y| < r \leqslant 0$,

(3) $0 \leqslant r < y$ ou $y < r \leqslant 0$,

(4) $-|y| < 2r \leqslant |y|$,

(5) $-|y| \leqslant 2r < |y|$.

Exemple. En effectuant la division euclidienne de -100 par -7, on peut, selon la condition souhaitée pour le reste, trouver, par exemple, le quotient 15 et le reste 5, ou le quotient 14 et le reste -2.

II.13. PGCD et PPCM

Les PGCD et les PPCM des nombres entiers sont définies de la même manière que pour les nombres naturels.

Définition. Un nombre entier d est dit un *plus grand commun diviseur* (*PGCD*) de nombres entiers x et y si et seulement si

(1) d est diviseur commun de x et y, et

(2) d est multiple de tout diviseur commun de x et y.

Définition. Un nombre entier m est dit un *plus petit commun multiple* (*PPCM*) de nombres entiers x et y si et seulement si

(1) m est multiple commun de x et y, et

(2) m est diviseur de tout multiple commun de x et y.

Dans le cas des nombres entiers, les PGCD et les PPCM ne sont uniques que lorsque ils sont nuls. En effet, si z est un PGCD de x et y, alors $-z$ l'est aussi, et si z est un PPCM de x et y, alors $-z$ l'est aussi.

Les deux propositions suivantes peuvent être prouvées assez facilement en utilisant l'existence des PGCD et PPCM pour les nombres naturels (ce qui a été prouvé précédemment).

Proposition. *Tous deux nombres entiers ont un unique PGCD positif (au sens large) et un unique PGCD négatif (au sens large), et ces deux PGCD sont opposés l'un de l'autre.*

Proposition. *Tous deux nombres entiers ont un unique PPCM positif (au sens large) et un unique PPCM négatif (au sens large), et ces deux PPCM sont opposés l'un de l'autre.*

Notation. Pour deux nombres entiers x et y, on va noter « $\mathrm{pgcd}(x, y)$ » l'unique PGCD positif de x et y, et « $\mathrm{ppcm}(x, y)$ » l'unique PPCM positif de x et y.

Observons que $\operatorname{pgcd}(x, y) = \operatorname{pgcd}(|x|, |y|)$, et que $\operatorname{ppcm}(x, y) = \operatorname{ppcm}(|x|, |y|)$.
Le lemme suivant sera utilisé pour justifier un algorithme de calcul du PGCD.

Lemme. *Si x, y, z, q sont quatre nombres entiers tels que $x = y \times q + z$, alors*

(1) *tout diviseur commun de y et z est diviseur de x,*

(2) *tout diviseur commun de x et y est diviseur de z,*

(3) *en particulier, les PGCD de x et y sont les mêmes que les PGCD de y et z.*

Exercice. Prouver ce lemme.

II.14. Algorithme d'Euclide

Pour trouver un PGCD de deux nombres entiers x et y, il suffit de trouver le PGCD naturel des nombres naturels $|x|$ et $|y|$, par exemple par la version de l'*algorithme d'Euclide* pour les nombres naturels.

Autrement, on peut appliquer l'algorithme d'Euclide directement au couple de x et y, avec une condition convenable sur les restes des divisions euclidiennes. Toute condition qui garantie qui la suite des valeurs absolues des restes est strictement décroissante (tant qu'il n'y pas eu du reste 0) convient.

Cependant, on peut réduire le nombres des divisions euclidiennes à effectuer en choisissant une telle condition que la valeur absolue du reste soit toujours inférieure ou égale à la moitié de la valeur absolue du diviseur :

$$\begin{aligned}
&r_0 = x, \qquad r_1 = y, \\
&r_0 = r_1 q_2 + r_2, \qquad 2\,|r_2| \leqslant |r_1|\,, \\
&r_1 = r_2 q_3 + r_3, \qquad 2\,|r_3| \leqslant |r_2|\,, \\
&\dots
\end{aligned}$$

II.15. Nombres premiers

Tout nombre entier divise 0, mais 0 ne divise que lui-même.

Les nombres ± 1 divisent tous les nombres entiers, mais les seuls nombres entiers qui divisent 1 ou -1 sont 1 et -1.

Ainsi, en ce qui concerne la relation de divisibilité pour les nombres entiers, les nombres 0 et ± 1 sont « les plus singuliers ».

Cependant, certains autres nombres entiers, qui sont dits *premiers*, se distinguent bien par rapport à la relation de divisibilité.

Définition. Un nombre entier a est dit *premier*[4] si et seulement si

(1) a ne divise pas 1, et

(2) les seuls nombres entiers qui divisent a sont ± 1 et $\pm a$.

Observons qu'un nombre entier a est premier si et seulement si $-a$ est premier.

Définition. Les nombres entiers différents de 0 et de ± 1 qui ne sont pas premiers sont dits *composés*.

Exemple. Les nombres ± 2, ± 3 et ± 5 sont premiers, alors que les nombres ± 4 et ± 6 sont composés.

Proposition. *Tout nombre entier composé peut être écrit comme un produit de nombres entiers premiers.*

Exercice. Prouver cette proposition.

II.16. Lemme de Bézout

Le lemme suivant est connu sous le nom de *lemme de Bézout*, parmi d'autres.

Lemme (Lemme de Bézout)**.** *Si x et y sont deux entiers et z est leur PGCD, alors il existe deux entiers s et t tels que*

$$z = xs + yt.$$

Exercice. Trouver des nombres entiers s et t tels que $12s + 30t = 6$.

Démonstration du lemme de Bézout. Clairement, il suffit de montrer le lemme pour le cas de x, y, z positifs, donc naturels. Démontrons cela par un raisonnent *par l'absurde* : supposons que cela est faux et en déduisons une absurdité.

Supposons qu'il existe deux nombres entiers positifs x et y tels que leur PGCD positif ne peut pas être écrit comme $xs + yt$ avec s et t entiers. Dans ce cas, il existe un couple de nombres entiers positifs avec cette propriété dont la somme est la plus petite parmi les sommes de tous les couples de nombres entiers positifs avec cette propriété.

Soient donc x et y deux nombres entiers positifs tels que leur PGCD positif ne peut pas être écrit comme $xs+yt$ avec s et t entiers, et qu'en plus la somme $x+y$ est inférieure ou égale à toute somme $u+v$ de nombres entiers positifs u et v dont le PGCD positif ne peut pas être écrit comme $us+vt$ avec s et t entiers. Sans perte de généralité, supposons en plus que $x \geqslant y$. (Sinon on peut échanger les rôles de x et y).

Dans ce cas, $y > 0$, car $\operatorname{pgcd}(x, 0) = x = x \cdot 1 + 0 \cdot 0$. D'où, $(x - y) + y = x < x + y$, et donc $\operatorname{pgcd}(x - y,\ y)$ peut être écrit comme $(x - y)s + yt$ avec s et t entiers (d'après le choix de x et y). Soient donc s et t deux entiers tels que

$$\operatorname{pgcd}(x - y,\ y) = (x - y)s + yt.$$

[4] Si on voulait suivre de près la terminologie de l'algèbre moderne, on devrait appeler ces nombres *irréductibles*, plutôt que premiers, et on devrait appeler *premiers* les nombres p différents de 0 et de ± 1 tels que pour tout produit $a \times b$ qui est divisible par p, a ou b est divisible par p. Cependant, d'après le *lemme d'Euclide*, une telle définition moderne des nombres premiers serait en fait équivalente à la définition donnée ici. Autrement dit, lorsqu'il s'agit des nombres entiers, on peut montrer qu'il n'y a pas de différence entre les éléments irréductibles et les éléments premiers au sens de l'algèbre moderne.

Or, $\operatorname{pgcd}(x, y) = \operatorname{pgcd}(x - y,\ y)$. Donc,

$$\operatorname{pgcd}(x, y) = (x - y)s + yt = xs + y(t - s).$$

Cela contredit le choix de x et y. □

Utilisons le lemme de Bézout pour en déduire quelques faits utiles.

Lemme. *Si x et y sont deux entiers premiers entre eux, et que z est un multiple commun de x et y, alors xy divise z.*

Démonstration. Soient u et v deux entiers tels que $xu = yv = z$. Soient s et t deux entiers tels que $xs + yt = 1$ (ils existent d'après le lemme de Bézout). Alors

$$z = (xs + yt)z = xsz + ytz = xsyv + ytxu = xy(sv + tu).$$ □

Corollaire. *Si x et y sont deux entiers premiers entre eux, alors xy est un PPCM de x et y.*

Lemme. *Si x et y sont deux entiers, z est un PGCD de x et y, et que w est un multiple commun de x et y, alors xy divise zw.*

Démonstration. Soient u et v deux entiers tels que $xu = yv = w$. Soient s et t deux entiers tels que $xs + yt = z$ (ils existent d'après le lemme de Bézout). Alors

$$zw = (xs + yt)w = xsw + ytw = xsyv + ytxu = xy(sv + tu).$$ □

Corollaire. *Si x et y sont deux entiers, alors*

$$\operatorname{ppcm}(x, y) \operatorname{pgcd}(x, y) = |xy|.$$

Démonstration. Sans perte de généralité, supposons que x et y sont positifs.

Soient u et v deux entiers tels que

$$x = \operatorname{pgcd}(x, y)u \quad \text{et} \quad y = \operatorname{pgcd}(x, y)v.$$

Alors $u \operatorname{pgcd}(x, y)v$ est un multiple commun de x et y. D'où, $\operatorname{ppcm}(x, y) \mid u \operatorname{pgcd}(x, y)v$, et donc

$$\operatorname{ppcm}(x, y) \operatorname{pgcd}(x, y) \mid u \operatorname{pgcd}(x, y)v \operatorname{pgcd}(x, y) = xy.$$

D'après le lemme précédent,

$$xy \mid \operatorname{ppcm}(x, y) \operatorname{pgcd}(x, y).$$

Comme xy et $\operatorname{ppcm}(x, y) \operatorname{pgcd}(x, y)$ sont deux entiers positifs dont chacun divise l'autre, c'est le même. □

Lemme (Lemme d'Euclide généralisé)**.** *Si x et y sont deux entiers et z est un diviseur de xy qui est premier avec x, alors z divise y.*

Démonstration. Soient s et t deux entiers tels que $zs + xt = 1$ (ils existent d'après le lemme de Bézout). Soit w un entier tel que $xy = zw$. Alors

$$y = (zs + xt)y = zsy + xyt = zsy + zwt = z(sy + wt),$$

et donc z divise y. □

II.17. Théorème fondamental de l'arithmétique

À l'aide du *lemme de Bézout*, on peut prouver le *théorème fondamental de l'arithmétique* :

Théorème (Théorème fondamental de l'arithmétique)**.** *Tout nombre naturel composé peut être écrit comme un produit de nombres naturels premiers d'une unique façon, à l'ordre près des facteurs.*

Commençons par les deux lemmes suivants.

