Chapitre 1

Les entiers naturels

Ce premier chapitre reprend largement le cheminement de [A-F, Chapitre II]. Il est aussi inspiré du document de Nicole Bopp : http://irma.math.unistra.fr/ bopp/CAPES/cours/N.pdf

1.1 Définitions

On considère les deux définitions suivantes de l'ensemble $\mathbb{N}$ des entiers naturels.

Définition 1 – Définition 1 : axiomatique de Peano. On appelle *ensemble des entiers naturels*, un triplet $(\mathbb{N}, 0, \mathrm{S})$ où $\mathbb{N}$ est un ensemble, 0 un élément de $\mathbb{N}$[1] et $\mathrm{S}\colon \mathbb{N} \to \mathbb{N}$ une application de $\mathbb{N}$ dans lui-même vérifiant les propriétés suivantes

(i) L'application S est injective ;
(ii) L'élément 0 n'est pas dans $\mathrm{S}(\mathbb{N})$;
(iii) Si $\mathrm{A} \subset \mathbb{N}$ est une partie de $\mathbb{N}$ vérifiant les deux propriétés
(I) $0 \in \mathrm{A}$;
(H) $n \in \mathrm{A} \implies \mathrm{S}(n) \in \mathrm{A}$;
alors $\mathrm{A} = \mathbb{N}$.

On dit que l'application S est l'application *successeur* et que, pour $n \in \mathbb{N}$, $\mathrm{S}(n)$ est le successeur de n.

Commentaires. Cette définition de $\mathbb{N}$ base les entiers naturels sur le principe de récurrence : la point (I) fait référence à l'initialisation et le point (H) à l'hérédité.

À partir de cet axiomatisation de $\mathbb{N}$, il est possible de construire par récurrence[2] une addition sur $\mathbb{N}$ (corollaire 6), une relation d'ordre (proposition-définition 10), puis une multiplication (proposition-définition 12) et même l'exponentiation (proposition-définition 15). Mais le point finalement le plus délicat dans tout cela est justement celui qui est le plus intuitif : le fait de pouvoir définir une suite par récurrence (théorème 5 de Dedekind).

On trouvera dans https://www.apmep.fr/IMG/pdf/PLegrand-Recurrence.pdf quelques éléments historiques sur la récurrence.

Remarque 2 – Tout élément sauf 0 est le successeur d'un élément de $\mathbb{N}$. La définition 1 implique que tout élément de $\mathbb{N}$ sauf 0 est le successeur d'un élément de $\mathbb{N}$[3], autrement dit $\mathrm{S}(\mathbb{N}) = \mathbb{N} \setminus \{0\}$. En effet, par le point (ii), $0 \in \mathrm{S}(\mathbb{N})$ ainsi $\mathrm{S}(\mathbb{N}) \subset \mathbb{N} \setminus \{0\}$. Pour montrer l'inclusion dans l'autre sens, on va utiliser le point (iii) qui donne un critère pour savoir qu'une partie de $\mathbb{N}$ est $\mathbb{N}$ tout entier. On considère donc la partie $\mathrm{A} = \{0\} \cup \mathrm{S}(\mathbb{N})$. On a bien sûr $0 \in \mathrm{A}$ et si $n \in \mathrm{A}$ alors $\mathrm{S}(n) \in \mathrm{S}(\mathbb{N})$ (puisque $n \in \mathbb{N}$) et donc $\mathrm{S}(n) \in \mathrm{A}$. Ainsi par ($iii$), $\mathrm{A} = \mathbb{N}$ et donc $\mathbb{N} = \{0\} \cup \mathrm{S}(\mathbb{N})$. Un élément $n \in \mathbb{N} \setminus \{0\}$ est donc dans $\mathrm{S}(\mathbb{N})$.

Définition 3 – Définition 2. On appelle *ensemble des entiers naturels* un couple $(\mathbb{N}, \leqslant)$ formé d'un ensemble $\mathbb{N}$ et d'une relation d'ordre $\leqslant$ sur $\mathbb{N}$ vérifiant les quatre propriétés suivantes

(i) l'ensemble $\mathbb{N}$ est non vide ;

1. En particulier, cela implique que $\mathbb{N}$ est non vide
2. Comment pourrait-il en être autrement, vu que c'est le seul outil dont on dispose ?
3. On ne confondra pas les expressions « a un successeur » et « est un successeur » qui reviennent respectivement à déterminer l'image par S et l'antécédent par S, on retrouve les mêmes difficultés dans les expressions scolaires « a pour double » et « est le double » ou encore « a pour moitié » et « est la moitié »

(ii) toute partie non vide de $\mathbb{N}$ admet un plus petit élément ;
(iii) toute partie non vide et majorée de $\mathbb{N}$ admet un plus grand élément ;
(iv) l'ensemble $\mathbb{N}$ n'admet pas de plus grand élément.

Remarque 4 – Ordre total. La propriété (ii) de la définition 2 assure que l'ordre sur $\mathbb{N}$ est un ordre total c'est-à-dire que pour tout $(n, m) \in \mathbb{N}$, on a $n \leqslant m$ ou $m \leqslant n$. En effet, la partie $\{m, n\}$ est non vide et admet donc un plus petit élément. Si c'est m alors $m \leqslant n$; si c'est n alors $n \leqslant m$.

1.2 De (2) vers (1).

Dans cette première section, le résultat que nous allons montrer est qu'un ensemble vérifiant la définition (2) vérifie la définition (1). De façon heuristique, un ensemble vérifiant la définition (2) vérifie le principe de récurrence. La preuve suit la démarche suivante :

on considère un ensemble ordonné $(\mathbb{N}, \leqslant)$ vérifiant les quatre propriétés de la définition (2).

a) on commence par définir l'élément 0 ;
b) puis on définit S ;
c) on montre que $0 \notin \mathrm{S}(\mathbb{N})$;
d) puis que S est injective ;
e) on montre ensuite que si $n \in \mathbb{N} \setminus \{0\}$ alors il existe $m \in \mathbb{N}$ tel que $\mathrm{S}(m) = n$;
f) enfin, on montre que l'ensemble $\mathbb{N}$ vérifie le point (iii) de la définition (i).

Preuve.

a) On considère l'ensemble $\mathbb{N}$ qui est non vide par le point (i). Il admet donc un plut petit élément par le point (ii). On note 0 cet élément qui est donc par définition le plus petit élément de $\mathbb{N}$.

b) De façon heuristique, $\mathrm{S}(n)$ est le successeur de n, c'est-à-dire celui qui vient après ce qu'on peut caractériser en terme d'ordre en disant que $\mathrm{S}(n)$ est le plus petit élément parmi les nombres qui sont strictement plus grand que n. De façon précise, pour $n \in \mathbb{N}$, on définit $\mathrm{A}(n) = \{m \in \mathbb{N}, \quad m > n\}$ [4]. L'ensemble $\mathrm{A}(n)$ est non vide. En effet, si $\mathrm{A}(n)$ était vide, alors comme l'ordre sur $\mathbb{N}$ est total, cela signifierait que $m \leqslant n$ pour tout $n \in \mathrm{NN}$ et donc que n serait un plus grand élément de $\mathbb{N}$ ce qui est en contradiction avec le point (iv). Ainsi $\mathrm{A}(n) \neq \varnothing$. D'après ($ii$), $\mathrm{A}(n)$ a un plus petit élément, on le note $\mathrm{S}(n)$.

c) Raisonnons par l'absurde. On suppose qu'il existe n tel que $0 = \mathrm{S}(n)$. En particulier, on en déduit que $0 \in \mathrm{A}(n) = \{m, m > n\}$. En particulier, on a $0 > n$ ce qui contredit la définition de 0 qui est le plus petit élément de $\mathbb{N}$.

d) On considère deux éléments $n, n' \in \mathbb{N}$ tel que $n \neq n'$. Comme l'ordre sur $\mathbb{N}$ est total, on peut supposer que $n < n'$. En particulier, on en déduit que $n' \in \mathrm{A}(n)$ et donc $\mathrm{S}(n) \leqslant n'$ puisque $\mathrm{S}(n)$ est le plus petit élément de $\mathrm{A}(n)$. Comme $n' < \mathrm{S}(n')$, par définition de $\mathrm{S}(n')$, on en déduit que $\mathrm{S}(n) \leqslant n' < \mathrm{S}(n')$ et donc $\mathrm{S}(n) \neq \mathrm{S}(n')$ [5].

e) Soit $m \in \mathbb{N} \setminus \{0\}$. On veut montrer qu'il existe $n \in \mathbb{N}$ tel que $\mathrm{S}(n) = m$. De façon heuristique, m va être le successeur de celui qui le précède c'est-à-dire va être le plus grand élément parmi tous les éléments qui sont plus petit que m. De façon précise, on considère $\mathrm{B}(m) = \{n \in \mathbb{N}, n < m\}$. Comme $m \neq 0$ et que 0 est le plus petit élément de $\mathbb{N}$, on a $0 \in \mathrm{B}(m)$ et on a donc $\mathrm{B}(m) \neq \varnothing$. De plus, $\mathrm{B}(m)$ est évidemment majoré par m. Le point (iii) montre que $\mathrm{B}(m)$ admet un plus grand élément. On le note $\mathrm{P}(m)$ [6]. Il s'agit à présent de montrer que $m = \mathrm{S}(\mathrm{P}(m))$ ce qui montrera bien que m est le successeur d'un élément de $\mathbb{N}$. Pour cela, on considère $\mathrm{A}(\mathrm{P}(m)) = \{n \in \mathbb{N}, n > \mathrm{P}(m)\}$. Par définition de $\mathrm{P}(m)$, on a $m \in \mathrm{A}(\mathrm{P}(m))$. On en déduit que $\mathrm{S}(\mathrm{P}(m)) \leqslant m$ puisque $\mathrm{S}(\mathrm{P}(m))$ est le plus petit élément de $\mathrm{A}(\mathrm{P}(m))$ par définition. Si jamais, on avait $\mathrm{S}(\mathrm{P}(m)) < m$, on aurait alors $\mathrm{S}(\mathrm{P}(m)) \in \mathrm{B}(m)$ et comme $\mathrm{P}(m) < \mathrm{S}(\mathrm{P}(m))$, cela contredirait la définition de $\mathrm{P}(m)$ qui ne serait plus le plus grand élément de $\mathrm{B}(m)$.

f) Soit A une partie de $\mathbb{N}$ vérifiant (I) et (H). On veut montrer que $\mathrm{A} = \mathbb{N}$. Pour cela, on raisonne par l'absurde et on suppose donc que ${}^{\mathrm{c}}\mathrm{A} \neq \varnothing$. Le point ($ii$) assure alors que ${}^{\mathrm{c}}\mathrm{A}$ admet un plus petit élément m. Bien entendu, $m \neq 0$ puisque $0 \in \mathrm{A}$ d'après (I). On en déduit, par **e**), qu'il existe n tel

4. l'ensemble $\mathrm{A}(n)$ est formé des éléments strictement plus grand que n
5. Au passage, on a montré que S est une application strictement croissante de $\mathbb{N}$ dans $\mathbb{N}$
6. Le nom P est pour faire penser à « prédécesseur »

que $m = \mathrm{S}(n)$. Comme $n < \mathrm{S}(n)$ par définition de S, on a $n < m$ et donc $n \notin {}^{\mathrm{c}}\mathrm{A}$. Ainsi $n \in \mathrm{A}$. Mais par (H), on a $\mathrm{S}(n) = m \in \mathrm{A}$ ce qui contredit le fait que $m \in {}^{\mathrm{c}}\mathrm{A}$. On en déduit que ${}^{\mathrm{c}}\mathrm{A} = \varnothing$ et donc $\mathrm{A} = \mathbb{N}$ [7].

1.3 De (1) vers (2).

L'objectif de cette section est de montrer qu'un ensemble vérifiant la définition (1) vérifiant nécessairement la propriété (2). Le chemin est beaucoup plus long notamment parce qu'il nécessite de définir la relation d'ordre ce qui ne se fait pas sans effort. En effet, le chemin est le suivant :

On considère un triplet $(\mathbb{N}, 0, \mathrm{S})$ vérifiant la définition (1).

a) on montre comment définir une suite par récurrence ;

b) on définit l'addition sur $\mathbb{N} \times \mathbb{N}$ (par récurrence) ;

c) on montre que l'addition est commutative, associative, a 0 pour élément neutre et que tout élément est régulier pour l'addition [8] ;

d) on définit l'ordre à partir de l'addition ;

e) on vérifie que c'est une relation d'ordre, grâce aux propriétés de l'addition.

1.3.1 Suite définie par récurrence

On commence par montrer le point **a**). L'énoncé étant fondamental, on l'érige avec le statut de théorème.

Théorème 5 – Définition d'une suite par récurrence (Dedekind, 1888). Soit E un ensemble non vide, $e \in \mathrm{E}$ et $f\colon \mathrm{E} \to \mathrm{E}$ une application de E dans lui-même. Il existe une unique application $u\colon \mathbb{N} \to \mathrm{E}$ [9] vérifiant les deux propriétés suivantes

(i) $u(0) = e$

(ii) $u \circ \mathrm{S} = f \circ u$ [10]

Preuve. Commençons par montrer l'unicité d'une application vérifiant les propriétés (i) et (ii). Supposons que u et v soient deux telles suites. On considère alors $\mathrm{A} = \{n \in \mathbb{N},\ u(n) = v(n)\}$. On va montrer que A vérifie les propriétés (I) et (H) du point (iii) de la définition (1). Comme u et v vérifient (i), on a $0 \in \mathrm{A}$; donc A vérifie (I). Supposons que $n \in \mathrm{A}$, montrons que $\mathrm{S}(n) \in \mathrm{A}$, il s'agit de calculer $u(\mathrm{S}(n))$. On a alors

$$u(\mathrm{S}(n)) = f(u(n)) = f(v(n)) = v(\mathrm{S}(n)\,.$$

En effet, la première égalité résulte du fait que u vérifie (ii), la deuxième du fait que $n \in \mathrm{A}$ et la troisième du fait que v vérifie (ii). Ainsi A vérifie (H). Ainsi $\mathrm{A} = \mathbb{N}$ et $u = v$.

Montrons maintenant l'existence de la suite u vérifiant (i) et (ii). Il y a un vrai travail à faire : définir une application n'est pas une chose aisée. Par cela, on va construire une partie de $\mathbb{N} \times \mathrm{E}$ qui va être le graphe de notre application c'est-à-dire l'ensemble des couples de la forme $(n, u(n))$. Une autre façon de dire ça est qu'on va construire une partie $\mathscr{I}$ de $\mathbb{N} \times \mathrm{E}$ telle que pour tout $n \in \mathbb{N}$, il existe un unique $x \in \mathrm{E}$ tel que $(n, x) \in \mathscr{I}$. Cela permet alors de définir $u(n) = x$. Il reste ensuite à vérifier que la suite u ainsi construite vérifie (i) et (ii).