Lemme (Lemme d'Euclide)**.** *Si x et y sont deux entiers et p est un diviseur premier de xy, alors p divise x ou p divise y.*

Démonstration. Supposons que p ne divise pas x. Alors p est premier avec x. Soient s et t deux entiers tels que $ps + xt = 1$ (ils existent d'après le lemme de Bézout). Soit q un entier tel que $xy = pq$. Alors

$$y = (ps + xt)y = psy + xyt = psy + pqt = p(sy + qt),$$

et donc p divise y. □

Remarque. Le lemme d'Euclide est un cas particulier du lemme d'Euclide généralisé.

Lemme. *Si $p, q_1, \ldots, q_n$ sont des nombres naturels premiers tels que p divise le produit $q_1 \cdots q_n$, alors il existe un indice i (entre 1 et n) tel que $p = q_i$.*

Démonstration. Posons

$$a_0 = 1, \quad a_1 = q_1, \quad a_2 = q_1q_2, \quad a_3 = q_1q_2q_3, \quad \ldots, \quad a_n = q_1 \cdots q_n.$$

Comme p ne divise pas a_0 mais divise a_n, il existe k entre 1 et n tel que p ne divise pas a_{k-1} mais divise a_k.

Soit k un indice entre 1 et n tel que p ne divise pas a_{k-1} mais divise $a_k = a_{k-1}q_k$. Alors, d'après le lemme précédent, p divise q_k, et donc $p = q_k$. □

Démonstration du théorème fondamental de l'arithmétique. Démontrons ce théorème par un raisonnent *par l'absurde* : supposons qu'il existe un nombre naturel composé qui peut être écrit comme un produit de nombres naturels premiers de deux façons essentiellement différentes, et en déduisons une absurdité.

Supposons qu'il existe un nombre naturel composé qui admet deux écritures comme un produit de nombres naturels premiers de manière qu'un certain nombre premier apparaît comme facteur dans les deux écritures un nombre différent des fois (par exemple, une fois dans une des écritures et deux fois dans l'autre, ou une fois dans une des écritures et pas du tout dans l'autre). Alors, en considérant deux telles écritures et en « supprimant » les facteurs communs dans les deux, on peut trouver un nombre naturel qui admet deux écritures comme un produit de nombres naturels premiers de manière qu'aucun nombre premier n'apparaît comme facteur dans les deux écritures à la fois. Or, cela contredit le lemme précédent. □

Le théorème fondamental de l'arithmétique peut être démontré un peu plus aisément en utilisant la notation suivante :

Notation. Si p est un entier premier et que a est un entier non nul, on va noter « $\nu_p a$ » le plus grand nombre naturel n tel que p^n divise a.

Exemples. $\nu_2 12 = 2$, $\nu_3 12 = 1$, $\nu_5 12 = 0$.

Exercice. Calculer $\nu_3 666$.

Définition. Pour un nombre entier premier p et pour un nombre entier non nul a, le nombre $\nu_p a$ est dit la *valuation p-adique* de a.

Exemple. La valuation triadique (3-adique) de 45 est 2.

Observons que si p et q sont deux nombres entiers premiers, alors

$$\nu_p q = \begin{cases} 1 & \text{si } q = p \text{ ou } q = -p, \\ 0 & \text{sinon.} \end{cases}$$

Proposition. *Si p est un entier premier et a et b sont deux entiers non nuls, alors*

$$\nu_p(ab) = \nu_p a + \nu_p b.$$

Démonstration. Posons $m = \nu_p a$ et $n = \nu_p b$. Soient c et d les entiers tels que $a = p^m c$ et $b = p^n d$. Alors p ne divise ni c, ni d. Donc, d'après le lemme d'Euclide, p ne divise pas cd. Or, $ab = p^{m+n} cd$. D'où, $\nu_p(ab) = m + n = \nu_p a + \nu_p b$. □

Ainsi, si $a_1, \ldots, a_m$ et $b_1, \ldots, b_n$ sont des nombres entiers non nuls tels que

$$a_1 \cdots a_m = b_1 \cdots b_n,$$

alors, pour tout nombre premier p,

$$\nu_p a_1 + \cdots + \nu_p a_m = \nu_p b_1 + \cdots + \nu_p b_n.$$

En particulier, si $a_1, \ldots, a_m$ et $b_1, \ldots, b_n$ sont des nombres naturels premiers tels que

$$a_1 \cdots a_m = b_1 \cdots b_n,$$

alors tout nombre premier apparaît comme facteur dans le premier membre de cette égalité (dans sa parti gauche) autant de fois qu'il apparaît dans son second membre (dans sa partie droite). D'où, $m = n$, et l'expression « $a_1 \cdots a_m$ » ne diffère de l'expression « $b_1 \cdots b_n$ » que par l'ordre des facteurs.

II.18. Congruences

Définition. Soient x, y, z trois entiers. On dit que x est *congru* à y suivant le *module* z, ou *modulo* z, si et seulement si il existe un entier w tel que

$$x = y + zw.$$

Autrement dit, deux entiers x et y sont congrus modulo un entier z si et seulement si z divise $x - y$.

Exercice. (1) Trouver tous les entiers congrus à 5 modulo 0.

(2) Trouver tous les entiers congrus à 5 modulo 1.

(3) Trouver tous les entiers congrus à 5 modulo -1.

Notation. On va écrire « $x \underset{z}{\equiv} y$ » pour dire « x est congru à y modulo z ».

Ainsi, pour tout entier m, on a défini la relation $(\underset{m}{\equiv})$ entre entiers, qui est dite la *relation de congruence modulo* m.

Lorsque la valeur du module m sera précisée dans le contexte, on pourra écrire « $x \equiv y$ » tout court au lieu de « $x \underset{m}{\equiv} y$ », par exemple :

$$2 \equiv 8 \pmod{3}.$$

En écriture mathématique contemporaine, il est courant d'abréger « modulo » comme « mod », sans point. Par exemple :

$$2 \equiv 8 \pmod 3.$$

Note étymologique. Le mot « module » vient du latin « *modulus* », qui est la forme diminutive de « *modus* » (qui peut se traduire comme « mesure », « rythme », « borne », « limite », « mode »). Voici le tableau de déclinaison de « *modulus* » en latin :

	Singulier	Pluriel
Nominatif	modulus	modulī
Vocatif	module	modulī
Accusatif	modulum	modulōs
Génitif	modulī	modulōrum
Datif	modulō	modulīs
Ablatif	modulō	modulīs

Proposition. *Les propriétés suivantes sont satisfaites pour tous entiers m, x, y, z :*

(1) *si* $x \underset{m}{\equiv} y \underset{m}{\equiv} z$, *alors* $x \underset{m}{\equiv} z$,

(2) $x \underset{m}{\equiv} x$,

(3) *si* $x \underset{m}{\equiv} y$, *alors* $y \underset{m}{\equiv} x$.

Exercice. Prouver cette proposition.

Proposition. *Soient m, x_1, x_2, y_1, y_2 des entiers tels que $x_1 \underset{m}{\equiv} x_2$ et $y_1 \underset{m}{\equiv} y_2$. Alors :*

(1) $x_1 + y_1 \underset{m}{\equiv} x_2 + y_2$, (2) $x_1 - y_1 \underset{m}{\equiv} x_2 - y_2$, (3) $x_1 y_1 \underset{m}{\equiv} x_2 y_2$.

Exercice. Prouver cette proposition.

Lemme. *Si x et y sont deux entiers et que r est le reste d'une division euclidienne de x par y, alors $x \underset{y}{\equiv} r$.*

Exercice. Prouver ce lemme.

Lemme. *Si m, x, y sont des entiers tels que $0 < |x - y| < |m|$, alors $x \underset{m}{\not\equiv} y$.*

Exercice. Prouver ce lemme.

Exercice. Est-ce que le nombre $1^2 + 2^2 + 3^2 + \cdots + 100^2$ est pair ou impair ?

Exercice. Soit $x = 333^{333}$.

(1) Trouver le dernier chiffre de l'écriture binaire de x.

(2) Trouver le dernier chiffre de l'écriture décimale de x.

(3) Trouver le reste de la division euclidienne de x par 7.

Exercice. Soit (Δ) une relation entre des entiers telle que :

(1) si $x \mathrel{\Delta} y \mathrel{\Delta} z$, alors $x \mathrel{\Delta} z$,

(2) $x \mathrel{\Delta} x$,

(3) si $x \mathrel{\Delta} y$, alors $y \mathrel{\Delta} x$,

(4) si $x_1 \mathrel{\Delta} x_2$ et $y_1 \mathrel{\Delta} y_2$, alors $x_1 + y_1 \mathrel{\Delta} x_2 + y_2$, $x_1 - y_1 \mathrel{\Delta} x_2 - y_2$, et $x_1 y_1 \mathrel{\Delta} x_2 y_2$.

Montrer qu'il existe un nombre entier m tel que la relation (Δ) est la congruence modulo m. (Autrement dit : montrer qu'il existe $m \in \mathbf{Z}$ tel que $(\underset{m}{\equiv}) = (\Delta)$.)

Définition. Une *congruence* sur les entiers[5] est une relation (Δ) entre des entiers telle que :

(1) si $x \mathrel{\Delta} y \mathrel{\Delta} z$, alors $x \mathrel{\Delta} z$,

(2) $x \mathrel{\Delta} x$,

(3) si $x \mathrel{\Delta} y$, alors $y \mathrel{\Delta} x$,

(4) si $x_1 \mathrel{\Delta} x_2$ et $y_1 \mathrel{\Delta} y_2$, alors $x_1 + y_1 \mathrel{\Delta} x_2 + y_2$, $x_1 - y_1 \mathrel{\Delta} x_2 - y_2$, et $x_1 y_1 \mathrel{\Delta} x_2 y_2$.

[5] La notion de *congruence* sur les entiers est un cas spécial d'une notion générale de *congruence* sur une *structure algébrique*.

II.19. Classes de congruence, arithmétique modulaire

Définition. Soit m un entier. Définissons les *classes de congruence* d'entiers modulo m ainsi :

(1) à tout entier x, on associe sa *classe de congruence* modulo m, notée « $[x]_m$ »[6] ;

(2) si x et y sont deux entiers, on admet que les *classes de congruence* de x et de y modulo m coïncident si et seulement si x est congru à y modulo m :

$$[x]_m = [y]_m \quad \Leftrightarrow \quad x \underset{m}{\equiv} y.$$

Remarque. Souvent on donne une définition différente des classes de congruence, en les *réalisant* comme des *ensembles* : on dit que la *classe de congruence* de x modulo m est l'ensemble de tous les entiers congrus à x modulo m. En pratique, en tant que l'*arithmétique modulaire* est concernée, cette définition équivaut la nôtre.

Notation. Lorsque la valeur du module m sera précisée dans le contexte, on pourra écrire « $[x]$ » au lieu de « $[x]_m$ ».

Définition. Soit m un entier. Soient α et β deux classes de congruence d'entiers modulo m. On définit la *somme* $\alpha + \beta$, la *difference* $\alpha - \beta$ et le *produit* $\alpha\beta$ ainsi : si x et y sont deux entiers tels que $\alpha = [x]_m$ et $\beta = [y]_m$, alors

(1) $\alpha + \beta = [x]_m + [y]_m \overset{\text{déf}}{=} [x+y]_m$,

(2) $\alpha - \beta = [x]_m - [y]_m \overset{\text{déf}}{=} [x-y]_m$,

(3) $\alpha\beta = [x]_m[y]_m \overset{\text{déf}}{=} [xy]_m$.

Exercice. Montrer que pour tout m entier, les définitions données de l'*addition*, de la *soustraction* et de la *multiplication* des classes de congruence d'entiers modulo m sont correctes et complètes.

Remarque. Il existe une pratique d'écrire « x » tout court à la place de « $[x]_m$ » ou « $[x]$ » lorsque le contexte permet de comprendre qu'il s'agit d'une classe de congruence d'entiers modulo m, plutôt que d'un entier (malgré l'apparence). Ainsi, on peut rencontrer des formules comme celle-là :

$$\text{« } -2 = 5 \cdot 8 \mod 3 \text{ ».}$$

Cette formule doit alors être lue comme

$$\text{« } [0]_3 - [2]_3 = [5]_3 \cdot [8]_3 \text{ »,}$$

ou comme « $[0]_3 - [2]_3 = [2]_3 \cdot [2]_3$ », (en simplifiant l'écriture des classes de congruence de 5 et de 8). Selon cette interprétation, dans la formule « $-2 = 5 \cdot 8 \mod 3$ », le numeral « 3 » représente l'entier 3, les numéraux « 2 », « 5 », et « 8 » représentent des classes de congruence d'entiers modulo 3, et les symboles « $-$ » et « $\cdot$ » représentent les opérations de soustraction et de multiplication des classes de congruence d'entiers modulo 3.

[6] La notation « $\bar{x}_m$ » au lieu de « $[x]_m$ » peut aussi être rencontrée.

Proposition. *Soit m un entier et soient α, β, γ des classes de congruence d'entiers modulo m. Alors les identités suivantes sont satisfaites* :

(1) $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$,

(2) $\alpha + [0]_m = \alpha = [0]_m + \alpha$,

(3) $\beta + \alpha = \alpha + \beta$,

(4) $(\alpha - \beta) + \beta = \alpha$,

(5) $\alpha(\beta\gamma) = (\alpha\beta)\gamma$,

(6) $\alpha[1]_m = \alpha = [1]_m\alpha$,

(7) $\beta\alpha = \alpha\beta$,

(8) $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$.

Exercice. Prouver cette proposition.

Exercice. Soit A l'ensemble des quatre classes de congruence modulo 4 suivantes : $[0]_4, [1]_4, [2]_4, [3]_4$.

(1) Montrer que A contient exactement 4 éléments, c'est-à-dire, que les 4 classes $[0]_4, [1]_4, [2]_4, [3]_4$ sont deux à deux distincts.

(2) Montrer que A contient toutes les classes de congruence d'entiers modulo 4.

(3) Montrer que la somme, la différence, et le produit de deux n'importe quels éléments de A est un élément de A.

(4) Dresser les tables d'addition, de soustraction et de multiplication des éléments de A.

Exercice. Est-il vrai que si α et β sont deux classes de congruence d'entiers modulo un entier m telles que $\alpha \neq [0]_m$ et $\beta \neq [0]_m$, alors $\alpha\beta \neq [0]_m$?

III. Nombres rationnels

III.1. Qu'est-ce que c'est, un nombre rationnel ?

Rappelons nous que l'opération de division de nombres entiers peut être appliquée à deux nombres entiers a et b à la condition que b n'est pas nul et que b divise a, et que dans ce cas le résultat de cette opération est le *quotient* de a par b, noté « a/b » ou « $\frac{a}{b}$ ». La valeur du quotient « a/b » n'est définie comme un nombre entier que si b divise a.

Exercice. Essayer de compléter les tableaux suivants :

5	15	9	18	18	9	4	10	1	0	0	1
3	9	12	24	24	12	10	25	5	0	0	5
21	?	?	10	?	10	6	?	100	?	?	100

Le quotient de deux nombres exprime un certain rapport entre ces nombres, qu'on pourrait appeler leur « rapport multiplicatif ». Par exemple, le « rapport multiplicatif » entre 15 et 5 est le même qu'entre 9 et 3, et le même qu'entre 63 et 21, mais différent de celui entre 18 et 9. En effet :

$$\frac{15}{5} = \frac{9}{3} = \frac{63}{21} = 3 \neq 2 = \frac{18}{9}.$$

Cependant, il paraît clair que le « rapport multiplicatif » entre 5 et 15 doit être le même qu'entre 3 et 9. Or, aucun nombre entier n'exprime, dans le sens précédent, le « rapport multiplicatif » entre 5 et 15, ni entre 3 et 9, car les valeurs des quotients « $5/15$ » et « $3/9$ » ne sont pas définies comme nombres entiers.

Notons $(\underset{\times}{\simeq})$ la relation entre couples de nombres entiers dont le sens sera le suivant :

> « $(a, b) \underset{\times}{\simeq} (c, d)$ » veut dire que le « rapport multiplicatif » entre b et a est le même qu'entre d et c.

Essayons de donner une définition précise de la relation $(\underset{\times}{\simeq})$ en accord avec l'idée intuitive du « rapport multiplicatif ». On souhaite, en particulier, que

$$(5, 15) \underset{\times}{\simeq} (3, 9) \underset{\times}{\simeq} (21, 63) \underset{\times}{\not\simeq} (9, 18),$$

mais aussi que

$$(15, 5) \underset{\times}{\simeq} (9, 3) \underset{\times}{\simeq} (63, 21) \underset{\times}{\not\simeq} (5, 15),$$

ainsi que

$$(1,0) \underset{\times}{\simeq} (5,0) \quad \text{et} \quad (0,1) \underset{\times}{\simeq} (0,5).$$

Dans le cas où $0 \neq a \mid b$ et $0 \neq c \mid d$, on souhaite que l'équivalence suivante soit satisfaite :

$$(a,b) \underset{\times}{\simeq} (c,d) \quad \Leftrightarrow \quad \frac{b}{a} = \frac{d}{c}.$$

Cependant, l'équation « $b/a = d/c$ » ne peut servir comme la définition du sens de « $(a,b) \underset{\times}{\simeq} (c,d)$ » que si $0 \neq a \mid b$ et $0 \neq c \mid d$, car sinon, les valeurs des quotients « b/a » et « d/c » ne sont pas toutes les deux définies (comme nombres entiers). Le problème est dans l'opération de division.

Comment peut-on vérifier si $b/a = d/c$ sans utiliser l'opération de division ? Une solution est évidente : il suffit de vérifier si $bc = da$, car

$$\frac{b}{a} = \frac{d}{c} \quad \Leftrightarrow \quad bc = da$$

dans le cas où $0 \neq a \mid b$ et $0 \neq c \mid d$.

Les valeurs des deux membres de l'équation « $bc = da$ » (de ses parties gauche et droite) sont définies pour tous nombres entiers a, b, c, d. On va utiliser cette équation pour définir la relation $(\underset{\times}{\simeq})$, qui est censée traduire l'idée intuitive du « rapport multiplicatif ».

Notons cependant que le couple $(0,0)$ est « spécial » : il est difficile de voir ce que pourrait être le « rapport multiplicatif » entre 0 et 0, cette notion ne semble pas avoir du sens. Pour cette raison, on ne va pas parler du « rapport multiplicatif » entre 0 et 0, et on va « exclure » le couple $(0,0)$ dans la définition suivante.

Définition. Définissons la relation $(\underset{\times}{\simeq})$ entre deux couples de nombres entiers (a,b) et (c,d) tels que $(a,b) \neq (0,0)$ et $(c,d) \neq (0,0)$ par l'équivalence suivante :

$$(a,b) \underset{\times}{\simeq} (c,d) \quad \Leftrightarrow \quad bc = da.$$

Notons que, d'après cette définition, si a, b, c, d sont des entiers non nuls, alors

$$\begin{aligned} (a,b) \underset{\times}{\simeq} (c,d) \quad &\Leftrightarrow \quad (b,a) \underset{\times}{\simeq} (d,c) \\ &\Leftrightarrow \quad (a,c) \underset{\times}{\simeq} (b,d) \quad \Leftrightarrow \quad (c,a) \underset{\times}{\simeq} (d,b). \end{aligned}$$

Exercice. Vérifier sur des exemples si la définition donnée ci-dessus de la relation $(\underset{\times}{\simeq})$ est en accord avec l'idée intuitive du « rapport multiplicatif ».