Pour réaliser le programme ci-dessus, on commence par définir l'application

$$h\colon \begin{cases} \mathbb{N} \times \mathrm{E} \longrightarrow \mathbb{N} \times \mathrm{E} \\ (n, e) \longmapsto (\mathrm{S}(n), f(e)) \end{cases}$$

et on définit l'ensemble $\mathscr{P}$ des parties de $\mathbb{N} \times \mathrm{E}$ qui contient $(0, e)$ et qui sont envoyées dans elle-même par h :

$$\mathscr{P} = \{\mathrm{A} \subset \mathbb{N} \times \mathrm{E}, \quad h(\mathrm{A}) \subset \mathrm{A},\ (0, e) \in \mathrm{A}\}$$

7. De façon heuristique, pour montrer que $\mathrm{A} = \mathbb{N}$, on considère le plus petit élément qui n'est pas dans A, c'est le successeur d'un élément qui lui est plus petit et qui lui est dans A, ce n'est pas possible.

8. Cela signifie que $\forall\,(m, n, p) \in \mathbb{N}^3$ tels que $m + p = n + p$, on a $m = n$

9. Une fonction de $\mathbb{N}$ dans E est évidemment une suite à valeurs dans E au lieu de noter $u(n)$, on note u_n pour retrouver la notation habituelle pour les suites

10. c'est-à-dire pour tout $n \in \mathbb{N}$, $u(\mathrm{S}(n)) = f(u(n))$ ou encore pour calculer l'image par u du successeur de n, je calcule l'image par f de $u(n)$.

On remarque que $\mathscr{P} \neq \varnothing$ puisque $\mathbb{N} \times \mathrm{E} \in \mathscr{P}$. On pose alors

$$\mathscr{I} = \bigcap_{\mathrm{A} \in \mathscr{P}} \mathrm{A}\,.$$

On va montrer que $\mathscr{I}$ est le graphe d'une fonction.

Pour cela, on commence par montrer que

$$\forall\, n \in \mathbb{N},\ \exists x \in \mathrm{E}, \quad (n, x) \in \mathscr{I}\,.$$

On introduit alors l'ensemble $\mathrm{B} = \{n \in \mathbb{N}, \exists x \in \mathrm{E}, \quad (n, x) \in \mathscr{I}\}$; il s'agit de montrer que c'est $\mathbb{N}$. On va utiliser le point (iii) de la définition (1). Comme $(0, e) \in \mathrm{A}$ pour tout $\mathrm{A} \in \mathscr{P}$, on a $(0, e) \in \mathscr{I}$. Ainsi $0 \in \mathrm{B}$. On suppose à présent que $n \in \mathrm{B}$, on souhaite montrer que $\mathrm{S}(n) \in \mathrm{B}$. Par définition de B, il existe $x \in \mathrm{E}$ tel que $(n, x) \in \mathscr{I}$. Soit $\mathrm{A} \in \mathscr{P}$, on a $(n, x) \in \mathrm{A}$ et donc $h(n, x) \in h(\mathrm{A}) \subset \mathrm{A}$ puisque $\mathrm{A} \in \mathscr{P}$. On en déduit que $(\mathrm{S}(n), f(x)) \in \mathrm{A}$. Ainsi $(\mathrm{S}(n), f(x)) \in \mathscr{I}$ et donc $\mathrm{S}(n) \in \mathrm{B}$.

On souhaite à présent montrer que

$$\forall\, n \in \mathbb{N},\ \exists\,! x \in \mathrm{E}, \quad (n, x) \in \mathscr{I}\,.$$

Pour cela, on commence par remarquer que $h(\mathscr{I}) \subset \mathscr{I}$. En effet, on a

$$h\left(\bigcap_{\mathrm{A} \in \mathscr{P}} \mathrm{A}\right) \subset \bigcap_{\mathrm{A} \in \mathscr{P}} h(\mathrm{A}) \subset \left(\bigcap_{\mathrm{A} \in \mathscr{P}} \mathrm{A}\right) = \mathscr{I}\,^{11}.$$

Puis on cherche à écrire $\mathscr{I}$ sous une autre forme : on va montrer qu'en posant $\mathscr{F} = \{(0, e)\} \cup h(\mathscr{I})$, on a en fait $\mathscr{F} = \mathscr{I}$. Comme $(0, e) \in \mathscr{I}$ et $h(\mathscr{I}) \subset \mathscr{I}$, on a $\mathscr{F} \subset \mathscr{I}$. De plus, on a évidemment $(0, e) \in \mathscr{F}$ et $h(\mathscr{F}) \subset h(\mathscr{I}) \subset \mathscr{F}$. Ainsi $\mathscr{F} \in \mathscr{P}$ et donc $\mathscr{I} \subset \mathscr{F}$.

On considère à présent $\mathrm{C} = \{n \in \mathbb{N}, \exists\,! x \in \mathrm{E}, \quad (n, x) \in \mathscr{I}\}$. On veut montrer que $\mathrm{C} = \mathbb{N}$. Pour cela, on va montrer que C vérifie (I) et (H). On suppose que $(0, x) \in \mathscr{I}$. Comme $\mathscr{I} = \mathscr{F}$, on a soit $x = e$ soit $(0, n) = h(n, y)$ pour un certain couple $(n, y) \in \mathscr{I}$. Mais on a alors $\mathrm{S}(n) = 0$ ce qui est impossible d'après le point (ii) de la définition (1). Ainsi $x = e$ et $0 \in \mathrm{C}$. On suppose que $n \in \mathrm{C}$. On souhaite montrer que $\mathrm{S}(n) \in \mathrm{C}$. On a vu précédemment qu'il existe x tel que $(\mathrm{S}(n), x) \in \mathscr{I}$ (quand on a montré que $\mathrm{B} = \mathbb{N}$). Il s'agit de montrer l'unicité d'un tel x. Soit $(\mathrm{S}(n), x) \in \mathscr{I}$ et $(\mathrm{S}(n), y) \in \mathscr{I}$. Comme $\mathscr{I} = \mathscr{F} = \{(\mathrm{O}, e)\} \cup h(\mathscr{I})$ et que $0 \notin \mathrm{S}(\mathbb{N})$, il existe $(m, x') \in \mathscr{I}$ tel que $h(m, x') = (\mathrm{S}(n), x)$; de même il existe $(m', y') \in \mathscr{I}$ tel que $h(m', y') = (\mathrm{S}(n), y)$. Par définition de h, on obtient

$$\mathrm{S}(m) = \mathrm{S}(n) = \mathrm{S}(m') \qquad f(x') = x \qquad \text{et} \qquad f(y') = y$$

L'injectivité de S implique alors $m = m' = n$. On en déduit alors que $(n, x') \in \mathscr{I}$ et $(n, y') \in \mathscr{I}$. Comme $n \in \mathrm{C}$, on en déduit que $x' = y'$ et on a donc $x = f(x') = f(y') = y$ ce qui montre que $\mathrm{S}(n) \in \mathrm{C}$.

Ainsi $\mathscr{I}$ est bien le graphe d'une fonction de $\mathbb{N}$ dans E : on définit $u(n)$ comme l'unique x tel que $(n, x) \in \mathscr{I}$.

Il ne reste plus qu'à s'assurer que u vérifie les propriétés (i) et (ii). Comme $(0, e) \in \mathscr{I}$, on a bien $u(0) = e$. Et pour $n \in \mathbb{N}$, on a $(n, u(n)) \in \mathscr{I}$. De plus, on a vu que $h(\mathscr{I}) \subset \mathscr{I}$. Ainsi $h(n, u(n)) = (\mathrm{S}(n), f(u(n))) \in \mathscr{I}$ ce qui montre que $u(\mathrm{S}(n)) = f(u(n))$.

1.3.2 Définition de l'addition

Grâce à la définition d'une suite par récurrence, on peut définir l'addition dans $\mathbb{N}$. De façon précise, pour $m \in \mathbb{N}$, on va définir une application de $\mathbb{N}$ dans $\mathbb{N}$ (c'est-à-dire une suite d'entiers) qui correspondra à l'application qui ajoute m à l'entier de départ.

Corollaire 6 – Ajouter $m \in \mathbb{N}$**.** Soit $m \in \mathbb{N}$ et $\mathrm{S}\colon \mathbb{N} \to \mathbb{N}$ l'application successeur. Il existe une unique application $\Delta_m\colon \mathbb{N} \to \mathbb{N}$ telle que

(i) $\Delta_m(0) = m$;

(ii) $\Delta_m(\mathrm{S}(n)) = \mathrm{S}(\Delta_m(n))$ pour tout $n \in \mathbb{N}$.

11. La première inclusion est purement ensembliste (et à savoir démontrer) : pour tout application $\varphi\colon \mathrm{X} \to \mathrm{Y}$ et toute famille de parties $(\mathrm{X}_i)_{i \in \mathrm{I}}$ de X, on a $\varphi(\bigcap_{i \in \mathrm{I}} \mathrm{X}_i) \subset \bigcap_{i \in \mathrm{I}} \varphi(\mathrm{X}_i)$; la deuxième inclusion résulte du fait que $\mathrm{A} \in \mathscr{P}$ implique $h(\mathrm{A}) \subset \mathrm{A}$ et l'égalité résulte de la définition de $\mathscr{I}$.

Preuve. On applique le théorème 5 avec $\mathrm{E} = \mathbb{N}$, $e = m$ et $f = \mathrm{S}$. La suite u obtenue est noté Δ_m.

Notation 7 – Notation additive. Pour simplifier la notation $\Delta_m(n)$, on utilise plutôt la notation $n + m$. L'application Δ_m est donc par définition l'opération d'ajout à droite de m.

On prendra garde que pour le moment cette notation est trompeuse car on n'a montré aucune des propriétés de cette addition. En particulier, on ne sait pas encore qu'elle est commutative, ni aucune autre de ces propriétés.

La définition par récurrence se résume ainsi : ajouter m à un entier différent de 0 c'est ajouter m a son prédécesseur puis prendre le successeur de ce nombre.

Avec la notation additive,

$$\text{l'égalité } (i) \text{ se réécrit } 0 + m = m \qquad \text{et} \qquad \text{l'égalité } (ii) \text{ se réécrit } \mathrm{S}(n) + m = \mathrm{S}(n + m) \quad (\star)$$

Remarque 8 – $2 + 3 = 5$. Par la définition (1), on a un élément 0 dans $\mathbb{N}$. On a vu dans la remarque 2 que 0 est même le seul élément de $\mathbb{N}$ qui n'est pas le successeur d'un autre élément. Il est ainsi entièrement caractérisé.

On définit les entiers $1, 2, 3, 4$ et 5 successivement par $1 = \mathrm{S}(0)$ puis $2 = \mathrm{S}(1)$, $3 = \mathrm{S}(2)$, $4 = \mathrm{S}(3)$.

On est maintenant en mesure de démontrer que $2+3 = 5$. En effet, par définition $2+3 = \mathrm{S}(1)+3 = \mathrm{S}(1+3)$ (la première égalité est la définition de 2 et la deuxième relève de (ii) avec $n = 1$ (pour Δ_3). Il s'agit à présent de calculer $1 + 3$. Comme $1 = \mathrm{S}(0)$, on a $1 + 3 = \mathrm{S}(0) + 3 = \mathrm{S}(0 + 3)$ (la deuxième égalité provenant de (ii) avec $n = 0$ pour Δ_3). Or $0 + 3 = 3$ d'après l'égalité (i) pour Δ_3. On a donc $1 + 3 = \mathrm{S}(3) = 4$ par définition de 4 puis $2 + 3 = \mathrm{S}(1 + 3) = \mathrm{S}(4) = 5$.

De la même façon, on peut montrer que $3 + 2 = 5$. Pour cela, on remarque que $3 + 2 = \mathrm{S}(2) + 2 = \mathrm{S}(2 + 2)$ puis que $2 + 2 = \mathrm{S}(1) + 2 = \mathrm{S}(1 + 2)$ puis que $1 + 2 = \mathrm{S}(0) + 2 = \mathrm{S}(0 + 2)$ (en appliquant le point (ii) pour Δ_2). Mais $0 + 2 = 2$ par le point (i) pour Δ_2. Ainsi $1 + 2 = \mathrm{S}(2) = 3$ puisque $2 + 2 = \mathrm{S}(1 + 2) = \mathrm{S}(3) = 4$ et $3 + 2 = \mathrm{S}(2 + 2) = \mathrm{S}(4) = 5$.

On obtient que $2 + 3 = 3 + 2$, les principes de calculs sont les mêmes mais on voit que les étapes de calculs pour les deux calculs sont différentes et même que le nombre d'étapes pour chacun des deux calculs sont différents.

1.3.3 Propriétés de l'addition

Proposition 9 L'application

$$+ : \begin{cases} \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N} \\ (n, m) \longmapsto n + m = \Delta_m(n) \end{cases}$$

est associative, commutative, admet 0 pour élément neutre et tout élément est régulier pour $+$. De plus, on a $\mathrm{S}(n) = n + 1$ pour tout $n \in \mathbb{N}$. Et si $m + n = 0$ alors $m = n = 0$.

Preuve. Soit $m, \ell \in \mathbb{N}$. On considère l'ensemble

$$\mathrm{A} = \{n \in \mathbb{N}, n + (m + \ell) = (n + m) + \ell\} \text{ et on sait montrer que } \mathrm{A} = \mathbb{N}\,[12]$$

On va montrer que A vérifie (I) et (H). Grâce à la relation $(\star)$, on a $0 + (m + \ell) = m + \ell$ et $(0 + m) + \ell = m + \ell$ (car $0 + m = m$). Ainsi $0 \in \mathrm{A}$.

Supposons que $n \in \mathrm{A}$. Montrons que $\mathrm{S}(n) \in \mathrm{A}$. On a $\mathrm{S}(n) + (m + \ell) = \mathrm{S}(n + (m + \ell))$ d'après $(\star)$. Par ailleurs, $(\mathrm{S}(n) + m) + \ell = \mathrm{S}(n + m) + \ell$ (d'après $(\star)$ appliquée à $+m$). En appliquant $(\star)$ à $+\ell$, on obtient $\mathrm{S}(n + m) + \ell = \mathrm{S}((n + m) + \ell)$. Comme $n \in \mathrm{A}$, on a $\mathrm{S}(n + m) + \ell = n + (m + \ell)$ et donc $\mathrm{S}((n + m) + \ell) = \mathrm{S}(n + (m + \ell))$ ce qui montre que $\mathrm{S}(n) \in \mathrm{A}$. Ainsi $\mathrm{A} = \mathbb{N}$.

L'opération $+$ est donc bien associative.

Montrons qu'elle est commutative. Alors que ce résultat nous paraît évident, il repose en fait sur de nombreux calculs intermédiaires. On va, en effet, démontrer successivement que

(i) $m + 0 = m$ pour tout $m \in \mathbb{N}$;

(ii) $\mathrm{S}(n) = n + 1$ pour tout $n \in \mathbb{N}$;

12. Pour l'écrire d'une façon qui montre qu'il y a réellement quelque chose à démontrer : on a $\mathrm{A} = \{n \in \mathbb{N}, \quad \Delta_{m+\ell}(n) = \Delta_\ell(\Delta_m(n))\}$

puis on montrera que pour $m \in \mathbb{N}$, l'ensemble $B = \{n \in \mathbb{N}, n+m = m+n\}$ est $\mathbb{N}$ grâce à l'associativité de $+$.

Montrons (i). On considère l'ensemble $C = \{n \in \mathbb{N}, n+0 = n\}$. Par définition de $+0$, on a $0 \in C$. De plus, pour $n \in C$, on a $S(n)+0 = S(n+0)$ (par définition de $+0$). Comme $n \in C$, on a $n+0 = n$. Ainsi $S(n)+0 = S(n)$ et $S(n) \in C$. On en déduit, par le point (iii) de la définition (i) que $C = \mathbb{N}$ ce qui est bien le résultat souhaité.

Montrons (ii). On considère l'ensemble $D = \{n \in \mathbb{N}, S(n) = n+1\}$. Par définition, on a $S(0) = 1$ et $0+1 = 1$ (c'est la définition de $+1$). Ainsi $0 \in D$. Supposons que $n \in D$. On veut montrer que $S(n) \in D$. On a alors $S(n)+1 = S(n+1)$ par définition de $+1$. Puis comme $n \in D$, on a $n+1 = S(n)$ et donc $S(n)+1 = S(S(n))$ c'est-à-dire $S(n) \in D$. Ainsi $D = \mathbb{N}$ par le point (iii) de la définition (i) [13].

On montre à présent que $B = \mathbb{N}$. Pour cela, on montre que $0 \in B$ et que si $n \in B$ alors $S(n) \in B$. Par définition de $+m$, on a $0+m = m$ et, d'après le point (i) qu'on vient de montrer, on a aussi $m+0 = m$. Ainsi $0 \in B$. On suppose que $n \in N$. Montrons que $S(n) \in B$. Par définition de $+m$, on a $S(n)+m = S(n+m)$ et d'après le point (ii) ci-dessus, on a donc $S(n)+m = (n+m)+1$. Par ailleurs, d'après (ii), on a $m+S(n) = m+(n+1)$. L'associativité de $+$ montre alors que $S(n)+m = m+S(n)$ et donc $S(n) \in B$. On a donc $B = \mathbb{N}$ et $+$ est commutative.

Par ailleurs, on a vu que $0+m = m+0 = m$ pour tout $m \in \mathbb{N}$. Ainsi 0 est élément neutre pour $+$ [14]. Et on a vu que $S(n) = n+1$ pour tout $n \in \mathbb{N}$ et par commutativité, on a aussi $1+n = S(n)$ pour tout $n \in \mathbb{N}$ [15].

Supposons que $m+n = 0$. Si $m \neq 0$ alors, d'après la remarque 2, il existe $m' \in \mathbb{N}$ tel que $S(m') = m$. On a donc $m+n = S(m'+n)$ qui ne peut pas être égal à 0. Ainsi $m = 0$. On a donc $0 = m+n = 0+n = n$ et donc $m = n = 0$.

Il ne reste plus qu'à montrer que les éléments de $\mathbb{N}$ sont réguliers pour $+$. Comme l'addition est commutative, il suffit que démontrer que si m, n et p sont tels que $m+n = m+p$ alors $n = p$. Pour cela, on considère l'ensemble $E = \{m \in \mathbb{N}, \quad m+n = m+p \implies n = p\}$. Comme $0+n = n$ et $0+p = p$, on a $0 \in E$. On suppose que $m \in \mathbb{N}$, montrons que $S(m) \in \mathbb{N}$. On suppose donc que $S(m)+n = S(m)+p$. Par définition de $+n$ et $+p$, on a $S(m)+n = S(m+n)$ et $S(m)+p = S(m+p)$. On a donc $S(m+n) = S(m+p)$. L'injectivité de S assure alors que $m+n = m+p$. Comme $m \in E$, on en déduit que $n = p$. Ainsi $S(m) \in E$. Finalement, $E = \mathbb{N}$ ce qui montre que tout m est régulier.

1.3.4 Définition de l'ordre

Proposition-Définition 10 On considère la relation $n \leqslant m$ s'il existe $\ell \in \mathbb{N}$ tel que $n+\ell = m$. La relation $\leqslant$ est une relation d'ordre sur $\mathbb{N}$ vérifiant les propriétés suivantes :

(i) toute partie non vide de $\mathbb{N}$ admet un plus petit élément ;

(ii) toute partie non vide et majorée de $\mathbb{N}$ admet un plus grand élément ;

(iii) l'ensemble $\mathbb{N}$ n'admet pas de plus grand élément.

De plus, la relation $\leqslant$ est compatible avec l'addition : si $m \leqslant n$ alors $p+m \leqslant p+n$ pour tout $p \in \mathbb{N}$. On a aussi si $m, n, p \in \mathbb{N}$ vérifient $p+m \leqslant p+n$ alors $m \leqslant n$.

Preuve. Comme $m+0 = m$. On a $m \leqslant m$. La relation $\leqslant$ est donc réflexive.

Si $\ell \leqslant m$ et $m \leqslant n$ alors il existe $a, b \in \mathbb{N}$ tel que $\ell+a = m$ et $m+b = n$. On a alors par associativité de l'addition $\ell+(a+b) = n$ et donc $\ell \leqslant n$. Ainsi $\leqslant$ est transitive [16].

Si $m \leqslant n$ et $n \leqslant m$ alors il existe $a, b \in \mathbb{N}$ tel que $n+a = m$ et $m+b = n$. Par associativité de $+$, on obtient $n+(a+b) = n = n+0$. Comme n est régulier, on en déduit que $a+b = 0$. On en déduit que $a = b = 0$ grâce à la proposition 9 puisque $n = m$ (puisque $n+0 = n$ pour tout $n \in \mathbb{N}$). Ainsi $\leqslant$ est antisymétrique.

La proposition 9 montre que $S(n) = n+1$ et donc $S(n) \geqslant n$. De plus, on ne peut pas avoir $S(n) = n$. En effet, si $S(n) = n$ alors $n+1 = n+0$ et comme n est régulier, on a $1 = S(0) = 0$ ce qui contredit le fait que $0 \in S(\mathbb{N})$. On en déduit que $S(n) > n$. Ainsi $\mathbb{N}$ n'a pas de plus grand élément : s'il y en avait un, alors $S(n)$ serait plus grand que lui d'après ce qu'on vient de montrer. Ainsi, on a démontré (iii).

13. Autrement dit : prendre le successeur et ajouter 1, c'est la même chose ! Ouf, c'est cohérent avec ce qu'on imagine.
14. Cette propriété donne une nouvelle caractérisation de 0.
15. Cette propriété peut aussi se démontrer directement de la façon suivante : $1+n = S(0)+n = S(0+n) = S(n)$ la deuxième et la troisième égalité résultat de la définition de $+n$.
16. On constate que la transitivité s'obtient à partir de l'associativité de $+$.

Montrons la propriété suivante portant sur l'ordre si $n < m$ alors $n+1 \leqslant m$ qui nous servira par la suite (on la note (**1**)). Par définition, il existe $a \in \mathbb{N}$ tel que $n+a=m$. De plus, on a $a \neq 0$ puisque $n \neq m$. On peut alors écrire $a = \mathrm{S}(a')$ pour un $a' \in \mathbb{N}$ d'après la remarque 2. On en déduit que par la commutativité et l'associativité de $+$ que $n+1+a'=m$ [17].

Soit A une partie non vide de $\mathbb{N}$. On considère l'ensemble min des minorants de A. Comme $0+m=m$ pour tout $m \in \mathbb{N}$, on a $0 \leqslant m$ pour tout $m \in \mathrm{M}$ et donc 0 est le plus petit élément de $\mathbb{N}$. Ainsi $0 \in \min$. Par ailleurs, $\min \neq \mathbb{N}$. En effet, si $a \in \mathrm{A}$ alors $a+1 = \mathrm{S}(a) > a$ n'est pas un minorant de A. On déduit du point (*iii*) de la définition (1) qu'il existe $n_0 \in \min$ tel que $n_0 + 1 = \mathrm{S}(n_0) \notin \min$. Montrons que $n_0 \in \mathrm{A}$ puis que n_0 est le plus petit élément de A.

Comme $n_0 \leqslant a$ pour tout $a \in \mathrm{A}$ puisque $n_0 \in \min$ et comme $n_0 \notin \mathrm{A}$, on a même $n_0 < a$ pour tout $a \in \mathrm{A}$. On en déduit, grâce à (**1**) que $n_0 + 1 \leqslant a$ pour tout $a \in \mathrm{A}$ et donc n_0+1 est un minorant de A ce qui contredit la définition de n_0. Ainsi $n_0 \in \mathrm{A}$ et comme n_0 est un minorant de A, c'est le plus petit élément de A.

Montrons la propriété suivante portant sur l'ordre si $n < m$ alors, en notant m' tel que $\mathrm{S}(m') = m$, on a $n \leqslant m'$ qui nous servira par la suite (on la note (**2**)). Par définition, il existe $a \in \mathbb{N}$ tel que $n+a=m$. De plus, on a $a \neq 0$ puisque $n \neq m$. On peut alors écrire $a = \mathrm{S}(a')$ pour un $a' \in \mathbb{N}$ d'après la remarque 2. On en déduit, par l'associativité de $+$ que $(n+a')+1=m$. L'injectivité de S montre alors que $m' = n+a'$ et donc $n \leqslant m'$.

Soit A une partie non vide et majorée de $\mathbb{N}$. On considère l'ensemble M de majorant de A. Comme A est majorée, M est non vide. Donc M admet, d'après ce qui précède un plus petit élément m. Montrons que m est dans A. Comme $a \leqslant m$ pour $a \in \mathrm{A}$ puisque m est un majorant de A, si m n'est pas dans a, on a $a < m$ pour tout $a \in \mathrm{A}$. On note alors m' tel que $\mathrm{S}(m') = m$. La propriété (**2**) montre alors que $a \leqslant m'$ pour tout $a \in \mathrm{A}$ ce qui montre que m' est un majorant de A et comme $\mathrm{S}(m') = m'+1 = m$, on a $m' < m$ ce qui contredit la définition de m comme plus petit majorant de A. Ainsi $m \in \mathrm{A}$ et est un majorant de A. C'est donc le plus grand élément de A.

Il reste à montrer que $\leqslant$ est compatible avec $+$. Pour cela, on considère $m \leqslant n$. Il existe $a \in \mathbb{N}$ tel que $m+a=n$. On a alors $p+n = p+(m+a) = (p+m)+a$. La première égalité est une réécriture de n, la deuxième égalité provient de l'associativité de $+$. Ainsi $p+m \leqslant p+n$.

Et si $p+m \leqslant p+n$ alors il existe $a \in \mathbb{N}$ tel que $p+m+a = p+n$. Par régularité de p, on a $m+a=n$ et donc $m \leqslant n$.

On a ainsi montré qu'à partir de la définition (1), on pouvait construire sur $\mathbb{N}$ un ordre vérifiant les propriétés souhaitées de la définition (2) (la définition (1) de $\mathbb{N}$ assure le fait qu'il soit non vide par l'existence de 0). Ainsi les deux définitions sont bien équivalentes.

Remarque 11 On suppose qu'un ensemble $(\mathbb{N}, 0, \mathrm{S})$ vérifie la définition (1), on vient de voir comment définir un ordre sur $\mathbb{N}$ qui vérifie la définition (2). Or, dans la section 1.2, on a vu comment définir $0'$ et S' à partir de cet ordre pour que l'ensemble vérifie la définition (1). Par construction, $0'$ est le plus petit élément de $(\mathbb{N}, \leqslant)$ mais on a vu que cet élément est précisément l'élément 0. De même, grâce à la propriété (**2**), on a $\mathrm{S}' = \mathrm{S}$.

1.4 Multiplication et exponentiation

À partir de l'addition et de la définition d'une suite par récurrence (théorème 5), il est à présent aisé de définir la multiplication dans $\mathbb{N}$ puis d'en montrer les propriétés : dans cette construction, la multiplication est ainsi construite comme une addition itérée. Puis à partir de la multiplication, en suivant le même principe, on construit l'exponentiation.

1.4.1 La multiplication

Proposition-Définition 12 – Définition de la multiplication. Soit $m \in \mathbb{N}$ et $+m = \Delta_m$ l'application qui consiste à ajouter m à un entier. Il existe une unique application $\mu_m : \mathbb{N} \to \mathbb{N}$ telle que

(*i*) $\mu_m(0) = 0$;

(*ii*) $\mu_m(\mathrm{S}(n)) = \mu_m(n) + m = \Delta_m(\mu_m(n))$ pour tout $n \in \mathbb{N}$.

Preuve. On applique le théorème 5 avec $\mathrm{E} = \mathbb{N}$, $f = \Delta_m = +m$ et $e = 0$.

17. En fait, la propriété $u+1 = 1+u = \mathrm{S}(u)$ pour tout $u \in \mathbb{N}$ et l'associativité suffisent.

Notation 13 – notation multiplicative. Plutôt que la notation $\mu_m(n)$, on notera souvent $\mu_m(n) = mn$ ou $\mu_m(n) = m \times n$. On prendra bien garde au sens de ces notations, surtout tant que les propriétés de la multiplication n'auront pas été montrées.

Proposition 14 L'application

$$\times : \begin{cases} \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N} \\ (m,n) \longmapsto \mu_m(n) = m \times n \end{cases}$$

est associative, distributive par rapport à $+$, commutative, admet 1 pour élément neutre, 0 pour élément absorbant et tout élément non nul est régulier pour $\times$ [18].

De plus, l'égalité $mn = 0$ implique $n = 0$ ou $m = 0$ et l'égalité $mn = 1$ implique $n = m = 1$.

Par ailleurs,la multiplication est compatible avec la relation d'ordre c'est-à-dire

$$\forall\, (m,n,p) \in \mathbb{N}^3, \qquad m \leqslant n \implies mp \leqslant np$$

et

$$\forall\, (m,n,p) \in \mathbb{N} \times \mathbb{N} \times (\mathbb{N} \setminus \{0\}), \qquad mp \leqslant np \implies m \leqslant n\,.$$

Preuve. On commence par montrer que 0 est un élément absorbant pour $\times$. Par définition, on a $m \times 0 = \mu_m(0) = 0$ pour tout $m \in \mathbb{N}$. Il reste à montrer que $0 \times n = 0$ pour tout $n \in \mathbb{N}$. Pour cela, on considère l'ensemble $\mathrm{A} = \{n \in \mathbb{N}, 0 \times n = 0\}$. On a bien sûr $0 \times 0 = 0$, ainsi $0 \in \mathrm{A}$. On suppose que $n \in \mathrm{A}$ et on souhaite montrer que $\mathrm{S}(n) \in \mathrm{A}$. Or, $0 \times \mathrm{S}(n) = 0 \times n + 0 = 0 \times n$. La première égalité repose sur la définition de $0\times$ et la deuxième repose sur le fait que 0 est élément neutre pour $+$. Comme $n \in \mathrm{A}$, on en déduit que $0 \times \mathrm{S}(n) = 0$ et donc $\mathrm{S}(n) \in \mathrm{A}$. La propriété (iii) de la définition (1) assure alors que $\mathrm{A} = \mathbb{N}$. Ainsi 0 est absorbant pour $\times$.