Exercice. Soient a, b, c, d quatre nombres entiers. Montrer que $(a,b) \underset{\times}{\simeq} (c,d)$ si et seulement si il existe deux nombres entiers e et f non nuls tels que $ea = fc$ et $eb = fd$.

Les trois propriétés suivantes de la relation $(\underset{\times}{\simeq})$ sont d'une importance particulière pour la définition des nombres rationnels : pour tous nombres entiers a, b, c, d, e, f tels que $(a,b) \neq (0,0)$, $(c,d) \neq (0,0)$ et $(e,f) \neq (0,0)$,

(1) si $(a,b) \underset{\times}{\simeq} (c,d)$ et $(c,d) \underset{\times}{\simeq} (e,f)$, alors $(a,b) \underset{\times}{\simeq} (e,f)$,

(2) $(a,b) \underset{\times}{\simeq} (a,b)$,

(3) si $(a,b) \underset{\times}{\simeq} (c,d)$, alors $(c,d) \underset{\times}{\simeq} (a,b)$.

Exercice. Démontrer ces propriétés.

Prenons en plus note des deux lemmes suivants.

Lemme. *Si a, b, c sont trois nombres entiers tels que $(a,b) \neq (0,0)$ et $c \neq 0$, alors $(a,b) \underset{\times}{\simeq} (ac,\ bc)$.*

Lemme. (1) *Si a, b, c sont trois nombres entiers tels que $a \neq 0$ et $(a,b) \underset{\times}{\simeq} (a,c)$, alors $b = c$.*

(2) *Si a, b, c sont trois nombres entiers tels que $c \neq 0$ et $(a,c) \underset{\times}{\simeq} (b,c)$, alors $a = b$.*

Exercice. Prouver ces lemmes.

Ainsi on a défini le sens de la phrase « le rapport multiplicatif entre b et a est le même qu'entre d et c » : cela veut dire que $bc = da$ (à la condition que $(a,b) \neq (0,0)$ et $(c,d) \neq (0,0)$). En plus, si $a \mid b$ et $c \mid d$, les « rapports multiplicatifs » entre b et a et entre d et c sont exprimés par les nombres entiers b/a et d/c, et pour voir si les deux « rapports multiplicatifs » sont les mêmes, il suffit de voir si $b/a = d/c$. Mais, comme déjà mentionné, aucun nombre entier n'exprime, dans ce sens, le « rapport multiplicatif » entre 5 et 15, ni entre 3 et 2, car les valeurs des quotients « $5/15$ » et « $3/2$ » ne sont pas définies comme nombres entiers.

Une issue de cette situation est d'inventer de nouveaux nombres pour exprimer les quotients « manquantes » de nombres entiers.

Définition. Définissons les nombres *rationnels* ainsi :

(1) tout nombre entier est *rationnel* ;

(2) si a et b sont deux entiers tels que $a \neq 0$, mais que la valeur du quotient « b/a » n'est pas définie comme un entier (car $a \nmid b$), on admet que le quotient b/a est un nombre *rationnel* ;

(3) si a, b, c, d sont quatre entiers tels que $a \neq 0$ et $c \neq 0$, on admet que le nombre *rationnel* d/c est le même que le nombre *rationnel* b/a si et seulement si $(c,d) \underset{\times}{\simeq} (a,b)$:

$$\frac{d}{c} = \frac{b}{a} \quad \Leftrightarrow \quad (c,d) \underset{\times}{\simeq} (a,b) \quad \Leftrightarrow \quad bc = da \ ;$$

(4) tout nombre *rationnel* est le quotient d'un entier par un entier non nul ;

(5) il n'existe toujours pas de quotient d'un entier par 0.

Notation. L'ensemble des nombres rationnels sera noté « $\mathbf{Q}$ ».

Remarque. On pourrait introduire un « nombre » pour exprimer le « rapport multiplicatif » entre un rationnel non nul et 0 (d'après notre définition, si x et y sont deux rationnels non nuls, alors $(0, x) \underset{\times}{\doteq} (0, y)$). Cependant, ce « nombre » aurait des propriétés assez particulières, souvent on devrait le traiter séparément, et il serait peu utile dans l'étude de l'arithmétique.[1] Si on note ce nombre « ∞ » et tente de prolonger les définitions des opérations usuelles pour pouvoir les appliquer à ∞, on pourra finir avec les propriétés suivantes :

(1) $x/0 = x \cdot \infty = \infty \cdot x = \infty$ pour tout $x \neq 0$. En particulier, $\infty/0 = \infty \cdot \infty = \infty$.

(2) Les valeurs de « $\infty \cdot 0$ » et de « $0 \cdot \infty$ » ne sont pas définies.

(3) $x/\infty = 0$ et $\infty/x = \infty$ pour tout $x \neq \infty$.

(4) La valeur de « ∞/∞ » n'est pas définie.

(5) $x + \infty = \infty + x = x - \infty = \infty - x = \infty$ pour tout $x \neq \infty$. En particulier, $-\infty = 0 - \infty = \infty$.

(6) Les valeurs de « $\infty + \infty$ » et de « $\infty - \infty$ » ne sont pas définies ; en particulier, « $\infty + \infty$ » ne veut pas dire la même chose que « $\infty \cdot 2$ », et « $\infty - \infty$ » ne fait pas 0.

On va se passer d'un tel « nombre » bizarre. Donc, la valeur de « $x/0$ » ne sera pas définie.

Notons que tout nombre rationnel peut être écrit comme le quotient de deux nombres entiers. En plus, tout nombre rationnel non nul peut être écrit comme le quotient de deux entiers premiers entre eux.

Proposition. *Pour tout nombre rationnel x, il existe un unique couple de nombres entiers a, b tel que* :

(1) $b/a = x$,

(2) *a et b sont premiers entre eux*,

(3) $a > 0$.

Démonstration. Montrons d'abord l'existence. Soient a et b deux nombres entiers tels que $x = b/a$. (En particulier, $a \neq 0$.) Soit d un PGCD entier de a et b. Soient u et v deux entiers tels que $a = du$ et $b = dv$. Alors :

[1] En *analyse complexe*, on utilise un tel « nombre » ∞ pour compléter le *plan complexe* en la *sphère complexe*. Cependant, il ne faut pas confondre ∞ de l'analyse complexe avec ce qu'on note « ∞ » en analyse réel, où les propriétés de ∞ sont différentes, et, en particulier, $-\infty$ n'est pas la même chose que ∞.

(1) $x = v/u$ et $x = (-v)/(-u)$,

(2) u est premier avec v et $-u$ est premier avec $-v$,

(3) soit $u > 0$, soit $-u > 0$.

Ainsi l'existence est établie.

Montrons maintenant l'unicité. Supposons que a, b, c, d sont des entiers tels que :

(1) $x = b/a$ et $x = d/c$,

(2) a est premier avec b et c est premier avec d,

(3) $a > 0$ et $c > 0$.

Montrons que dans ce cas $a = c$ et $b = d$.

Comme $b/a = d/c$, on a que $bc = da$. Vu que $bc = da$ et que a et b sont premiers entres eux, a divise c (et aussi b divise d) d'après le lemme d'Euclide généralisé. Par ce même raisonnement, comme c et d sont premiers entres eux, c divise a (et aussi d divise b). Comme a et c divisent l'un l'autre et sont tous les deux strictement positifs, ils sont égaux ($a = c$). D'où, $ba = da$, et donc $b = d$ (car $a \neq 0$).

Donc, l'unicité est démontrée aussi. □

Définition. Une *fraction* est une expression de la forme « b/a » (ou « $\frac{b}{a}$ », ou « $b \div a$ »), qui représente le résultat de la division (le quotient) de la valeur de « b » par la valeur de « a ». Le *numérateur* de la fraction « b/a » est « b », et le *dénominateur* de « b/a » est « a ». On peut aussi appeler *numérateur* et *dénominateur* de « b/a » les valeurs de « b » et de « a ».

Définition. Une fraction dont le numérateur et le dénominateur sont entiers est dite :

(1) *irréductible* si et seulement si son numérateur et son dénominateur sont premiers entre eux,

(2) *réductible* si et seulement si son numérateur et son dénominateur ont un diviseur commun différent de ± 1.

Exemples. Les fractions « $3/1$ », « $1/3$ », « $3/10$ », « $10/3$ » sont irréductibles. Les fractions « $3/6$ », « $6/3$ », « $4/10$ », « $10/4$ » sont réductibles.

III.2. Relations d'ordre usuelles

Définition. Définissons les relations ($\leqslant$), ($\geqslant$), ($<$), ($>$) entre des rationnels par les équivalences suivantes, où a est un entier *strictement positif* ($a > 0$), alors que b et c sont deux nombres entiers arbitraires :

$$\frac{b}{a} \leqslant \frac{c}{a} \quad \Leftrightarrow \quad b \leqslant c, \qquad \frac{b}{a} \geqslant \frac{c}{a} \quad \Leftrightarrow \quad b \geqslant c,$$

$$\frac{b}{a} < \frac{c}{a} \quad \Leftrightarrow \quad b < c, \qquad \frac{b}{a} > \frac{c}{a} \quad \Leftrightarrow \quad b > c.$$

Il reste à vérifier que ces définitions sont toutes correctes et complètes.

Proposition. *La définition donnée ci-dessus de la relation* $(\leqslant)$ *est correcte. C'est-à-dire, quels que soient six nombres entiers* a_1, a_2, b_1, b_2, c_1, c_2, *tels que* $a_1 > 0$ *et* $a_2 > 0$, *si* $b_1/a_1 = b_2/a_2$ *et* $c_1/a_1 = c_2/a_2$, *alors*

$$b_1 \leqslant c_1 \quad \Leftrightarrow \quad b_2 \leqslant c_2.$$

Démonstration. Soient a_1, a_2, b_1, b_2, c_1, c_2 six nombres entiers tels que $a_1 > 0$, $a_2 > 0$, $b_1/a_1 = b_2/a_2$ et $c_1/a_1 = c_2/a_2$. Alors,

$$(a_1, b_1) \underset{\times}{\simeq} (a_2, b_2) \quad \text{et} \quad (a_1, c_1) \underset{\times}{\simeq} (a_2, c_2)$$

(voir la définition des *nombres rationnels*), c'est-à-dire, $b_1 a_2 = b_2 a_1$ et $c_1 a_2 = c_2 a_1$.