Montrons que 1 est élément neutre pour $\times$. Par définition de μ_m, on a

$$m \times 1 = m \times \mathrm{S}(0) = m \times 0 + m$$

Comme $m \times 0 = 0$ et que 0 est élément neutre pour $+$, on a donc $m \times 1 = m$. Montrons que $1 \times m = m$ pour tout $m \in \mathbb{N}$. Pour cela, on considère l'ensemble $\mathrm{B} = \{n \in \mathbb{N}, 1 \times m = m\}$. Par définition de $1\times$, on a $0 \in \mathrm{B}$. On suppose que $n \in \mathrm{B}$ et on veut montrer que $\mathrm{S}(n) \in \mathrm{B}$. Par définition, on a $1 \times \mathrm{S}(n) = 1 \times n + 1$. Comme $1 \times n = n$ puisque $n \in \mathrm{B}$, on en déduit que $1 \times \mathrm{S}(n) = n + 1 = \mathrm{S}(n)$. Ainsi $\mathrm{S}(n) \in \mathrm{B}$. La propriété (iii) de la définition (1) assure alors que $\mathrm{B} = \mathbb{N}$. Ainsi 1 est élément neutre pour $\times$.

On va à présent montrer la distributivité à droite de la multiplication c'est-à-dire

$$\forall\, (\ell,n,m) \in \mathbb{N}^3, \qquad \ell(m+n) = \ell m + \ell n\,.$$

Pour cela, on considère l'ensemble $\mathrm{C} = \{n \in \mathbb{N}, \ell(n+m) = \ell n + \ell m\}$. Vérifions que $0 \in \mathrm{C}$. On a $0 + m = m$ puisque 0 est élément neutre pour l'addition. Ainsi $\ell(0+m) = \ell m$. De plus, on a vu que $\ell 0 = 0$ et comme 0 est élément neutre pour $+$, on a $\ell 0 + \ell m = 0 + \ell m = \ell m$. Ainsi $0 \in \mathrm{C}$. Montrons à présent que si $n \in \mathrm{C}$ alors $\mathrm{S}(n) \in \mathrm{C}$. On calcule

$$\ell(\mathrm{S}(n) + m) = \ell \mathrm{S}(n+m) = \ell(n+m) + \ell\,.$$

La première égalité repose sur la définition de $+m$ et la deuxième de $\ell\times$. Par ailleurs comme $n \in \mathrm{C}$, on a $\ell(n+m) + \ell = \ell n + \ell m + \ell$. La commutativité de $+$ assure alors que $\ell m + \ell = \ell + \ell m$. Ainsi, on en déduit que

$$\ell(\mathrm{S}(n) + m) = \ell \mathrm{S}(n+m) = \ell n + (\ell + \ell m) = (\ell n + \ell) + \ell m = \ell \mathrm{S}(n) + \ell m\,.$$

La troisième égalité repose sur l'associativité de $+$ et la quatrième sur la définition de $\ell\times$. On obtient ainsi que $\mathrm{S}(n) \in \mathrm{C}$. La propriété (iii) de la définition (1) assure alors que $\mathrm{C} = \mathbb{N}$ ce qu'on souhaitait démontrer.

Montrons à présent la distributivité à gauche de la multiplication c'est-à-dire

$$\forall\, (\ell,n,m) \in \mathbb{N}^3, \qquad (\ell+m)n = \ell n + mn\,.$$

Pour cela, on considère l'ensemble $\mathrm{D} = \{n \in \mathbb{N}, (\ell+m)n = \ell n + mn\}$. Vérifions que $0 \in \mathrm{D}$. On a $(\ell+m)0 = 0$ par définition de $(\ell+m)\times$. De même, on a $\ell 0 = 0$ et $m0 = 0$. Comme $0+0 = 0$ (puisque 0 est élément neutre pour $+$). On en déduit que $0 \in \mathrm{D}$. Montrons à présent que si $n \in \mathrm{D}$ alors $\mathrm{S}(n) \in \mathrm{D}$. Par définition de la la multiplication par $\ell + m$, on a

18. Cette dernière propriété signifie que si $m \neq 0$ alors $\mu_m(n) = \mu_m(p)$ implique $n = p$

$$(\ell + m)(\mathrm{S}(n)) = (\ell + m)n + (\ell + m)\,.$$

Par ailleurs comme $n \in \mathrm{D}$, on a $(\ell + m)n = \ell n + mn$. La commutativité et l'associativité de $+$ donnent alors

$$(\ell + m)(\mathrm{S}(n)) = (\ell n + \ell) + (m\ell + m)\,.$$

Les définitions de $\ell\times$ et $m\times$ donnent alors

$$(\ell n + \ell) + (m\ell + m) = \ell\mathrm{S}(n) + m\mathrm{S}(n)\,.$$

et ainsi $\mathrm{S}(n) \in \mathrm{D}$. La propriété (iii) de la définition (1) assure alors que $\mathrm{D} = \mathbb{N}$ ce qu'on souhaitait démontrer.

Montrons à présent l'associativité de la multiplication c'est-à-dire

$$\forall\,(\ell, m, n) \in \mathbb{N}^3, \quad (\ell \times m) \times n = \ell \times (m \times n)$$

On considère l'ensemble $\mathrm{E} = \{n \in \mathbb{N}, \quad \ell(mn) = (\ell m)n\}$. Montrons que $0 \in \mathrm{E}$. On a $\ell(m0) = \ell 0 = 0$ (la première égalité provient que fait que $m0 = 0$ et la deuxième du fait que $m0 = 0$) et $(\ell m)(0) = 0$ par définition de la multiplication par ℓm. On suppose que $n \in \mathrm{E}$. Montrons que $\mathrm{S}(n) \in \mathrm{E}$. On a $\ell(m\mathrm{S}(n)) = \ell(mn + m)$ par définition de la $m\times$. La distributivité à droite montrée précédemment assure alors que

$$\ell(m\mathrm{S}(n)) = \ell(mn + m) = \ell(mn) + \ell m$$

Par ailleurs, on a $(\ell m)\mathrm{S}(n) = (\ell m)n + \ell m$. Comme $n \in \mathrm{E}$, on en déduit que $\ell(mn) = (\ell m)n$ et donc $\ell(m\mathrm{S}(n)) = (\ell m)\mathrm{S}(n)$. Ainsi $\mathrm{S}(n) \in \mathrm{E}$. La propriété (iii) de la définition (1) assure alors que $\mathrm{E} = \mathbb{N}$ et donc la loi $\times$ est associative.

Passons à présent à la commutativité de la multiplication. Là encore, on voit que c'est une propriété loin d'être évidente qui va reposer sur les propriétés déjà démontrées de la multiplication. On considère l'ensemble $\mathrm{F} = \{n \in \mathbb{N}, mn = nm\}$. On a vu que $0 \in \mathrm{F}$ puisque 0 est absorbant pour $\times$. On suppose que $n \in \mathrm{F}$. Montrons que $\mathrm{S}(n) \in \mathrm{F}$. On a $m\mathrm{S}(n) = mn + m$. Par ailleurs, $\mathrm{S}(n)m = (n + 1)m$. La distributivité à gauche assure alors que $\mathrm{S}(n)m = nm + 1m$. Comme 1 est élément neutre pour $\times$, on a $1m = m$ et donc $m\mathrm{S}(n) = \mathrm{S}(n)m$. Ainsi $\mathrm{S}(n) \in \mathrm{F}$ et la propriété (iii) de la définition (1) assure alors que $\mathrm{F} = \mathbb{N}$. La loi $\times$ est commutative.

On suppose que $mn = 0$. On suppose que $n \neq 0$. D'après la remarque 2, il existe n' tel que $n = \mathrm{S}(n')$. On a alors $mn = m\mathrm{S}(n') = mn' + m = 0$. La proposition 9 indique alors que $m = 0$.

On suppose que $mn = 1$. On en déduit que $m \neq 0$ et $n \neq 0$ (puisque 0 est absorbant pour $+$). Ainsi, il existe $m' \in \mathbb{N}$ tel que $\mathrm{S}(m') = m$ et $n' \in \mathbb{N}$ tel que $\mathrm{S}(n') = n$. On a alors $mn = m\mathrm{S}(n') = mn' + m = mn' + m' + 1 = \mathrm{S}(mn' + m') = 1 = \mathrm{S}(0)$. L'injectivité de S assure alors que $mn' + m' = 0$. D'après la proposition 9, on en déduit que $mn' = 0$ et $m' = 0$. Ainsi $m = 1$. On en déduit que $mn' = 1n' = n' = 0$ puisque 1 est élément neutre pour $\times$. Ainsi $n = 1$.

Intéressons-nous à présent aux relations entre la multiplication et l'ordre. On suppose que $m \neq n$. On va montrer que $mp \leqslant np$ pour tout $p \in \mathbb{N}$. Par définition, il existe $a \in \mathbb{N}$ tel que $n = m + a$. On a alors $np = mp + ap$ par distributivité à gauche de la multiplication. Ainsi $np \geqslant mp$.

On considère à présent $p \in \mathbb{N} \setminus \{0\}$ et $(m, n) \in \mathbb{N}^2$ tel que $mp \leqslant np$. On raisonne par l'absurde pour montrer que $m \leqslant n$. Si ce n'est pas le cas, on a $n < m$ et il existe donc $a \neq 0$ tel que $m = n + a$. On a alors, toujours par distributivité à gauche de la multiplication, $mp = np + ap$. Mais comme $a \neq 0$ et $p \neq 0$, on a $ap \neq 0$ (c'est l'une des propriétés montrées ci-dessus). On en déduit que $mp > np$ (par régularité pour $+$ de np) ce qui est absurde.

On en déduit alors, le dernier point manquant : si $p \in \mathbb{N} \setminus \{0\}$ alors p est régulier pour $\times$. En effet, si $pm = pn$ alors on a, à la fois $pm \leqslant pn$ et $pn \leqslant pm$ et donc, grâce à ce qu'on vient de démontrer $m \leqslant n$ et $n \leqslant m$ c'est-à-dire $m = n$.

1.4.2 L'exponentiation

Proposition-Définition 15 – Définition de l'exponentiation. Soit $m \in \mathbb{N}$ et μ_m l'application qui consiste à multiplier par m un entier. Il existe une unique application : $\mathbb{N} \to \mathbb{N}$ telle que

(i) $p_m(0) = 1$;
(ii) $p_m(\mathrm{S}(n)) = mp_m(n)$ pour tout $n \in \mathbb{N}$.

Preuve. On applique le théorème 5 avec $\mathrm{E} = \mathbb{N}$, $f = \mu_m$ et $e = 1$.

Notation 16 – notation multiplicative. Plutôt que la notation $p_m(n)$, on notera souvent $p_m(n) = m^n$. On prendra bien garde au sens de ces notations, surtout tant que les propriétés de l'exponentiation n'auront pas été montrées.

Proposition 17 On a les propriétés suivantes

(i) $\forall n \in \mathbb{N}, \quad n^0 = 1,\ n^1 = n,\ 1^n = 1$;

(ii) $\forall n \in \mathbb{N} \setminus \{0\}, \quad 0^n = 0$ et $0^0 = 1$;

(iii) $\forall (\ell, m, n) \in \mathbb{N}^3, \quad n^{\ell+m} = n^\ell \times n^m$;

(iv) $\forall (\ell, m, n) \in \mathbb{N}^3, \quad (n^\ell)^m = n^{\ell m}$;

(v) $\forall (\ell, m, n) \in \mathbb{N}^3, \quad (nm)^\ell = n^\ell m^\ell$.

(vi) On a ($m^n = 1$ implique $n = 0$ ou $m = 1$) et ($m^n = 0$ implique $n \neq 0$ et $m = 0$).

Preuve. La relation $n^0 = 1$ provient de la définition.

Par ailleurs, par définition, on a $n^1 = n \times n^0 = n \times 1 = n$, la dernière égalité provenant du fait que 1 est élément neutre pour la multiplication.

On considère l'ensemble $\mathrm{A} = \{n \in \mathbb{N}, 1^n = 1\}$. D'après ce qui précède, on a $0 \in \mathrm{A}$. De plus, si $n \in \mathrm{A}$ alors $1^{\mathrm{S}(n)} = 1 \times 1^n = 1^n$ puisque 1 est élément neutre pour $\times$. Comme $n \in \mathrm{A}$, on obtient que $1^{\mathrm{S}(n)} = 1^n = 1$ et donc $\mathrm{S}(n) \in \mathrm{A}$. Ainsi $\mathrm{A} = \mathbb{N}$.

On a $0^0 = 1$ par définition. Si $n \in \mathbb{N} \setminus \{0\}$ il existe, d'après 2, m tel que $n = \mathrm{S}(m)$. On a ainsi $0^n = 0 \times 0^m$ et donc $0^n = 0$ puisque 0 est un élément absorbant pour $\times$.

On définit $\mathrm{B} = \{\ell \in \mathbb{N},\ n^{\ell+m} = n^\ell \times n^m\}$. Montrons que $0 \in \mathrm{B}$. On a $0+m = 0$ et donc $n^{\ell+m} = n^m$. Par ailleurs, $n^0 = 1$ et donc $n^0 \times n^m = 1 \times n^m = n^m$. Ainsi $0 \in \mathrm{B}$. Supposons que $\ell \in \mathrm{B}$ et montrons que $\mathrm{S}(\ell) \in \mathrm{B}$. On a $\mathrm{S}(\ell) + m = \mathrm{S}(\ell + m)$ et donc $n^{\mathrm{S}(\ell)+m} = n^{\mathrm{S}(\ell+m)} = n \times n^{\ell+m}$. Comme $\ell \in \mathrm{B}$, on obtient $n \times (n^\ell n^m)$. L'associativité de $\times$ assure alors que $n^{\mathrm{S}(\ell)+m} = (n \times n^\ell)n^m = n^{\mathrm{S}(\ell)}n^m$. Ainsi $\mathrm{S}(\ell) \in \mathrm{B}$. On en déduit que $\mathrm{B} = \mathbb{N}$ ce qui prouve la relation (iii).

On considère $\mathrm{C} = \{m \in \mathbb{N},\ (n^\ell)^m = n^{\ell m}\}$. Montrons que $0 \in \mathrm{C}$. On a $n^{\ell 0} = 1$ par définition et, comme $\ell 0 = 0$, on a $n^{\ell 0} = 1$. Ainsi $0 \in \mathrm{C}$. Montrons que si $m \in \mathrm{C}$ alors $\mathrm{S}(m) \in \mathrm{C}$. Par définition, on a $(n^\ell)^{\mathrm{S}(m)} = n^\ell \times (n^\ell)^m$. Comme $m \in \mathrm{C}$, on en déduit que $(n^\ell)^{\mathrm{S}(m)} = n^\ell \times n^{\ell m}$. La relation précédente assure que $(n^\ell)^{\mathrm{S}(m)} = n^{\ell+\ell m}$. Par commutativité de l'addition, $\ell + \ell m = \ell m + \ell = \ell \mathrm{S}(m)$. Ainsi $\mathrm{S}(m) \in \mathrm{C}$ et donc $\mathrm{C} = \mathbb{N}$ ce qui prouve la relation (iv).