D'après les propriétés des nombres entiers déjà établies,

$$b_1 \leqslant c_1 \quad \Leftrightarrow \quad b_1 a_2 \leqslant c_1 a_2 \quad \Leftrightarrow \quad b_2 a_1 \leqslant c_2 a_1 \quad \Leftrightarrow \quad b_2 \leqslant c_2. \qquad \square$$

Exercice. Vérifier si les définitions des relations $(\geqslant)$, $(<)$, $(>)$ sont correctes elles aussi.

Proposition. *Les définitions données ci-dessus des relations* $(\leqslant)$, $(\geqslant)$, $(<)$, $(>)$ *sont toutes complètes. C'est-à-dire, quels que soient deux nombres rationnels* x *et* y, *il existe trois nombres entiers* a, b, c *tels que* $a > 0$, $x = b/a$ *et* $y = c/a$.

Démonstration. Soient x et y deux nombres rationnels arbitraires. Soient a, b, c, d nombres entiers tels que $x = a/b$ et $y = c/d$. Alors

$$x = \frac{ad}{bd} \quad \text{et} \quad y = \frac{cb}{db} = \frac{cb}{bd}. \qquad \square$$

Les relations $(\leqslant)$, $(\geqslant)$, $(<)$, $(>)$ sont reliées par les équivalences suivantes :

(1) $x \leqslant y$ si et seulement si $y \geqslant x$,

(2) $x < y$ si et seulement si $y > x$,

(3) $x \leqslant y$ si et seulement si $x < y$ ou $x = y$,

(4) $x < y$ si et seulement si $x \leqslant y$ et $x \neq y$.

Exercice. Vérifier ces équivalences.

Les quatre propriétés suivantes de la relation $(\leqslant)$ entre des nombres rationnels sont les mêmes que pour la relation $(\leqslant)$ entre des nombres entiers :

(1) si $x \leqslant y$ et $y \leqslant z$, alors $x \leqslant z$,

(2) $x \leqslant x$,

(3) si $x \leqslant y$ et $y \leqslant x$, alors $x = y$,

(4) $x \leqslant y$ ou $y \leqslant x$.

Exercice. Démontrer ces propriétés.

Les trois propriétés suivantes de la relation $(<)$ entre des nombres rationnels sont les mêmes que pour la relation $(<)$ entre des nombres entiers :

(1) si $x < y$ et $y < z$, alors $x < z$,

(2) si $x < y$, alors $x \neq y$,

(3) si $x \neq y$, alors $x < y$ ou $y < x$.

Exercice. Démontrer ces propriétés.

Exercice. Écrire les nombres rationnels suivants sous la forme simplifiée en les rangeant dans l'ordre croissant : $\frac{4}{7}, \frac{-2}{5}, \frac{1}{-3}, \frac{-4}{-6}$.

Notation. Si x et y sont deux rationnels, on va noter « $\max(x, y)$ » le plus grand entre x et y et « $\min(x, y)$ » le plus petit entre x et y :

$$\max(x,y) \overset{\text{déf}}{=} \begin{cases} x & \text{si} \quad x \geqslant y, \\ y & \text{si} \quad x \leqslant y; \end{cases} \qquad \min(x,y) \overset{\text{déf}}{=} \begin{cases} x & \text{si} \quad x \leqslant y, \\ y & \text{si} \quad x \geqslant y. \end{cases}$$

Rationnels positifs et négatifs

Définition. Un nombre rationnel x est dit :

(1) *positif* (au sens large) si et seulement si $x \geqslant 0$,

(2) *négatif* (au sens large) si et seulement si $x \leqslant 0$,

(3) *strictement positif* si et seulement si $x > 0$,

(4) *strictement négatif* si et seulement si $x < 0$.

III.3. « Translation multiplicative » d'un entier par un nombre rationnel

Définition. Si a est un entier non nul, b est un entier, et $x = b/a$, alors le *produit* de a et du nombre rationnel x, noté « ax », est b :

$$a(b/a) \overset{\text{déf}}{=} b.$$

Cette définition est clairement en accord avec la définition de la multiplication des nombres entiers, car si a, b et b/a sont tous nombres entiers ($a \neq 0$), alors le produit de a et b/a est b, au sens de la multiplication des nombres entiers. Ainsi, cette définition, pourvu qu'elle soit correcte, *prolonge* l'opération de multiplication des nombres entiers.

Il est facile de montrer que cette définition est correcte, c'est-à-dire, que si a est un nombre entier non nul et x est un nombre rationnel tels que la définition s'applique pour donner une valeur de « ax », alors elle ne donnera qu'une valeur unique. En effet : si b_1 et b_2 sont deux nombres entiers tels que $x = b_1/a = b_2/a$, alors $b_1 = b_2$, d'après un lemme précédent.

Exemple. $6(2/3) = 6(4/6) = 4$.

Exercice. Calculer et simplifier : $6(3/2)$.

Cependant, la valeur de « $3(1/2)$ » n'est pas encore définie.

Soit x un nombre rationnel. Si a et b sont deux entiers tels que $x = b/a$, alors on va, de manière informelle, appeler $b = ax$ le *« translaté multiplicatif »* de a par x. On peut parler de l'opération de *« translation multiplicative »* par x, qui a certains entiers associe leurs translatés multiplicatifs par x.

III.4. Addition et soustraction

D'après la définition de la « translation multiplicative », quels que soient trois nombres entiers a, b, c, avec $a \neq 0$, on a :

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

Cette observation suggère qu'il est naturel de définir l'opération d'*addition* $(+)$ des nombres rationnels de telle manière que pour tous nombres entiers a, b, c, avec $a \neq 0$, on ait l'égalité :

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

Définition. Si a est un entier non nul, b et c sont deux entiers, $x = b/a$ et $y = c/a$, alors la *somme* des nombres rationnels x et y, notée « $x + y$ », est $(b + c)/a$:

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

Exercice. Montrer que cette définition est correcte et complète.

Ainsi on a défini l'opération d'*addition* $(+)$ qui à deux n'importe quels nombres rationnels associe leur somme.

Exemples.

$$\frac{1}{2} + \frac{3}{4} = \frac{2}{4} + \frac{3}{4} = \frac{5}{4}, \qquad \frac{3}{4} + \frac{5}{6} = \frac{9}{12} + \frac{10}{12} = \frac{19}{12}.$$

Exercice. Calculer et simplifier : $2/3 + 3/2$, $(-2)/3 + 3/2$, $(-2)/3 + 3/(-2)$.

En général, pour tous nombres entiers a, b, c, d, avec b et d non nuls,

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

Les trois identités suivantes satisfaites par l'opération d'addition de nombres rationnels sont les mêmes que pour l'opération d'addition de nombres entiers :

(1) $x + (y + z) = (x + y) + z$,

(2) $x + 0 = x = 0 + x$,

(3) $y + x = x + y$.

Exercice. Démontrer ces identités.

Lemme. *Soit x un nombre rationnel arbitraire. Soient a et b deux entiers tels que $x = b/a$. Posons $y = (-b)/a$. Alors $x + y = 0 = y + x$.*

Exercice. Prouver ce lemme.

Proposition. *Pour tous nombres rationnels x et y, il existe un unique nombre rationnel z tel que $z + y = x$.*

Exercice. Prouver cette proposition.

Définition. Deux nombres rationnels x et y sont dits *opposés* l'un de l'autre si et seulement si $x + y = 0$.

Définition. Si x et y sont deux nombres rationnels, alors l'unique nombre rationnel z tel que $z + x = y$ est dit la *différence* de y et x et est noté « $y - x$ ».

Ainsi on a défini l'opération de *soustraction* $(-)$ qui à deux n'importe quels nombres rationnels associe leur différence.

Exercice. Calculer et simplifier : $2/3 - 3/2$, $(-2)/3 - 3/2$, $(-2)/3 - 3/(-2)$.

La définition de l'opération de soustraction $(-)$ donnée ci-dessus peut être exprimée par l'équivalence suivante :

$$y - x = z \quad \Leftrightarrow \quad y = z + x.$$

L'opération de soustraction $(-)$ de nombres rationnels peut aussi être définie par les deux identités suivantes, à la condition que l'opération d'addition $(+)$ est déjà définie :

(1) $(x + y) - y = x$, (2) $(x - y) + y = x$.

En fait, n'importe quelle de ces deux identités suffit toute seule pour définir l'opération de soustraction de nombres rationnels.

Exercice. Montrer que n'importe quelle de ces deux identités suffit toute seule pour définir l'opération de soustraction de nombres rationnels.

Exercice. Soient a, b, c, d quatre nombres entiers, avec b et d non nuls. Montrer que

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

Les identités suivantes satisfaites pour tous x, y, z rationnels sont les même que pour les nombres entiers :

(1) $x + (y - z) = (x + y) - z$,
(2) $x - (y + z) = (x - z) - y$,
(3) $x - (y - z) = (x + z) - y$,
(4) $(x - y) + (y - z) = x - z$,
(5) $(x + z) - (y + z) = x - y$,
(6) $(x - y) + z = (x + z) - y$,
(7) $(x - y) - z = (x - z) - y$,
(8) $x - (x - y) = y$,
(9) $x - 0 = x$,
(10) $x - x = 0$.

Exercice. Démontrer ces identités.

Notation. L'expression « $+x$ » veut dire $0 + x = x$. L'expression « $-x$ » veut dire $0 - x$.

Rapport aux relations d'ordre usuelles

Proposition. *Pour tous nombres rationnels x, y, z, si $x < y$, alors $x + z < y + z$.*

Exercice. Prouver cette proposition.

Corollaire. *Pour tous nombres rationnels x, y, z, les équivalences suivantes sont satisfaites* :

$$x < y \quad \Leftrightarrow \quad x + z < y + z, \qquad\qquad x \leqslant y \quad \Leftrightarrow \quad x + z \leqslant y + z.$$

Proposition. *Pour tous nombres rationnels x, y, z, si $x < y$, alors $z - x > z - y$.*

Exercice. Prouver cette proposition.