On considère $\mathrm{D} = \{\ell \in \mathbb{N}, (nm)^\ell = n^\ell m^\ell\}$. Montrons que $0 \in \mathrm{D}$. Par définition, on a $(nm)^0 = 1$, $n^0 = 1$ et $m^0 = 1$. Comme $1 \times 1 = 1$, on en déduit que $0 \in \mathrm{D}$. Supposons que $\ell \in \mathrm{D}$. Montrons que $\mathrm{S}(\ell) \in \mathrm{D}$. Par définition, on a $(nm)^{\mathrm{S}(\ell)} = (nm) \times (nm)^\ell$. Comme $\ell \in \mathrm{D}$, on obtient par associativité et commutativité de la multiplication $(nm)^{\mathrm{S}(\ell)} = (n \times n^\ell) \times (m \times m^\ell)$. Or, par définition, on a $(n \times n^\ell) = n^{\mathrm{S}(\ell)}$ et $(m \times m^\ell) = m^{\mathrm{S}(\ell)}$. Ainsi $\mathrm{S}(\ell) \in \mathrm{D}$ et donc $\mathrm{D} = \mathbb{N}$. On obtient bien la relation (v).

Si $m^n = 1$ et $n \neq 0$ alors il existe n' tel que $n = \mathrm{S}(n')$. Ainsi $m^n = m \times m^{n'} = 1$. La proposition 14 assure alors que $m = 1$.

Si $m^n = 0$, on a $n \neq 0$ car $m^0 = 1$. De plus, si $m \neq 0$ alors $m \geqslant 1$. On considère alors $\mathrm{E} = \{n \in \mathbb{N}, m^n \geqslant 1\}$. On a $0 \in \mathrm{E}$ par définition de m^0 et si $n \in \mathrm{E}$ alors, comme $m^n \geqslant 1$, on a $m \times m^n \geqslant m$ d'après la proposition 14 et donc $m^{n+1} \geqslant m \geqslant 1$. Ainsi $\mathrm{S}(n) \in \mathrm{E}$ et $\mathrm{E} = \mathbb{N}$ et donc $m^n \neq 0$ pour tout n. Finalement, $m = 0$.

1.5 Application de la récurrence à l'étude des entiers

Cette section utilise un certain nombre de définitions qui ne sont pas rappelées.

Proposition 18 – Décomposition en nombre premier. Soit $n \in \mathbb{N} \setminus \{0\}$. Il existe un entier r et des nombres premiers $p_1, \ldots, p_r$ tel que $n = p_1 \cdots p_r$.

Preuve. On considère l'ensemble A des entiers $n \in \mathbb{N} \setminus \{0\}$ qui ne s'écrivent pas comme un produit de facteurs premiers. Si cet ensemble A est non vide, il possède un plus petit élément n.

Évidemment, n n'est pas premier, sinon on aurait la décomposition souhaitée avec $r = 1$ et $n = p_1$. Comme n n'est pas premier, il existe $n_1, n_2 \in \mathbb{N} \setminus \{0, 1\}$ tels que $n = n_1 \times n_2$. En particulier, on a $n_1 < n$ et $n_2 < n$.

Par minimalité de n, on en déduit qu'il existe des entiers r et s et des nombres premiers $p_1, \ldots, p_r$, $q_1, \ldots, q_s$ tels que $n_1 = p_1 \cdots p_r$ et $n_2 = q_1 \cdots q_s$. On en déduit que $n = n_1 n_2 = p_1 \cdots p_r q_1 \cdots q_s$ ce qui

contredit le fait que $n \in \mathrm{A}$. Ainsi A est vide et on obtient la proposition souhaitée.

1.5.1 Décomposition additive

Proposition 19 Soit $(u_n)_{n\in\mathbb{N}}$ une suite d'entiers strictement croissante. Alors, pour tout $m \in \mathbb{N}$, il existe $n \in \mathbb{N}$ tel que $u_n > m$.

Preuve. Par l'absurde, si ce n'était pas le cas, on aurait pour tout $n \in \mathbb{N}$, $u_n \leqslant m$. Ainsi l'ensemble $\mathrm{U} = \{u_n,\ n \in \mathbb{N}\}$ serait borné. Par la propriété (iii) de la définition (2), on en déduit que U a un plus grand élément. Il existe donc n_0 tel que u_{n_0} est le plus grand élément de U. Mais comme u est strictement croissante, on a $u_{n_0+1} > u_{n_0}$ ce qui est une contradiction.

Exemple 20 – Les multiples d'un entier. On fixe $m \in \mathbb{N} \setminus \{0\}$. La suite $(nm)_{n\in\mathbb{N}}$ des multiples de m est une suite strictement croissante.

En effet, d'après la proposition 14, si $n < n'$ alors $nm \leqslant n'm$. De plus, comme $m \neq 0$ si $nm = n'm$ alors $n = n'$. NON. Ainsi $nm < n'm$.

Application 21 – Division euclidienne. Soit $b \in \mathbb{N} \setminus \{0,1\}$. Soit $n \in \mathbb{N}$. Il existe un unique couple $(q,r) \in \mathbb{N}^2$ vérifiant les deux relations suivantes :

(i) $n = bq + r$;
(ii) $0 \leqslant r < b$.

On dit que q est le *quotient de la division euclidienne de n par b* et r est le *reste de la division euclidienne de n par b*.

Montrons ce résultat. On considère l'ensemble A des entiers qui ne vérifient pas l'existence d'une telle écriture sous la forme $bq + r$ avec $0 \leqslant r < b$. On suppose que A est non vide. Il admet donc un plus petit élément. On le note n.

Comme $b \neq 0$, la suite des multiples de b est strictement croissante (voir l'exemple 20. La proposition 19 assure alors qu'il existe m tel que $mb > n$. Ainsi, $\mathrm{B} = \{m \in \mathbb{N}, mb > n\}$ est non vide. Il admet donc un plus petit élément d'après le point (ii) de la définition 3. Évidemment ce plus petit élément ne peut être 0 puisque sinon $0b = 0 > n$. NON. Ainsi, ce plus petit élément est supérieur à 1. On note q l'élément qui précède le plus petit élément de B. On a donc $qb \leqslant n < (q+1)b$. La définition de l'ordre assure alors qu'il existe r tel que $n = qb + r$ et les propriétés de l'ordre relativement à $+$ (proposition-définition 10 montrent que $0 \leqslant r < b$. Ainsi $n \in \mathrm{A}$ ce qui contredit la définition de n.

Reste à montrer l'unicité d'une telle décomposition. On suppose que $bq+r = bq'+r'$ avec $0 \leqslant r < b$ et $0 \leqslant r' \leqslant b$. On suppose $q \neq q'$. Par exemple $q < q'$. On a alors $bq + r < bq + b = b(q+1)$. Mais $(q+1) \leqslant q'$. Ainsi $bq + r < (q+1)b \leqslant q'b \leqslant q'b + r'$.

Quelques commentaires. L'écriture sous la forme $n = bq + r$ n'est évidemment pas unique (par exemple $20 = 2 \times 7 + 6 = 1 \times 7 + 13$. Ainsi, la contrainte portant sur r $(0 \leqslant r < b)$ est indispensable pour obtenir la propriété d'unicité de l'écriture.

Si elle n'est pas formulée de la sorte, la démonstration ci-dessus indique cependant un algorithme pour déterminer les entiers q et r. On calcule les multiples successifs de b dès qu'on dépasse n, on s'arrête et on revient en arrière pour prendre le multiple précédent.

L'énoncé et démonstration proposés s'appliquent évidemment au cas où $b = 1$. Mais l'énoncé est alors sans intérêt puisque r est nécessairement nul et l'écriture proposée est $n = 1 \times n + 0$.

Exercice 1 – Python-Scratch. Programmer le calcul de division euclidienne de n par b reposant sur la démonstration ci-dessus.

Exemple 22 – Les puissances d'un entier. On fixe $m \in \mathbb{N} \setminus \{0,1\}$. La suite $(m^n)_{n\in\mathbb{N}}$ des puissances de m est une suite strictement croissante.

En effet, on a $m > 1$. Comme $m^n \neq 0$ (voir le point (vi) de la proposition 17), on en déduit $m^{n+1} = m \times m^n > m^n$ grâce à la proposition 14.

Application 23 – Écriture en base b. Soit $b \in \mathbb{N} \setminus \{0,1\}$ et $n \in \mathbb{N} \setminus \{0\}$. Il existe un unique entier r et une unique famille $(a_0, \ldots, a_r) \in \{0, \ldots, b-1\}^{r+1}$ vérifiant $n = a_0 b^0 + \cdots + a_r b^r$ et $a_r \neq 0$.

Cette écriture s'appelle la *décomposition de n en base b*. La famille $(a_0, \ldots, a_r)$ s'appelle les *chiffres de l'écriture de n en base b*.

Montrons ce résultat. Pour cela, on considère l'ensemble A des entiers non nuls qui n'ont pas d'écriture sous cette forme. On suppose que A est non vide. Il admet donc un plus petit élément n.

Comme $b \geqslant 2$, la suite des puissances de b est strictement croissante. La proposition 19 assure alors qu'il existe un entier m tel que $b^m > n$. Ainsi, $\mathrm{B} = \{m \in \mathbb{N}, b^m > n\}$ est non vide. Il admet donc un plus petit élément d'après le point (ii) de la définition 3. Évidemment ce plus petit élément ne peut être 0 puisque sinon $b^0 = 1 > n$ et donc $n = 0$, cas qu'on a exclu. Ainsi, ce plus petit élément de B est supérieur à 1. On note r l'élément qui précède le plus petit élément de B. On a donc $b^r \leqslant n < b^{r+1}$.

On considère alors l'entier $n - b^r$. S'il est nul alors $n = b^r$ et on a la forme souhaitée. Sinon $n - b^r \neq 0$ et n'est pas dans A puisque $n - b^r < n$. Ainsi, il existe $s \in \mathbb{N}$ et $(b_0, \dots, b_s) \in \{0, \dots, b-1\}^{s+1}$ tel que $n - b^r = b_0 b^0 + \cdots + b_s b^s$ et $b_s \neq 0$. On a $s \leqslant r$. En effet, sinon, $b_0 b^0 + \cdots + b_s b^s \geqslant b_s b^s \geqslant b^{r+1} > n$. NON.

Si $s < r$, on pose $a_i = b_i$ pour $0 \leqslant i \leqslant s$, $a_i = 0$ pour $s < i < r-1$ et $a_r = 1 \neq 0$ pour obtenir la forme voulu pour n.

Si $s = r$, on a alors $b_r \leqslant b - 2$. En effet, si $b_r = b - 1$, on a

$$n = b^r + b_0 b^0 + \cdots + b_{r-1} b^{r-1} + (b-1) b^r = b_0 b^0 + \cdots + b_{r-1} b^{r-1} + b^{r+1} \geqslant b^{r+1}\,,$$

ce qui contredit la définition de r. On obtient alors l'écriture souhaitée en posant, pour $0 \leqslant i \leqslant r-1$, $a_i = b_i$ et $a_r = 1 + b_r \neq 0$ et $a_r \leqslant b - 1$ puisque $b_r \leqslant b - 2$.

Passons à l'unicité. La preuve repose de façon essentielle sur la relation $(b-1)\sum_{i=0}^{r} b^i = b^{r+1} - 1$ [19].

Là encore, on considère l'ensemble B des entiers pour lesquels il existe plusieurs écritures différentes. On suppose qu'il est non vide et on considère n le plus petit élément.

On considère deux écritures $n = a_0 b^0 + \cdots + a_r b^r$ et $n = a'_0 b^0 + \cdots + a'_s b^s$ avec $(a_0, \dots, a_r) \in \{0, \dots, b-1\}^{r+1}$ et $(a'_0, \dots, a'_s) \in \{0, \dots, b-1\}^{s+1}$ et $a_r \neq 0$ et $a'_s \neq 0$.

On commence par montrer que $s = r$. Par l'absurde, si $s < r$, on a $n = a'_0 b^0 + \cdots + a'_s b^s \leqslant (b-1)\sum_{i=0}^{s} b^i \leqslant b^{s+1} < b^r$, alors que $n \geqslant b_r b^r \geqslant b^r$ car $b_r \neq 0$. NON [20].

Montrons à présent que $a_r = a'_r$. Par l'absurde, si $a'_r < a_r$. On a alors

$$n = a'_r b^r + a'_{r-1} b^{r-1} \cdots a'_0 \leqslant a'_r b^r + (b-1)\sum_{i=0}^{r-1} b^i \leqslant a'_r b^r + b^r - 1 < (a'_r + 1) b^r \leqslant a_r b^r \leqslant n.$$

On obtient ainsi une contradiction [21].

On considère alors $m = n - a_r b^r$. Si $m = 0$ alors nécessaire $a_i = a'_i = 0$ pour tout $0 \leqslant i \leqslant r-1$ et on a l'égalité souhaitée. Si $m \neq 0$ alors il existe $i, j \in \mathbb{N}$ tel que $a_i \neq 0$ et $a'_j \neq 0$. On considère alors r' le plus grand i tel que $a_i \neq 0$ et s' le plus grand j tel que $a'_j \neq 0$. On a alors les décompositions

$$m = \sum_{i=0}^{r'} a_i b^i = \sum_{j=0}^{s'} a'_i b^i$$

Comme $n - a_r b^r < n$, $n - a_r b^r$ admet une unique décomposition sous la forme souhaitée. Ainsi $s' = r'$ et $a_i = a'_i$ pour $0 \leqslant i \leqslant r'$. De plus, comme $a_i = a'_i = 0$ pour $r' < i < r$, on obtient l'égalité de l'écriture ce qui contredit la définition de n et l'ensemble A est vide.

Quelques commentaires. Pour $n = 0$, on convient de choisir $r = 0$ et $a_0 = 0$ mais on ne peut alors pas assurer $a_r \neq 0$. On peut aussi convenir que la somme est vide.

Si elle n'est pas formulée de la sorte, la démonstration ci-dessus indique cependant un algorithme pour déterminer la décomposition. On calcule les puissances successives de b et dès qu'on dépasse n, on s'arrête et on revient en arrière. On recommence avec $n - b^r$.

Exercice 2 – Python-Scratch. Programmer le calcul de la décomposition en base b reposant sur la démonstration précédente.

---

19. Cette relation sur la somme des termes d'une suite géométrique est au programme de Première, il est indispensable de savoir la connaître et de savoir la démontrer. En voici une démonstration sous une forme légèrement différente :

$$1 + b\sum_{i=0}^{r} b^i = 1 + \sum_{i=0}^{r} b^{i+1} = 1 + \sum_{i=1}^{r+1} b^i = \sum_{i=0}^{r+1} b^i = b^{r+1} + \sum_{i=0}^{r} b^i\,.$$

20. De façon heuristique, les termes jusqu'au rang $s < r$ ne peuvent apporter un terme de rang r.

21. De façon heuristique, en rendant maximaux les termes de rang inférieur à $r-1$, on n'arrive pas à obtenir quelque chose de la taille de b^r pour commencer l'écart entre a'_r et a_r.

Exemple 24 – La suite de Fibonacci. On définit une suite par récurrence via $\mathrm{F}_0 = 0, \mathrm{F}_1 = 1$ et pour tout $n \in \mathbb{N}$, $\mathrm{F}_{n+2} = \mathrm{F}_{n+1} + \mathrm{F}_n$. La suite $(\mathrm{F}_n)_{n\in\mathbb{N}}$ s'appelle la suite de Fibonacci.

A priori, le théorème 5 n'assure pas directement l'existence de la suite $(\mathrm{F}_n)_{n\in\mathbb{N}}$ puisqu'il ne concerne que les récurrences à un pas. Pour remédier à cela, l'idée des remplacer la suite d'entiers $(\mathrm{F}_n)_{n\in\mathbb{N}}$ par une suite de couple d'entiers $(\mathrm{F}_n, \mathrm{F}_{n+1})_{n\in\mathbb{N}}$. Pour mettre cela au propre, on considère $\mathrm{E} = \mathbb{N} \times \mathbb{N}$, $e = (0,1)$ et $f\colon \mathrm{E} \to \mathrm{E}$ définie par $(a,b) \mapsto (b, a+b)$. L'application du théorème 5 permet alors la construction de la suite de Fibonacci. Cette idée se retrouve dans l'étude des équations différentielles pour transformer une équation différentielle du second ordre en une équation différentielle du premier ordre.

La suite $(\mathrm{F}_n)_{n\in\mathbb{N}}$ est croissante. En effet, par définition de la relation d'ordre $\mathrm{F}_{n+2} \geqslant \mathrm{F}_{n+1}$ pour tout $n \in \mathbb{N}$ et par ailleurs $\mathrm{F}_1 \geqslant \mathrm{F}_0$.

On en déduit que pour tout $n \geqslant 1$, $\mathrm{F}_n \geqslant \mathrm{F}_1$. Ainsi $\mathrm{F}_n > 0$ pour tout $n \geqslant 1$. On en déduit que pour tout $n \geqslant 1$, $\mathrm{F}_{n+2} \geqslant \mathrm{F}_{n+1}$. Ainsi la suite de Fibonacci est strictement croissante à partir du rang $n = 2$.

Exercice 3 – Théorème de Zeckendorf. Voir [ZEK]. Démontrer le résultat suivant : $n \in \mathbb{N} \setminus \{0\}$. Il existe un unique entier r et une unique famille $(i_0, \ldots, i_r) \in (\mathbb{N} \setminus \{0,1\})^{r+1}$ vérifiant $n = \mathrm{F}_{i_0} + \cdots + \mathrm{F}_{i_r}$ et $i_j + 2 \leqslant i_{j+1}$ pour tout $j \in \{0, \ldots, r-1\}$.

Chapitre 2

Les entiers relatifs

Les entiers naturels forment un système de nombres avec de nombreuses propriétés. Ils recèlent cependant certaines insuffisances. On peut les exprimer en terme d'ensembles des solutions d'une équations : ainsi les équations $x+n=m$ n'ont pas nécessairement de solutions (par exemple $x+3=2$) ; de même, les équations $nx=p$ n'ont pas nécessairement de solutions (par exemple $2x=3$). De façon précise, l'équation $x+n=m$ n'a de solution que si $m \geqslant n$ (c'est même la définition de l'ordre) et l'équation $nx=p$ n'a de solution que si p est un multiple de n. « Il manque donc des nombres ». Il s'agit donc, à partir des nombres existants, de construire de nouveaux nombres qui vont pallier ces manques. École et mathématiques choisissent là deux chemins différents.

À l'école, on étudie en premier lieu les fractions (d'entiers positifs) en CM1 avant d'introduire les nombres négatifs en cinquième. Cela suit d'ailleurs, l'évolution historique de l'introduction des nombres : les mathématiciens grecs manipulaient des rapports de grandeurs (sans les considérer comme des nombres) et le concept de nombres négatifs a été bien plus tardif.

Les mathématiques actuelles choisissent, le plus fréquemment, de construire d'abord les entiers relatifs $\mathbb{Z}$ pour obtenir une structure algébrique supplémentaire (celle d'anneaux) et ensuite de passer aux fractions pour construire $\mathbb{Q}$ le corps des nombres rationnels. C'est le chemin que nous suivrons. Ainsi, l'idée est d'abord d'ajouter les solutions des équations de la forme $x+n=m$ quand $n \geqslant m$ (pour construire $\mathbb{Z}$) avant de passer aux équations de la forme $nx=p$ (pour construire $\mathbb{Q}$, en prenant n et p dans $\mathbb{Z}$).

2.1 Construction des entiers relatifs

La construction explicite de $\mathbb{Z}$ peut sembler très abstraite, tentons d'en donner quelques explications heuristiques. On part du constat qu'il faut inventer des nouveaux objets mathématiques (des nouveaux nombres) parce qu'il y a des équations sans solutions ($x+3=2$ par exemple). Quels vont être ces nouveaux objets mathématiques ? L'idée fondamentale est alors de dire que ce nouvel objet mathématique va justement être l'équation en question : on remplace la solution de l'équation par l'équation elle-même ! Bien entendu, en faisant cela, on a beaucoup trop d'objets : l'équation $x+4=3$ et l'équation $x+3=2$ sont des équations distinctes alors qu'une fois construit $\mathbb{Z}$, elles auront la même solution. Comme ce qui nous intéresse est l'ensemble des solutions des équations et pas les équations en elle-même, il faut identifier les équations. Par exemple, comme tout élément $p \in \mathbb{N}$ est régulier, les équations $x+n=m$ et $x+n+p=m+p$ sont équivalentes (c'est-à-dire de façon intuitive ont les mêmes solutions) : on les identifie. L'étape suivante est donc, étant donné deux équations, de trouver une condition qui permet de les identifier. On considère donc $x+n=m$ et $x+n'=m'$ qu'on suppose équivalente. L'ordre sur $\mathbb{N}$ étant total, on peut supposer par exemple $m' \geqslant m$. On peut donc supposer qu'il existe $a \in \mathbb{N}$ tel que $m+a=m'$. Comme la première équation $x+n=m$ est équivalente à $x+n+a=m+a=m'=x+n'$, on obtient que $n+a=n'$ (on imagine que notre nouveau nombre est régulier pour $+$). Lorsque deux équations sont équivalentes, on peut passer de la première (celle où le second membre est le plus petit) à la deuxième en ajoutant un même nombre au deux membres. Peut-on traduire directement cette propriété uniquement sur les couples (m,n) et (m',n'). Si les équations sont équivalentes, on a alors $m+n'=m+n+a=m'+n$. Inversement, supposons que $m+n'=m'+n$ et $m' \geqslant m$. Il existe donc $a \in \mathbb{N}$ tel que $m'=m+a$ et donc $m+n'=m+a+n$. Comme m est régulier, on obtient $n'=a+n$ et les équations $x+n=m$ et $x+n'=m'$ sont bien équivalentes. On a ainsi trouvé notre condition. Il ne reste plus qu'à remarquer que se donner l'équation $x+n=m$ revient

simplement à se donner le couple (m,n)([1]. On arrive ainsi la proposition-définition suivante.

Proposition-Définition 25 – Les entiers relatifs. Sur l'ensemble $\mathbb{N}\times\mathbb{N}$, la relation $\mathscr{R}$ définie par

$$(m,n)\mathscr{R}(m',n') \quad \Longleftrightarrow \quad m+n'=m'+n$$

est une relation d'équivalence. On note $\mathbb{Z}$ l'ensemble quotient $(\mathbb{N}\times\mathbb{N})/\mathscr{R}$ et on l'appelle l'ensemble des entiers relatifs.

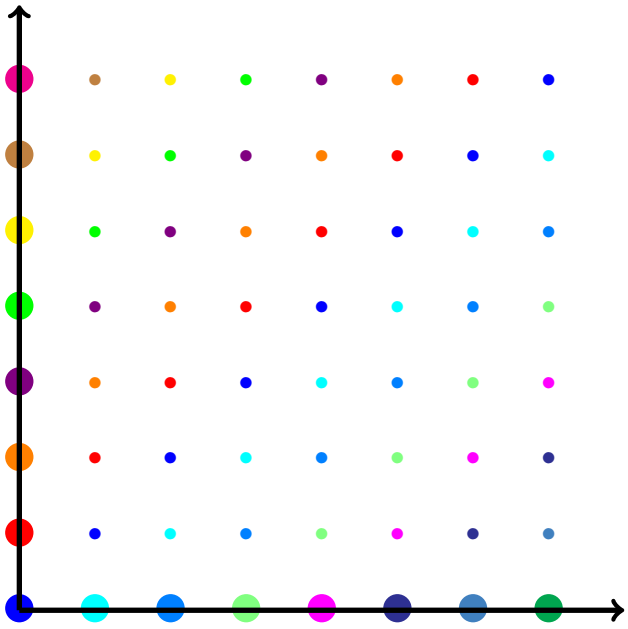
On note $\pi\colon \mathbb{N}\times\mathbb{N}\to\mathbb{Z}$ la surjection canonique c'est-à-dire l'application qui au couple (m,n) associe sa classe d'équivalence[2].

Preuve. Montrons que $\mathscr{R}$ est une relation d'équivalence. On a évidemment $m+n=m+n$ donc $(m,n)\mathscr{R}(m,n)$ et la relation $\mathscr{R}$ est réflexive.

On suppose que $(m,n)\mathscr{R}(m',n')$ c'est-à-dire $m+n'=m'+n$. Montrons que $(m',n')\mathscr{R}(m,n)$. Il s'agit de vérifier que $m'+n=m+n'$ ce qui découle de l'égalité précédente. Ainsi $\mathscr{R}$ est symétrique.

Enfin, on suppose que $(m,n)\mathscr{R}(m',n')$ et $(m',n')\mathscr{R}(m'',n'')$. On veut montrer que $\mathscr{R}$ est transitive. Il s'agit donc de montrer que $m+n''=m''+n$. Or on sait que $m+n'=m'+n$ et $m'+n''=m''+n'$. En ajoutant n'' à l'égalité $m+n'=m'+n$, on obtient $m+n'+n''=m'+n+n''$, l'associativité et commutativité de $+$ dans $\mathbb{N}$ donnent alors $m+n'+n''=m''+n'+n$ grâce à l'égalité $m'+n''=m''+n'$. Par commutativité et associativité, on conclut à l'égalité $m+n''=m''+n$ en utilisant la régularité de n' pour $+$.

On peut représenter l'ensemble $\mathbb{N}\times\mathbb{N}$ dans le plan. Sur la représentation ci-dessous sont indiqués d'une même couleur les couples équivalents. Les classes d'équivalences des éléments $\mathbb{N}\times\mathbb{N}$ sont les parties de $\mathbb{N}\times\mathbb{N}$ qui sont contenues dans les droites d'équations $y=x+\ell$ avec $\ell\in\mathbb{Z}$ puisque $(m,n)\mathscr{R}(m',n')$ si et seulement si $n-m=n'-m'$ (la différence entre l'ordonnée et l'abscisse est constante sur les classes d'équivalence). Bien entendu, cette interprétation n'est possible qu'une fois qu'on aura définit la notion $n-m$ pour n'importe quel couple d'éléments de $\mathbb{N}$ c'est-à-dire qu'on aura étudier largement $\mathbb{N}$.



2.1.1 Lien entre les entiers naturels et les entiers relatifs

Maintenant qu'on a construit l'ensemble $\mathbb{Z}$, il s'agit de vérifier qu'il a bien les propriétés attendus. En particulier, on va vérifier que cet ensemble permet bien de définir des nouveaux nombres, qu'il « contient » les anciens[3]. On va ensuite construire sur $\mathbb{Z}$ de nouvelles opérations (qu'on va encore noté $+$ et $\times$) qui vont étendre celles de $\mathbb{N}$. De même, on a étendre la relation d'ordre à $\mathbb{Z}$ tout entier.

1. On aurait plus faire la convention que ça revient à se donner le couple (n,m) pour respecter l'ordre dans lequel apparaissent les symboles dans l'équation mais il s'avère que cette deuxième convention est moins pratique pour la suite.
2. Par définition, $\pi(m,n)=\pi(m',n')$ si et seulement si $m+n'=m'+n$.
3. en fait, il ne les contient pas au sens ensembliste mais chaque élément de $\mathbb{N}$ peut bien être vu comme un élément de $\mathbb{Z}$

Proposition 26 – La relation entre $\mathbb{N}$ et $\mathbb{Z}$. L'application

$$i\colon \begin{cases} \mathbb{N} \longrightarrow \mathbb{Z} \\ n \longmapsto \pi(n,0) \end{cases}$$

est injective et permet ainsi d'identifier $\mathbb{N}$ a un sous-ensemble de $\mathbb{Z}$.

Tout élément de $\mathbb{Z}$ a un représentant de la forme $(a,0)$ ou $(0,a)$. De plus, si $a \neq b$ alors $\pi((0,a)) \neq \pi(0,b)$. Enfin, on a $\pi(a,0) = \pi(0,b)$ si et seulement si $a = b = 0$.

Commentaires. Pourquoi est-il normal de penser à cette application ? On a construit $\mathbb{Z}$ en y pensant comme les solutions des équations $x + n = m$. Mais évidemment, l'élément $n \in \mathbb{N}$ est solution de l'équation $x + 0 = n$ qui dans notre construction correspond bien à la classe de l'équation représentée par $(n,0)$.

Par ailleurs, à l'aide de la représentation graphique ci-dessous, la proposition 26 s'interprète en disant que tout élément de $\mathbb{Z}$ a un unique représentant qui situé sur l'axe des abscisses ou des ordonnées et qu'il n'y a un qu'une seule de classe d'équivalence qui a un représentant situé à la fois sur l'axe des ordonnées et sur l'axe des abscisses : ce sont les points matérialisés en gros.

Preuve. On suppose que $i(n) = i(m)$ c'est-à-dire $\pi(n,0) = \pi(m,0)$ ou encore que $n + 0 = m + 0$. Or $n + 0 = n$ et $m + 0 = m$ et donc $m = n$. Ainsi i est bien injective.

Soit $\pi(m,n)$ un élément de $\mathbb{Z}$. Il s'agit de montrer qu'il existe $a \in \mathbb{N}$ tel que $(m,n)\mathscr{R}(a,0)$ ou $(m,n)\mathscr{R}(0,a)$.

On suppose que $m \geqslant n$ alors, par définition de l'ordre, il existe $a \in \mathbb{N}$ tel que $n + a = m = m + 0$. Ainsi $(a,0)\mathscr{R}(m,n)$ par définition de $\mathscr{R}$. Inversement, si $n \geqslant m$ alors par définition de l'ordre il existe $a \in \mathbb{N}$ tel que $m + a = n = n + 0$. Ainsi $(m,n)\mathscr{R}(0,a)$.

Si $\pi(0,a) = \pi(0,b)$ alors $0 + b = 0a$ et donc $a = b$. Enfin si $\pi(0,b) = \pi(a,0)$ alors $0 + 0 = b + a$. Ainsi $a + b = 0$. Or on a vu (voir la proposition 9) que cela implique $a = b = 0$.