Corollaire. *Pour tous nombres rationnels x, y, z, les équivalences suivantes sont satisfaites* :

$$x < y \quad \Leftrightarrow \quad z - x > z - y, \qquad\qquad x \leqslant y \quad \Leftrightarrow \quad z - x \geqslant z - y.$$

III.5. Multiplication et division

Définition. Si n est un nombre naturel et x est un nombre rationnel, alors le *produit* de x et n, noté « $x \times n$ », « $x \cdot n$ », ou « xn », est défini par la règle :

$$xn \overset{\text{déf}}{=} 0 \underbrace{+ x + x + \cdots + x}_{n \text{ fois}}.$$

Définition. Si m et n sont deux nombres naturels, x est un nombre rationnel, et $a = n - m$, alors le *produit* de x et a, noté « $x \times a$ », « $x \cdot a$ », ou « xa », est défini par la règle :

$$x(n - m) \overset{\text{déf}}{=} 0 \underbrace{+ x + x + \cdots + x}_{n \text{ fois}} \underbrace{- x - x - \cdots - x}_{m \text{ fois}} = xn - xm.$$

Lemme. *Si a est un entier non nul et b et c sont deux entiers, alors*

$$\frac{b}{a} \cdot c = \frac{bc}{a}.$$

Exercice. Prouver ce lemme.

Lemme. *Soient a et b deux entiers non nuls et c un entier. Alors*

$$\frac{c}{ab} \cdot a = \frac{c}{b}.$$

En plus, si x est un nombre rationnel tel que $xa = c/b$, alors $x = c/(ab)$.

Exercice. Prouver ce lemme.

Lemme. *Pour tout nombre rationnel x et pour tout entier a non nul, il existe un unique nombre rationnel y tel que $ya = x$.*

Exercice. Prouver ce lemme.

Définition. Si a est un entier non nul et x est un nombre rationnel, alors l'unique nombre rationnel y tel que $ya = x$ est dit le *quotient* de x par a et est noté « $x \div a$ », ou « $x : a$ », ou « x/a », ou « $a\backslash x$ », ou « $\dfrac{x}{a}$ ».

Définition. Si a est un entier non nul, b est un entier, x est un nombre rationnel, et $y = b/a$, alors le *produit* de x et y, noté « $x \times y$ », « $x \cdot y$ », ou « xy », est défini par la règle :

$$x \cdot \frac{b}{a} \overset{\text{déf}}{=} \frac{xb}{a} = \frac{x}{a} \cdot b.$$

Exercice. Vérifier si ces définitions sont toutes correctes.

Ainsi on a défini l'opération de *multiplication* $(\cdot)$ (aussi notée « $(\times)$ ») qui à deux n'importe quels nombres rationnels associe leur produit.

Exercice. Calculer et simplifier : $(1/2)(3/4)$, $((-1)/2)(3/4)$, $((-1)/2)/(3/(-4))$.

Remarque. Le produit de nombres rationnels *non nuls* pourrait être défini par la règle : si a, b, c sont des entiers non nuls, alors

$$\frac{b}{a} \cdot \frac{c}{b} = \frac{c}{a}.$$

Proposition. *Pour tous nombres rationnels x et y, $yx = xy$.*

Exercice. Prouver cette proposition.

Les identités suivantes sont satisfaites :

(1) $x(yz) = (xy)z$,

(2) $x \cdot 1 = x = 1 \cdot x$,

(3) $yx = xy$,

(4) $x(y + z) = xy + xz$,

(5) $x(y - z) = xy - xz$,

(6) $x \cdot 0 = 0$.

Exercice. Démontrer ces identités.

Lemme. *Soit x un nombre rationnel non nul. Soient a et b deux entiers tels que $x = b/a$. Posons $y = a/b$. Alors $xy = 1 = yx$.*

Exercice. Prouver ce lemme.

Proposition. *Pour tous nombres rationnels x et y avec $y \neq 0$, il existe un unique nombre rationnel z tel que $zy = x$.*

Démonstration. Soient x un nombre rationnel arbitraire et y un nombre rationnel non nul. Soit v un nombre rationnel tel que $yv = vy = 1$ (il existe d'après le lemme précédent). Alors

$$(xv)y = x(vy) = x \cdot 1 = x.$$

On a montré l'existence, il reste à montrer l'unicité : que si z est un nombre rationnel tel que $zy = x$, alors $z = xv$.

Soit z un nombre rationnel tel que $zy = x$. Alors

$$z = z \cdot 1 = z(yv) = (zy)v = xv. \qquad \square$$

Corollaire. *Si x et y sont nombres rationnels tels que $x \neq 0$ et $y \neq 0$, alors $xy \neq 0$.*

Définition. Deux nombres rationnels x et y sont dits *réciproques* l'un de l'autre si et seulement si $xy = 1$.

Définition. Si x est un nombre rationnel non nul et y est un nombre rationnel, alors l'unique nombre rationnel z tel que $zx = y$ est dit le *quotient* de y par x et est noté « $y \div x$ », ou « $y : x$ », ou « y/x », ou « $x \backslash y$ », ou « $\dfrac{y}{x}$ ».

Ainsi on a défini l'opération de *division* $(/)$ qui à n'importe quels deux nombres rationnels, dont le deuxième n'est pas zéro, associe leur quotient.

Exercice. Calculer et simplifier : $(1/2)/(3/4)$, $((-1)/2)/(3/4)$, $((-1)/2)/(3/(-4))$.

La définition de l'opération de division donnée ci-dessus peut être exprimée par l'équivalence suivante :

$$\frac{y}{x} = z \quad \Leftrightarrow \quad \begin{cases} y = zx \\ x \neq 0 \end{cases}.$$

L'opération de division $(/)$ de rationnels peut aussi être définie par les trois propriétés suivantes, à la condition que l'opération de multiplication $(\cdot)$ est déjà définie :

(1) $(xy)/y = x$ si $y \neq 0$,

(2) $(x/y)y = x$ si $y \neq 0$,

(3) la valeur de « x/y » n'est pas définie si $y = 0$.

En fait, la deuxième propriété résulte de la première, et la première résulte de la deuxième, donc il suffit de garder une seule parmi les deux.

Exercice. Montrer que la deuxième propriété résulte de la première, et que la première résulte de la deuxième.

Voici quelques identités remarquables satisfaites par l'opération de division des nombres rationnels *à la condition que les valeurs de tous les quotients soient définis* (que les dénominateurs ne soient pas 0) :

(1) $x(y/z) = (xy)/z$,

(2) $x/(yz) = (x/z)/y$,

(3) $x/(y/z) = (xz)/y$,

(4) $(x/y)(y/z) = x/z$,

(5) $(xz)/(yz) = x/y$,

(6) $(x/y)z = (xz)/y$,

(7) $(x/y)/z = (x/z)/y$,

(8) $x/(x/y) = y$,

(9) $x/1 = x$,

(10) $x/x = 1$,

(11) $(x+y)/z = x/z+y/z$,

(12) $(x-y)/z = x/z-y/z$,

(13) $0/x = 0$.

Exercice. Démontrer ces identités.

Rapport aux relations d'ordre usuelles

Proposition. *Pour tous nombres rationnels x, y, z,*

(1) *si $x < y$ et $z > 0$, alors $xz < yz$,*

(2) *si $x < y$ et $z < 0$, alors $xz > yz$.*

Exercice. Prouver cette proposition.

Corollaire. *Pour tous nombres rationnels x, y, z,*

(1) *si $z > 0$, alors les équivalences suivantes sont satisfaites :*

$$x < y \quad \Leftrightarrow \quad xz < yz, \qquad\qquad x \leqslant y \quad \Leftrightarrow \quad xz \leqslant yz,$$

(2) *si $z < 0$, alors les équivalences suivantes sont satisfaites :*

$$x < y \quad \Leftrightarrow \quad xz > yz, \qquad\qquad x \leqslant y \quad \Leftrightarrow \quad xz \geqslant yz.$$

Corollaire. *Pour tous nombres rationnels x et y,*

(1) *si $x > 0$ et $y > 0$, alors $xy > 0$,*

(2) *si $x > 0$ et $y < 0$, alors $xy < 0$,*

(3) *si $x < 0$ et $y > 0$, alors $xy < 0$,*

(4) *si $x < 0$ et $y < 0$, alors $xy > 0$.*

Corollaire. *Pour tout nombre rationnel* x, $xx \geqslant 0$.

Proposition. *Pour tous nombres rationnels* strictement positifs x, y, z, *si* $x < y$, *alors* $z/x > z/y$.

Exercice. Prouver cette proposition.

Corollaire. *Pour tous nombres rationnels* strictement positifs x, y, z, *les équivalences suivantes sont satisfaites* :

$$x < y \quad \Leftrightarrow \quad z/x > z/y, \qquad\qquad x \leqslant y \quad \Leftrightarrow \quad z/x \geqslant z/y.$$

III.6. Pour cent et pour mille

Définition. Si x est un nombre rationnel, alors x *pour cent*, noté « $x\,\%$ », est le quotient de x par cent :

$$x\,\% \overset{\text{déf}}{=} \frac{x}{100}.$$

Exemples.

$$125\,\% = \frac{125}{100} = \frac{5}{4} = 1{,}25, \qquad \frac{3}{2}\,\% = \frac{3}{200} = 0{,}015, \qquad \frac{2}{3}\,\% = \frac{1}{150}.$$

Définition. Si x est un nombre rationnel, alors x *pour mille*, noté « $x\,‰$ », est le quotient de x par mille :

$$x\,‰ \overset{\text{déf}}{=} \frac{x}{1000}.$$

Exemples.

$$125\,‰ = \frac{125}{1000} = \frac{1}{8} = 0{,}125, \qquad \frac{3}{2}\,‰ = \frac{3}{2000} = 0{,}0015, \qquad \frac{2}{3}\,‰ = \frac{1}{1500}.$$

III.7. Valeur absolue

Définition. La *valeur absolue* d'un nombre rationnel x, notée « $|x|$ », est définie ainsi :

$$|x| \overset{\text{déf}}{=} \begin{cases} +x & \text{si} \quad x \geqslant 0, \\ -x & \text{si} \quad x \leqslant 0. \end{cases}$$

En utilisant la notation avec « max », on peut définir la valeur absolue d'un nombre rationnel x par la formule :

$$|x| = \max(x, -x).$$

Une autre façon (équivalente) de définir la valeur absolue d'un nombre rationnel x est par l'équivalence suivante :

$$|x| = y \quad \Leftrightarrow \quad \begin{cases} xx = yy \\ y \geqslant 0 \end{cases}.$$

Exercice. Montrer que la valeur absolue peut être définie par cette équivalence.