2.2 Opération et ordre sur les entiers relatifs

2.2.1 Structure de groupe additif

Proposition 27 – Définition de la loi $+$ sur $\mathbb{Z}$. Il existe une application, notée $+$, de $\mathbb{Z} \times \mathbb{Z}$ dans $\mathbb{Z}$ vérifiant

$$\forall\, (m,n,m',n') \in \mathbb{N}^4, \qquad \pi(m,n) + \pi(m',n') = \pi(m+m', n+n')$$

De plus, l'application $i\colon \mathbb{N} \to \mathbb{Z}$ vérifie $i(n+m) = i(n) + i(m)$ [4] pour tout $n, m \in \mathbb{Z}$.

Le couple $(\mathbb{Z}, +)$ est un groupe abélien d'élément neutre $\pi(0,0)$. L'opposé de $\pi(m,n)$ est $\pi(n,m)$.

Commentaires. Revenons sur la principale difficulté de cette définition de l'addition dans $\mathbb{Z}$. L'idée est la suivante, on prend une classe d'équivalence (si on s'inspire de la représentation ci-dessous, on prend tous les points d'une même couleur) et une autre [5] classe d'équivalence (tous les points d'une autre [6] couleur) et on cherche à ajouter cela. Évidemment, comme cela, on ne sait pas faire grand chose. Alors ce qu'on fait, on choisit un point de la première couleur et on l'ajoute à un point de la deuxième couleur et ça on sait le faire car on sait ajouter des entiers (on ajoute la première coordonnée du premier point avec la première coordonnée du deuxième point, et on fait de même avec les deuxièmes coordonnées). On obtient ainsi un troisième point et donc une troisième couleur. Le problème qui se pose alors est est-ce que cette troisième couleur est toujours la même si je prends une autre point de la première couleur et que je l'ajoute avec un autre point de la deuxième couleur. Si c'est bien le cas, alors, je peux bien définir que la somme de la première couleur avec la deuxième couleur est la troisième couleur. Et ici, c'est bien ce qui se passe. Faites le test : ajouter un point orange à un point bleu ciel donne systématiquement un point rouge. Essayez avec d'autres couleurs.

4. Il faut remarquer que si le symbole $+$ utilisé dans l'égalité est le même dans les deux membres, il ne représente pas le même objet mathématique, le $+$ du membre de gauche est celui qui permet d'ajouter des entiers naturels comme définit dans le chapitre1 et le $+$ du membre de gauche est celui qu'on vient de définir et qui permet d'ajouter les éléments de $\mathbb{Z}$

5. éventuellement la même

6. éventuellement la même

Interprétons la relation $i(n+m)=i(n)+i(m)$: elle signifie que si on ajoute n et m dans $\mathbb{N}$ et qu'ensuite, on envoie le résultat dans $\mathbb{Z}$, on obtient le même résultat qu'en envoyant d'abord n et m dans $\mathbb{Z}$ et en ajoutant leur image. Ainsi finalement les calculs de sommes entre éléments de $\mathbb{N}$ se fait de la même façon dans $\mathbb{Z}$.

Preuve. La première étape est de vérifier que l'application $+$ est bien définie c'est-à-dire de vérifier que si

$$(m,n)\mathscr{R}(m',n') \quad \text{et} \quad (m_1,n_1)\mathscr{R}(m'_1,n'_1) \implies (m+m_1,n+n_1)\mathscr{R}(m'+m'_1,n'+n'_1) \qquad \star$$

Cela se revient à vérifier que $m+m_1+n'+n'_1=m'+m'_1+n+n_1$ sachant que $m+n'=m'+n$ et $m_1+n'_1=m'_1+n_1$. L'associativité et la commutativité de l'addition donne alors le résultat en ajoutant les deux dernières égalités.

Ainsi, l'application $+$ est bien définie.

Vérifions alors les points restants. Soit $m,n\in\mathbb{N}$, on a, d'une part $i(m+n)=\pi(m+n,0)$ et d'autre part $i(m)+i(n)=\pi(n,0)+\pi(m,0)$. Or, par la définition qu'on vient de donner, $\pi(n,0)+\pi(m,0)=\pi(n+m,0+0)=\pi(n+m,0)$. On obtient bien l'égalité voulue.

Assurons à présent que les axiomes de groupes sont vérifiés pour $(\mathbb{Z},+)$.

Commençons par l'associativité. On considère $(m,n,m',n',m'',n'')\in\mathbb{N}^6$. On calcule, en utilisant la définition de l'addition dans $\mathbb{Z}$[7],

$$(\pi(m,n)+\pi(m',n'))+\pi(m'',n'')=\pi(m+m',n+n')+\pi(m'',n'')=\pi((m+m')+m'',(n+n')+n'')$$

$$\pi(m,n)+(\pi(m',n')+\pi(m'',n''))=\pi(m,n)+\pi(m'+m'',n'+n'')=\pi(m+(m'+m''),n+(n'+n''))$$

L'associativité de la loi $+$ de $\mathbb{N}$ permet de conclure puisque $((m+m')+m'',(n+n')+n'')=(m+(m'+m''),n+(n'+n''))$ et donc leur image par π sont aussi égales.

Montrons que $\pi(0,0)$ est l'élément neutre pour $+$. Pour $(m,n)\in\mathbb{N}$, on a

$$\pi(m,n)+\pi(0,0)=\pi(m+0,n+0)=\pi(m,n) \qquad \text{et} \qquad \pi(0,0)+\pi(m,n)=\pi(0+m,0+n)=\pi(m,n)$$

Montrons que la loi $+$ de $\mathbb{Z}$ est commutative. On considère $(m,n,m',n')\in\mathbb{N}^4$, on a

$$\pi(m,n)+\pi(m',n')=\pi(m+m',n+n') \qquad \text{et} \qquad \pi(m',n')+\pi(m,n)=\pi(m'+m,n'+n)$$

La commutativité de la loi $+$ de $\mathbb{N}$ permet de conclure puisque $(m'+m,n'+n)=(m+m',n+n')$ et donc leur image par π sont aussi égales.

Montrons que $\pi(n,m)$ est l'opposé de $\pi(m,n)$. On a

$$\pi(m,n)+\pi(n,m)=\pi(m+n,n+m) \qquad \text{et} \qquad \pi(n,m)+\pi(m,n)=\pi(n+m,m+n)$$

Comme $n+m=m+n$, puisque la loi $+$ de $\mathbb{N}$ est commutative, il suffit, pour conclure de montre que si $a\in\mathbb{N}$ alors $\pi(a,a)=\pi(0,0)$ ce qui s'obtient en appliquant la définition puisque $a+0=0+a=a$. Ainsi on a bien

$$\pi(m,n)+\pi(n,m)=\pi(0,0) \qquad \text{et} \qquad \pi(n,m)+\pi(m,n)=\pi(0,0)\,.$$

Notation 28 – Le signe $-$ et la soustraction. Dans $\mathbb{Z}$, comme pour tout groupe abélien dont la loi est notée $+$, on utilise le signe $-$ pour désigner deux choses différentes. D'une part, c'est la notation qui permet de désigner l'opposée d'un élément : $-x$ désigne l'opposé de x c'est-à-dire l'unique élément y de $\mathbb{Z}$ tel que $x+y$ et $y+x$ soient l'élément neutre de $\mathbb{Z}$.

D'autre part, $-$ désigne une nouvelle application de $\mathbb{Z}\times\mathbb{Z}$ dans $\mathbb{Z}$ définie par

$$\forall\,(x,y)\in\mathbb{Z}, \qquad x-y=x+(-y)\,.$$

Ainsi par définition, dans $\mathbb{Z}$, soustraire c'est ajouter l'opposé !

Ces deux sens et interprétations du signe $-$ sont déjà présents dès la classe de cinquième et ne sont pas sans poser de soucis aux élèves.

Remarque 29 – Retour sur la proposition 26. D'après la proposition 27 et en utilisant la notation 28, on a $\pi(0,a)=-\pi(a,0)=-i(a)$. Avec cette notation, on a alors que $\pi(m,n)=\pi(m,0)+\pi(0,n)=i(m)+(-i(n))=i(m)-i(n)$ pour tout $(m,n)\in\mathbb{Z}$: tout élément de $\mathbb{Z}$ est la différence de deux éléments qui proviennent de $\mathbb{N}$.

7. pour simplifier l'interprétation des calculs, on a noté en rouge la loi $+$ de $\mathbb{Z}$ et en noir, celle de $\mathbb{N}$.

On a même mieux : la proposition 26 se interprète sous la forme $\mathbb{Z} = i(\mathbb{N}) \cup -i(\mathbb{N})$ et $i(\mathbb{N}) \cap -i(\mathbb{N}) = \{0\}$ où ce dernier symbole 0 désigne en fait $\pi(0,0)$ qui est l'élément neutre de $\mathbb{Z}$.

En oubliant de noter i (qui est injective), on retrouve exactement les entiers relatifs qu'on connait $\mathbb{Z} = \mathbb{N} \cup -\mathbb{N}$ et $\mathbb{N} \cap -\mathbb{N} = \{0\}$: un entier relatif est un entier ou l'opposé d'un entier et un entier relatif qui est à la fois un entier naturel et l'opposé d'un entier naturel est forcément nul.

2.2.2 Structure multiplicative

On souhaite maintenant définir une multiplication entre les éléments de $\mathbb{Z}$, multiplication qui prolonge, bien sûr, celle des éléments de $\mathbb{N}$. Une solution, basée sur la remarque 29, serait la suivante : on souhaite définir ce que ça veut dire de multiplier un entier relatif par un autre entier relatif. Une première étape serait de définir ce que cela signifie de multiplier un entier relatif par un entier naturel. Cela peut se faire par addition itérée comme cela a été fait pour $\mathbb{N}$ (voir le processus à la proposition-définition) 12) puis de définir la multiplication d'un entier relatif par l'opposé d'un entier naturel, en se ramenant au cas précédent, en imposant par exemple une règle de signe. L'inconvénient de cette méthode est dès que l'on souhaitera montrer des propriétés de cette opération (distributivité par rapport à $+$, associativité,...), il faudra distinguer de nombreux cas. On préfère ainsi construire la multiplication de façon plus canonique en la construisant par passage au quotient.

Donnons une idée heuristique de la formule : on souhaite définir une multiplication et bien entendu que cette multiplication soit distributive par rapport à $+$ (et donc par rapport à $-$) et étende la multiplication de $\mathbb{N}$. Si une telle multiplication existe, on doit alors avoir (par distributivité)

$$\pi(m,n) \times \pi(m',n') = (i(m) - i(n)) \times (i(m') - (n')) = i(m)i(m') + i(n)i(n') - i(n)i(m') - i(m)i(n')$$

et donc (par le fait que la multiplication de $\mathbb{Z}$ étende celle de $\mathbb{N}$

$$\pi(m,n) \times \pi(m',n') = i(m)i(m') + i(n)i(n') - i(n)i(m') - i(m)i(n') = i(mm' + nn') - i(nm' + mn')$$

Ainsi, si cette multiplication existe, on doit avoir $\pi(m,n) \times \pi(m',n') = \pi(mm' + nn', nm' + mn')$. Il ne reste plus qu'à vérifier qu'une telle opération existe et vérifie les propriétés qu'on souhaite. C'est le sens de la proposition suivante.

Proposition 30 Il existe une application, notée $\times$, de $\mathbb{Z} \times \mathbb{Z}$ dans $\mathbb{Z}$ vérifiant

$$\forall\, (m,n,m',n') \in \mathbb{N}^4, \qquad \pi(m,n) \times \pi(m',n') = \pi(mm' + nn', mn' + nm')$$

De plus, l'application $i \colon \mathbb{N} \to \mathbb{Z}$ vérifie $i(nm) = i(n) \times i(m)$.

L'opération $\times$ est associative, distributive par rapport à $+$ et à $-$, commutative, admet $i(1)$ pour élément neutre, $i(0)$ pour élément absorbant et tout élément non nul est régulier pour $\times$.

Commentaires. La proposition précédente se résume par le fait que $(\mathbb{Z}, +, \times)$ est un anneau commutatif, unitaire intègre.

Preuve. Commençons par montrer que la loi est bien définie. L'idée du raisonnement est la même que pour l'addition mais les calculs sont un peu plus complexes. On se donne $(m,n,m',n',m_1,n_1,m_1',n_1') \in \mathbb{N}^8$, on suppose que

$$(m,n)\mathscr{R}(m',n') \qquad \text{et} \qquad (m_1,n_1)\mathscr{R}(m_1',n_1')$$

et on souhaite montrer que

$$(mm_1 + nn_1, mn_1 + nm_1)\mathscr{R}(m'm_1' + n'n_1', m'n_1' + n'm_1')$$

c'est-à-dire $mm_1 + nn_1 + m'n_1' + n'm_1' = mn_1 + nm_1 + m'm_1' + n'n_1'$.

On sait que $m + n' = m' + n$ et $m_1 + n_1' = n_1 + m_1'$. On écrit alors

$$(m' + n)m_1' + nn_1 = m'm_1' + nm_1' + nn_1 = m'm_1' + n(n_1 + m_1')$$

On en déduit alors que

$$(m + n')m_1' + nn_1 = m'm_1' + n(m_1 + n_1')\,.$$

En ajoutant mn_1 et $m'n_1'$, on obtient l'égalité

$$(m(m_1' + n_1) + nn_1 + n'm_1' + m'n_1' = m'm_1' + (m' + n)n_1' + nm_1 + mn_1\,.$$

qui se réécrit, en utilisant les relations $m + n' = m' + n$ et $m_1 + n_1' = n_1 + m_1'$, sous la forme

$$m(m_1 + n_1') + nn_1 + n'm_1' + m'n_1' = m'm_1' + (m + n)n_1' + nm_1 + mn_1\,.$$

La régularité de mn'_1 pour $+$ donne alors l'égalité souhaitée.

Montrons à présent les propriétés de $\times$. Débutons par l'associativité. Pour $(m,n,m',n',m'',n'') \in \mathbb{N}^6$, calculons

$$\pi(m,n) \times (\pi(m',n') \times \pi(m'',n'')) = \pi(m,n) \times \pi(m'm'' + n'n'', m''n' + m'n'')$$

ce qui donne (en utilisant l'associativité et la commutativité de $+$ et $\times$ dans $\mathbb{N}$)

$$\pi(m,n) \times (\pi(m',n') \times \pi(m'',n'')) = \pi(mm'm'' + mn'n'' + nn'm'' + nm'n'', mm''n' + mm'n'' + nm'm'' + nn'n'')\,.$$

On calcule ensuite

$$(\pi(m,n) \times \pi(m',n')) \times \pi(m'',n'') = \pi(mm' + nn', m'n + mn') \times \pi(m'',n'')$$

ce qui donne (en utilisant l'associativité et la commutativité de $+$ et $\times$ dans $\mathbb{N}$)

$$(\pi(m,n) \times \pi(m',n')) \times \pi(m'',n'') = \pi(mm'm'' + nn'm'' + m'nn'' + mn'n'', mm'n'' + nn'n'' + nm'm'' + mn'm'')\,.$$

La commutativité et l'associativité de $+$ et $\times$ dans $\mathbb{N}$ donne alors l'égalité souhaitée et l'associativité de $+$ dans $\mathbb{Z}$.