Lemme. *Pour tous nombres rationnels x et y,*

$$|x| \leqslant y \quad \Leftrightarrow \quad -y \leqslant x \leqslant y \qquad \textit{et} \qquad |x| < y \quad \Leftrightarrow \quad -y < x < y.$$

Une démonstration de ce lemme est identique au cas des entiers.

Proposition (Inégalité triangulaire)**.** *Pour tous nombres rationnels x et y,*

$$|x + y| \leqslant |x| + |y|\,.$$

Une démonstration de cette proposition est identique au cas des entiers.

Proposition. *Pour tous nombres rationnels x et y,*

$$|xy| = |x|\,|y|\,.$$

Exercice. Prouver cette proposition.

Corollaire. *Pour tous nombres rationnels x et $y \neq 0$,*

$$\left|\frac{x}{y}\right| = \frac{|x|}{|y|}.$$

Exercice. Prouver ce corollaire.

III.8. Exponentiation, puissances, racines

Définition. Si n est un nombre naturel et x est un nombre rationnel, alors x *puissance* n, ou la n-ième *puissance* de x, ou x *élevé à la n-ième puissance*, est le nombre noté « x^n » et défini par la règle :

$$x^n \overset{\text{déf}}{=} 1 \underbrace{\cdot x \cdot x \cdot \cdots \cdot x}_{n \text{ fois}}.$$

Définition. Si m et n sont deux nombres naturels, x est un nombre rationnel non nul, et $a = n - m$, alors x *puissance* a est le nombre noté « x^a » et défini par la règle :

$$x^{n-m} \overset{\text{déf}}{=} 1 \underbrace{\cdot x \cdot x \cdot \cdots \cdot x}_{n \text{ fois}} \underbrace{/x/x/ \cdots /x}_{m \text{ fois}} = \frac{x^n}{x^m}.$$

Exercice. Calculer : 3^2, 2^3, 3^{-2}, 2^{-3}, $(-3)^{-2}$, $(-2)^{-3}$, $(2/3)^2$, $(3/2)^2$, $(2/3)^{-2}$, $(3/2)^{-2}$.

Voici quelques identités remarquables pour a et b entiers et pour x et y rationnels *non nuls* :

(1) $x^{ab} = (x^a)^b$,

(2) $x^1 = x$,

(3) $x^{a+b} = x^a x^b$,

(4) $x^{a-b} = x^a / x^b$,

(5) $x^0 = 1$,

(6) $(xy)^a = x^a y^a$,

(7) $(x/y)^a = x^a / y^a$,

(8) $1^a = 1$.

Exercice. Démontrer ces identités.

Question. Est-ce qu'il existe un nombre rationnel x tel que $x^2 = 2$?

Définition. Si n est un nombre naturel non nul, une *racine n-ième* d'un nombre x est un nombre y tel que $y^n = x$. Une racine deuxième est aussi dite *racine carrée*, et une racine troisième est aussi dite *racine cubique*.

Définition. Soient n un nombre naturel impair et x un nombre rationnel qui est la n-ième puissance d'un nombre rationnel y ($x = y^n$). Alors ***la*** racine n-ième de x est l'unique racine n-ième rationnelle de x (donc y).

Définition. Soient n un nombre naturel non nul et x un nombre rationnel positif ($x \geqslant 0$) qui est la n-ième puissance d'un nombre rationnel y ($x = y^n$). Alors ***la*** racine n-ième de x est l'unique racine n-ième positive de x (donc $|y|$). Si x est strictement positif ($x > 0$), alors la racine n-ième positive de x est aussi dite la racine n-ième *principale* de x.

Notation. Si n est un nombre naturel non nul et x est un nombre rationnel qui admet une racine n-ième rationnelle[2], alors on note « $\sqrt[n]{x}$ » ou « $\sqrt[n]{x}$ » l'unique racine n-ième rationnelle de x si n et impair, et on note « $\sqrt[n]{x}$ » ou « $\sqrt[n]{x}$ » l'unique racine n-ième positive de x si n est pair. Si n est pair et x est strictement négatif, alors la valeur de l'expression « $\sqrt[n]{x}$ » n'est pas définie (l'expression « $\sqrt[n]{x}$ » n'a pas de sens). Dans le cas où $n = 2$, on utilise aussi la notation « $\sqrt{x}$ » au lieu de « $\sqrt[2]{x}$ ».

Ainsi, si n est un nombre naturel *impair*, alors pour tous x et y rationnels,

$$\sqrt[n]{x} = y \quad \Leftrightarrow \quad x = y^n,$$

et si n est un nombre naturel non nul *pair*, alors pour tous x et y rationnels,

$$\sqrt[n]{x} = y \quad \Leftrightarrow \quad \begin{cases} x = y^n \\ y \geqslant 0 \end{cases}.$$

Pour n naturel *impair*, l'opération $\sqrt[n]{}$ sur les nombres rationnels peut aussi être définie par les trois propriétés suivantes :

(1) $\sqrt[n]{x^n} = x$,

(2) $(\sqrt[n]{x})^n = x$ si x est la n-ième puissance d'un nombre rationnel,

(3) la valeur de « $\sqrt[n]{x}$ » n'est définie (comme un nombre rationnel) que si x est la n-ième puissance d'un nombre rationnel.

[2] La même notation sera utilisée pour les racines *réelles*.

En fait, la deuxième propriété résulte de la première, et la première résulte de la deuxième, donc il suffit de garder une seule parmi les deux.

Pour n naturel non nul *pair*, l'opération $\sqrt[n]{}$ sur les nombres rationnels peut aussi être définie par les trois propriétés suivantes :

(1) $\sqrt[n]{x^n} = x$ si $x \geqslant 0$,

(2) $(\sqrt[n]{x})^n = x$ si x est la n-ième puissance d'un nombre rationnel,

(3) la valeur de « $\sqrt[n]{x}$ » n'est définie (comme un nombre rationnel) que si x est la n-ième puissance d'un nombre rationnel.

En fait, la deuxième propriété résulte de la première, et la première résulte de la deuxième, donc il suffit de garder une seule parmi les deux.

Voici quelques identités remarquables pour m et n naturels non nuls, a entier, et x et y rationnels, qui sont satisfaites *à la condition que les valeurs des deux membres* (des parties gauche et droite) *soient définies comme nombres rationnels* :

(1) $\sqrt[n]{x^a} = \left(\sqrt[n]{x}\right)^a$,

(2) $\sqrt[n]{\sqrt[m]{x}} = \sqrt[nm]{x}$,

(3) $\sqrt[n]{xy} = \sqrt[n]{x}\sqrt[n]{y}$,

(4) $\sqrt[n]{x/y} = \sqrt[n]{x}/\sqrt[n]{y}$,

(5) $\sqrt[n]{1} = 1$, $\sqrt[n]{0} = 0$.

Exercice. Démontrer ces identités.

Définition. Si n est un nombre naturel non nul, a est un entier, x est un nombre rationnel strictement positif tel que la valeur de « $\sqrt[n]{x^a}$ » soit définie, et $y = \dfrac{a}{n}$, alors x *puissance* y est le nombre noté « x^y » et défini par la règle :

$$x^{a/n} \overset{\text{déf}}{=} \sqrt[n]{x^a} \qquad \text{(si la valeur de « } \sqrt[n]{x^a} \text{ » est définie).}$$

Exercice. Vérifier si toutes les définitions données sont correctes et cohérentes entre elles.

Exercice. Calculer : $8^{2/3}$, $8^{-2/3}$, $9^{1,5}$, $9^{-1,5}$.

Voici quelques identités remarquables pour x et y rationnels *strictement positifs* et pour s et t rationnels, qui sont satisfaites à la condition que les valeurs des deux membres (des parties gauche et droite) soient définies comme nombres rationnels :

(1) $x^{st} = (x^s)^t$,

(2) $x^1 = x$,

(3) $x^{s+t} = x^s x^t$,

(4) $x^{s-t} = x^s/x^t$,

(5) $x^0 = 1$,

(6) $(xy)^t = x^t y^t$,

(7) $(x/y)^t = x^t/y^t$,

(8) $1^t = 1$.

Exercice. Démontrer ces identités.

Rapport aux relations d'ordre usuelles

Proposition. *Pour tous nombres rationnels* strictement positifs x *et* y *et pout tout nombre rationnel* t *tels que les valeurs de « x^t » et de « y^t » soient définies comme nombres rationnels, on a* :

(1) *si* $x < y$ *et* $t > 0$, *alors* $x^t < y^t$, (2) *si* $x < y$ *et* $t < 0$, *alors* $x^t > y^t$.

Exercice. Prouver cette proposition.

Proposition. *Pour tous nombres rationnels* s *et* t *et pout tout nombre rationnel* strictement positif x *tels que les valeurs de « x^s » et de « x^t » soient définies comme nombres rationnels, on a* :

(1) *si* $s < t$ *et* $x > 1$, *alors* $x^s < x^t$, (2) *si* $s < t$ *et* $x < 1$, *alors* $x^s > x^t$.

Exercice. Prouver cette proposition.

III.9. Systèmes de numération positionnels n-aires

En utilisant un *système de numération positionnel n-aire*, on peut écrire certains nombres rationnels positifs qui ne sont pas entiers en utilisant une virgule pour indiquer la fin de l'écriture de leur *partie entière*. Par exemple, en décimal,

$$\begin{aligned}
\frac{1}{10} &= 0{,}1 && = 0 \cdot 10^0 + 1 \cdot 10^{-1},\\
\frac{3}{4} = \frac{75}{100} &= 0{,}75 && = 0 \cdot 10^0 + 7 \cdot 10^{-1} + 5 \cdot 10^{-2},\\
\frac{6}{5} = \frac{12}{10} &= 1{,}2 && = 1 \cdot 10^0 + 2 \cdot 10^{-1},
\end{aligned}$$

et en base 3,

$$\begin{aligned}
\frac{1}{3} = \frac{1_3}{10_3} &= 0{,}1_3 && = 0 \cdot 3^0 + 1 \cdot 3^{-1},\\
\frac{5}{9} = \frac{12_3}{100_3} &= 0{,}12_3 && = 0 \cdot 3^0 + 1 \cdot 3^{-1} + 2 \cdot 3^{-2},\\
\frac{7}{3} = \frac{21_3}{10_3} &= 2{,}1_3 && = 2 \cdot 3^0 + 1 \cdot 3^{-1}.
\end{aligned}$$

Cependant, on ne peut pas écrire $1/3$ en décimal, ni $1/2$ en base 3.

III.10. Nombres n-aires

Définition. Soit $n > 1$ un nombre naturel. Un nombre rationnel est dit *n-aire* si et seulement si il est de la forme a/n^m avec m naturel et a entier.

Comme dans les autres contextes, on utilise d'habitude les adjectifs « *binaire* », « *ternaire* », « *quaternaire* » au lieu de « deux-aire », « trois-aire », « quatre-aire », et ainsi de suite.

En particulier, un nombre rationnel est dit

- *binaire* si et seulement si il est de la forme $a/2^n$ avec n naturel et a entier,
- *ternaire* si et seulement si il est de la forme $a/3^n$ avec n naturel et a entier,
- *quaternaire* si et seulement si il est de la forme $a/4^n$ avec n naturel et a entier,
- *octal* si et seulement si il est de la forme $a/8^n$ avec n naturel et a entier,
- *décimal* si et seulement si il est de la forme $a/10^n$ avec n naturel et a entier,
- *hexadécimal* si et seulement si il est de la forme $a/16^n$ avec n naturel et a entier.

Exemples. Le nombre $1/2$ est binaire et quaternaire, ainsi que décimal, mais il n'est pas ternaire. En effet :

$$\frac{1}{2} = \frac{1}{2^1} = \frac{2}{4^1} = \frac{5}{10^1},$$

mais il est impossible d'écrire $1/2$ sous la forme « $a/3^n$ » avec n naturel et a entier. Le nombre $2/3$ est ternaire, mais il n'est pas binaire, ni quaternaire, ni décimal.

Tout nombre entier est binaire, ternaire, quaternaire, et ainsi de suite. En effet, quels que soient un nombre naturel $m > 1$ et un nombre entier a, $a = a/m^0$.

Exercice. Parmi les nombres suivants, déterminer lesquels sont binaires, lesquels sont ternaires, et lesquels sont décimaux : $3/4$, $-4/5$, 1,5, 0,33.

Proposition. *Soit $n > 1$ un nombre naturel. Soient x et y deux nombres rationnels n-aires. Alors les nombres $x + y$, $x - y$ et xy sont tous n-aires.*

Exercice. Prouver cette proposition.

En particulier, la somme, la différence et le produit de deux nombres décimaux sont décimaux.

Proposition. *Soit $n > 1$ un nombre naturel. Alors un nombre rationnel est n-aire si et seulement si il peut être écrit en système de numération positionnel n-aire (avec un nombre fini de chiffres après la virgule).*

Exercice. Prouver cette proposition.

En particulier, un nombre rationnel est décimal si et seulement si il peut être écrit en système de numération arabe occidental (avec un nombre fini de chiffres après la virgule).

III.11. Logarithmes

Définition. Si x et y sont nombres rationnels strictement positifs et $x \neq 1$, alors l'unique nombre rationnel z tel que $x^z = y$ (si un tel z existe) est dit le *logarithme* de y en *base* x et est noté « $\log_x y$ ».

Cette définition de $\log_x$ (pour x strictement positif et différent de 1) peut être exprimée par l'équivalence suivante :

$$\log_x y = z \quad \Leftrightarrow \quad y = x^z.$$

Pour x strictement positif et différent de 1, l'opération $\log_x$ sur les nombres rationnels peut aussi être définie par les trois propriétés suivantes :

(1) $\log_x x^y = y$,

(2) $x^{\log_x y} = y$ si y est une puissance rationnelle de x,

(3) la valeur de « $\log_x y$ » n'est définie (comme un nombre rationnel) que si y est une puissance rationnelle de x.

En fait, la deuxième propriété résulte de la première, et la première résulte de la deuxième, donc il suffit de garder une seule parmi les deux.

Exercice. Calculer $\log_3 3$, $\log_2 4$, $\log_4 2$, $\log_{10} 1\,000$, $\log_{10} 1\,000\,000$, $\log_{10} 0{,}001$.

Voici quelques identités remarquables qui sont satisfaites pour tous nombres rationnels x, y, z, w, t, tels que $x > 0$, $y > 0$, $z > 0$, $w > 0$, $x \neq 1$, $y \neq 1$, à la condition que les valeurs des deux membres (des parties gauche et droite) soient définies comme nombres rationnels :

(1) $(\log_x y)(\log_y z) = \log_x z$,

(2) $(\log_x y)(\log_y x) = 1$,

(3) $\log_x x = 1$,

(4) $\log_x zw = \log_x z + \log_x w$,

(5) $\log_x \dfrac{z}{w} = \log_x z - \log_x w$,

(6) $\log_x 1 = 0$.

Exercice. Démontrer ces identités.

III.12. Décomposition en une somme de nombres plus « simples »

Lemme. *Si a et b sont deux nombres entiers non nuls premiers entre eux, alors il existe deux nombres entiers c et d tels que*

$$\frac{1}{ab} = \frac{c}{a} + \frac{d}{b}.$$

Démonstration. Soient a et b deux nombres entiers non nuls premiers entre eux. Appliquons le lemme de Bézout à a et b. Soient alors c et d deux nombres entiers tels que $1 = bc + ad$ (ils existent d'après le lemme de Bézout). Alors

$$\frac{1}{ab} = \frac{bc+ad}{ab} = \frac{c}{a} + \frac{d}{b}.$$ □

En utilisant ce lemme, on peut prouver que tout nombre rationnel non entier peut être écrit comme la somme d'un entier et d'une ou de plusieurs fractions de la forme « r/p^m », où p, r, m sont des nombres naturels non nuls, p est premier, et $r < p$, de manière que les dénominateurs des fractions qui apparaissent dans la somme soient deux à deux distincts.

Exemple. Voici une telle décomposition de $11/36$:

$$\frac{11}{36} = \frac{1}{2} + \frac{1}{4} + \frac{1}{3} + \frac{2}{9} - 1.$$

En fait, on peut prouver le théorème suivant :

Théorème. *Si $p_1, \ldots, p_n$ sont n nombres naturels premiers et deux a deux distincts, $m_1, \ldots, m_n$ sont n nombres naturels non nuls, et que a est un nombre entier, alors il existe une famille de $m_1 + \cdots + m_n$ nombres naturels $r_{1,1}, \ldots, r_{1,m_1}, \ldots, r_{n,1}, \ldots, r_{n,m_n}$ et un nombre entier b tels que $r_{i,j} < p_i$ pour tout i de 1 à n et pour tout j de 1 à m_i, et que*

$$\frac{a}{p_1^{m_1} \cdots p_n^{m_n}} = \frac{r_{1,1}}{p_1} + \cdots + \frac{r_{1,m_1}}{p_1^{m_1}} + \cdots + \frac{r_{n,1}}{p_n} + \cdots + \frac{r_{n,m_n}}{p_n^{m_n}} + b.$$

En plus, sous ces conditions, il n'y a qu'un seul choix possible de $r_{1,1}, \ldots, r_{1,m_1}, \ldots, r_{n,1}, \ldots, r_{n,m_n}$ (et de b).

Exemple. Quel que soit un nombre entier a, il existe des entiers $r_{1,1}$, $r_{1,2}$, $r_{2,1}$, $r_{2,2}$ et b tels que

$$\frac{a}{100} = \frac{a}{2^2 \cdot 5^2} = \frac{r_{1,1}}{2^1} + \frac{r_{1,2}}{2^2} + \frac{r_{2,1}}{5^1} + \frac{r_{2,2}}{5^2} + b = \frac{r_{1,1}}{2} + \frac{r_{1,2}}{4} + \frac{r_{2,1}}{5} + \frac{r_{2,2}}{25} + b,$$

avec

$$0 \leqslant r_{1,1} < 2, \qquad 0 \leqslant r_{1,2} < 2, \qquad 0 \leqslant r_{2,1} < 5, \qquad 0 \leqslant r_{2,2} < 5.$$

Par exemple :

$$\frac{1}{100} = \frac{0}{2} + \frac{1}{4} + \frac{3}{5} + \frac{4}{25} - 1, \qquad \frac{2}{100} = \frac{1}{2} + \frac{0}{4} + \frac{2}{5} + \frac{3}{25} - 1,$$

$$\frac{3}{100} = \frac{1}{2} + \frac{1}{4} + \frac{1}{5} + \frac{2}{25} - 1, \qquad \frac{4}{100} = \frac{0}{2} + \frac{0}{4} + \frac{0}{5} + \frac{1}{25},$$

$$\frac{5}{100} = \frac{0}{2} + \frac{1}{4} + \frac{4}{5} + \frac{0}{25} - 1, \qquad \frac{6}{100} = \frac{1}{2} + \frac{0}{4} + \frac{2}{5} + \frac{4}{25} - 1,$$

$$\frac{7}{100} = \frac{1}{2} + \frac{1}{4} + \frac{1}{5} + \frac{3}{25} - 1, \qquad \frac{8}{100} = \frac{0}{2} + \frac{0}{4} + \frac{0}{5} + \frac{2}{25},$$

$$\frac{9}{100} = \frac{0}{2} + \frac{1}{4} + \frac{4}{5} + \frac{1}{25} - 1, \qquad \frac{10}{100} = \frac{1}{2} + \frac{0}{4} + \frac{3}{5} + \frac{0}{25} - 1.$$

En plus, pour un nombre a donné, il n'y a qu'un seul choix possible de $r_{1,1}$, $r_{1,2}$, $r_{2,1}$, $r_{2,2}$ (et de b).