Passons à la commutativité de $\times$. Pour $(m,n,,m',n',) \in \mathbb{N}^4$, on a

$$\pi(m,n) \times \pi(m',n') = \pi(mm' + nn', mn' + nm') \quad \text{et} \quad \pi(m',n') \times \pi(m,n) = \pi(m'm + n'n, m'n + n'm)\,.$$

La commutativité de $+$ et $\times$ dans $\mathbb{N}$ donne alors le résultat.

Montrons la distributivité de $\times$ par rapport à $+$. Comme $\times$ est commutative, il suffit d'étudier la commutativité à droite. Pour $(m,n,,m',n',m'',n'') \in \mathbb{N}^6$, calculons

$$\pi(m,n) \times (\pi(m',n') + \pi(m'',n'')) = \pi(m,n) \times \pi(m' + m'', n' + n'')$$

ce qui donne

$$\pi(m,n) \times (\pi(m',n') + \pi(m'',n'')) = \pi(m(m' + m'') + n(n' + n''), m(n' + n'') + n(m' + m'')\,.$$

Par ailleurs,

$$\pi(m,n) \times \pi(m',n') + \pi(m,n) \times \pi(m'',n'')) = \pi(mm' + nn', nm' + mn') + \pi(mm'' + nn'', nm'' + mn'')$$

En utilisant la définition de l'addition dans $\mathbb{Z}$, on obtient

$$\pi(m,n) \times \pi(m',n') + \pi(m,n) \times \pi(m'',n'')) = \pi(mm' + nn' + mm'' + nn'', nm' + mn' + nm'' + mn'')$$

L'associativité et la commutativité de $+$ dans $\mathbb{N}$ ainsi que la distributivité de $\times$ dans $\mathbb{N}$ par rapport à $+$ donne le résultat souhaité.

On a $i(1) = \pi(1,0)$. Pour $(m,n) \in \mathbb{N}^2$, on a $\pi(m,n) \times i(1) = \pi(m + n0, m0 + n1) = \pi(m,n)$ car 0 est absorbant pour $\times$ dans $\mathbb{N}$ et un élément neutre pour $+$ dans $\mathbb{N}$ et 1 est un élément neutre pour 1 dans $\mathbb{N}$. Par commutativité, on en déduit que $i(1) \times \pi(m,n) = \pi(m,n)$ et $i(1)$ est bien un élément neutre pour $\times$.

Ainsi, on en déduit que $(\mathbb{Z}, +, \times)$ est un anneau unitaire. Cette propriété assure immédiatement que 0 est un élément absorbant pour $\times$ et que $\times$ est distributive par rapport à $-$ [8].

Pour $(m,n) \in \mathbb{N}^2$, on a $i(m)i(n) = \pi(m,0)\pi(n,0) = \pi(mn+0\times 0, 0\times n+m\times 0) = \pi(mn,0) = i(mn)$. Ainsi calculer un produit dans $\mathbb{N}$ puis l'envoyer dans $\mathbb{Z}$ revient à envoyer les entiers naturels dans $\mathbb{Z}$ puis à calculer leur produit dans $\mathbb{Z}$.

On considère un élément non nul $m \in \mathbb{Z}$. On veut montrer que m est régulier pour $\times$ c'est-à-dire que si $m \times x = m \times y$ alors $x = y$. En utilisant la distributivité par rapport à $-$, il suffit de montrer que si $m \times x = 0$ alors $x = 0$. En effet, l'égalité $m \times x = m \times y$ implique $m \times (x - y) = 0$ et donc $x - y = 0$ c'est-à-dire $x = y$.

On considère donc x tel que $mx = 0$. Si $mx = 0$ alors $m(-x) = 0$ [9]. Ainsi, d'après la remarque 29, on peut supposer que $x \in i(\mathbb{N})$. De même, on a aussi $(-m)x = 0$. Ainsi, on peut aussi supposer que $m \in i(\mathbb{N})$. L'égalité s'écrit alors $i(m')i(x') = 0$ avec $i(m') = m$ et $i(x') = x$. Mais, on a $i(m')i(x') = i(m'x') = 0 = i(0)$. L'injectivité de i assure alors que $m'x' = 0$ et donc $m' = 0$ ou $x' = 0$ d'après la proposition 14. Mais si $m' = 0$ alors $m = 0$ ce qui n'est pas le cas. Ainsi $x' = 0$ et donc $x = i(x') = i(0) = 0$.

---

8. Démonstrations à savoir faire !

9. C'est une propriété générale sur les anneaux à savoir démontrer : c'est la distributivité qui intervient : on a $0m \times 0 = m(x + (-x)) = mx + m(-x)$. Ainsi, comme $mx = 0$, on a bien $m(-x) = 0$.

2.2.3 Relation d'ordre sur les entiers relatifs

Proposition-Définition 31 Soit $x, y \in \mathbb{Z}$, la relation $\leqslant$ définie par $x \leqslant y$ si $y - x \in i(\mathbb{N})$ est une relation d'ordre totale sur $\mathbb{Z}$.

Elle vérifie les propriétés suivantes

(i) L'application $i\colon \mathbb{N} \to \mathbb{Z}$ est strictement croissante [10].

(ii) $\forall (x,y) \in \mathbb{Z}^2, \quad x \leqslant y \iff -y \leqslant -x$;

(iii) $\forall (x,y,z) \in \mathbb{Z}^3, \quad x \leqslant y \iff x + z \leqslant y + z$;

(iv) $\forall (x,y,z) \in \mathbb{Z}^3, \quad x \leqslant y \iff x - z \leqslant y - z$;

(v) $\forall (x,y,z) \in \mathbb{Z} \times \mathbb{Z} \times i(\mathbb{N}), \quad x \leqslant y \implies xz \leqslant yz$;

(vi) $\forall (x,y,z) \in \mathbb{Z} \times \mathbb{Z} \times -i(\mathbb{N}), \quad x \leqslant y \implies yz \leqslant xz$;

(vii) $\forall (x,y,z) \in \mathbb{Z} \times \mathbb{Z} \times i(\mathbb{N} \setminus \{0\}), \quad xz \leqslant yz \implies x \leqslant y$;

$(viii)$ $\forall (x,y,z) \in \mathbb{Z} \times \mathbb{Z} \times -i(\mathbb{N} \setminus \{0\}), \quad xz \leqslant yz \implies y \leqslant x$;

(ix) toute partie non vide et majorée de $\mathbb{Z}$ admet un plus grand élément ;

(x) toute partie non vide et minorée de $\mathbb{Z}$ admet un plus petit élément ;

(xi) L'ensemble $\mathbb{Z}$ n'admet ni plus grand, ni plus petit élément.

Preuve. Comme $0 \in i(\mathbb{N})$, on a $x \leqslant x$ et la relation est réflexive.

Supposons que $x \leqslant y$ et $y \leqslant x$. On a ainsi $y - x \in i(\mathbb{N})$ et $x - y \in i(\mathbb{N})$ c'est-à-dire $x - y \in i(\mathbb{N}) \cap -i(\mathbb{N})$. Or on a vu dans la remarque 29 que $i(\mathbb{N}) \cap -i(\mathbb{N}) = \{0\}$. Ainsi $x - y = 0$ et $x = y$. La relation $\leqslant$ est donc antisymétrique.

Supposons que $x \leqslant y$ et $y \leqslant z$. Il existe donc $(n,m) \in \mathbb{N}^2$ tel que $y - x = i(n)$ et $z - y = i(m)$. On a alors $z - x = (z - y) + (y - x) = i(m) + i(n) = i(m+n)$; la dernière égalité venant de la proposition 27. On en déduit que $x \leqslant z$ et la relation $\leqslant$ est transitive.

Soit $(x,y) \in \mathbb{Z}$, comme $\mathbb{Z} = i(\mathbb{N}) \cup -i(\mathbb{N})$, on a $x - y \in i(\mathbb{N})$ ou $y - x \in i(\mathbb{N})$. Ainsi $y \leqslant x$ ou $x \leqslant y$. L'ordre sur $\mathbb{Z}$ est donc total.

Montrons à présent les propriétés.

(i) Soient $(m,n) \in \mathbb{N}^2$ tel que $m \leqslant n$. Il existe a tel que $m + a = n$. On a alors $i(n) = i(m) + i(a)$ et donc $i(n) - i(m) = i(a)$. Ainsi $i(n) - i(m) \in i(\mathbb{N})$ c'est-à-dire $i(m) \leqslant i(n)$. La fonction i est croissante. Si en plus $m < n$, alors $a \neq 0$. L'injectivité de i assure alors que $i(a) \neq i(0) = 0$. Ainsi $i(n) \neq i(m)$ et donc $i(m) < i(n)$ [11].

(ii) On a $y - x = (-x) - (-y)$, la relation $y - x \in i(\mathbb{N})$ est équivalente à $(-x) - (-y) \in i(\mathbb{N})$

(iii) Comme $y - x = (y+z) - (x+z)$, la relation $y - x \in i(\mathbb{N})$ est équivalente à $(y+z) - (x+z) \in i(\mathbb{N})$.

(iv) Cette propriété est équivalente à la précédente car soustraire z revient à ajouter $-z$. On peut aussi la démontrer directement comme la précédente en remarquant que $y - x = (y - z) - (x - z)$.

(v) Il existe $n \in \mathbb{N}$ tel que $y - x = i(n)$ et $m \in \mathbb{N}$ tel que $z = i(m)$. On a alors $yz - xz = (y - x)z = i(n)i(m) = i(nm)$, la dernière égalité résultat de la proposition 30.

(vi) Il existe $n \in \mathbb{N}$ tel que $y - x = i(n)$ et $m \in \mathbb{N}$ tel que $z = -i(m)$. On a alors $xz - yz = (x - y)z = (y - x)(-z) = i(n)i(m) = i(nm)$. Ainsi $yz \leqslant xz$.

(vii) On suppose que $xz \leqslant yz$. Comme l'ordre est total, si on n'a pas $x \leqslant y$, on aura $y < x$. Ainsi $x - y \in i(\mathbb{N} \setminus \{0\})$ c'est-à-dire qu'il existe $n \in \mathbb{N} \setminus \{0\}$ tel que $x - y = i(n)$. Comme $z \in i(\mathbb{N} \setminus \{0\})$, il existe $m \in \mathbb{N} \setminus \{0\}$ tel que $z = i(m)$. On a alors $xz - yz = (x - y)z = i(n)i(m) = i(nm)$. Mais, d'après la proposition 14, on a $nm \neq 0$ et comme i est injective, on a aussi $i(nm) \neq 0$. Ainsi $yz < xz$ ce qui contredit l'hypothèse. On a aussi le résultat souhaité. Il est aussi équivalent au fait que la multiplication par $z \in i(\mathbb{N} \setminus \{0\})$ est strictement croissante.

$(viii)$ On applique le résultat précédent à $-z$.

(ix) Soit A une partie non vide et majorée. On distingue deux cas. Supposons que $\mathrm{A} \cap i(\mathbb{N})$. L'ensemble $\mathrm{A} \cap i(\mathbb{N})$ est alors une partie non vide de $i(\mathbb{N})$. Comme l'ordre sur $\mathbb{N}$ et $i(\mathbb{N})$ coïncident (d'après (i)), on en déduit que cette partie $\mathrm{A} \cap i(\mathbb{N})$ admet une plus grand élément z. Montrons que z est le plus grand élément de z. Si $y \in \mathrm{A} \cap i(\mathbb{N})$, on a bien $y \leqslant z$. Si $y \in \mathrm{A} \setminus (\mathrm{A} \cap i(\mathbb{N}))$ alors $y \in -i(\mathbb{N})$ (puisque $\mathbb{Z} = i(\mathbb{N}) \cup -i(\mathbb{N})$. En particulier, on a $y \leqslant 0 \leqslant z$. Ainsi z est bien le

10. Cela est équivalent au fait de dire que l'ordre sur $\mathbb{Z}$ prolonge l'ordre défini au chapitre 1 sur $\mathbb{N}$

11. Cela suffit à montrer que l'ordre sur $i(\mathbb{N})$ est bien le même que l'ordre induit par celui de $\mathbb{N}$. En effet, on a déjà vu que $m \leqslant n$ implique $i(m) \leqslant i(n)$. Réciproquement, on suppose que $i(m) \leqslant i(n)$ si on n'avait pas $m \leqslant n$, on aurait $n < m$ puisque l'ordre sur $\mathbb{N}$ est total. On en déduit alors par stricte croissante que $i(n) < i(m)$. NON.

plus grand élément de A.

Si $A \cap i(\mathbb{N}) =$ alors $A \subset -i(\mathbb{N})$. La partie $-A = \{-x,\ x \in A\}$ est alors une partie non vide de $i(\mathbb{N})$. Elle admet donc un plus petit élément d'après les propriétés de l'ordre sur $\mathbb{N}$. Il existe donc $z \in A$ tel que $-z \leqslant -x$ pour tout $x \in A$. On a donc (grâce à (ii)) $x \leqslant z$ pour tout $x \in A$ et z est le plus grand élément de A.

(x) Soit A une partie non vide et minorée. Le point La partie $-A$ est donc non vide et majorée (d'après (ii)). Elle admet donc un plus grand élément d'après (ix) (de la forme $-z$ pour $z \in A$. Le point (ii) assure alors que z est un plus petit élément pour A.

(xi) Pour tout $x \in \mathbb{Z}$, on a $x < x + i(1)$ et $x - i(1) < x$ ce qui montre que $\mathbb{Z}$ n'a pas de plus petit ni de plus grand élément.

Remarque 32 – Signe et inversible. On a $i(\mathbb{N}) = \{x \in \mathbb{Z}, x \geqslant 0\}$ et $-i(\mathbb{N}) = \{x \in \mathbb{Z}, x \leqslant 0\}$. En effet, on a $x \geqslant 0$ si et seulement $x = x - 0 \in i(\mathbb{N})$. Comme $x \leqslant 0$ est équivalent d'après le point (ii) de la proposition précédente est équivalent à $-x \geqslant 0$, on obtient le résultat souhaité.

Le relation (v) et (vi) assurent aussi que le produit de deux éléments positifs est positifs, le produit de deux éléments négatifs est négatif et le produit d'un nombre positif et d'un nombre négatif est négatif.

Soit $x, y \in \mathbb{Z}$ tels que $xy = 1$. Montrons que $x = y = 1$ ou $x = y = -1$. Si $xy = 1$ alors $(-x)(-y) = 1$. Ainsi, quitte à changer x en $-x$, on peut supposer (grâce au fait que $\mathbb{Z} = i(\mathbb{N}) \cup -i(\mathbb{N})$ que $x \in i(\mathbb{N})$ et évidemment $x \neq \{0\}$ car 0 est absorbant pour $\times$. Si $y \in -i(\mathbb{N} \setminus \{0\})$ alors d'après ce qui précède $xy \in -i(\mathbb{N})$ et donc $xy \neq 1$. Ainsi $y \in i(\mathbb{N})$. Il existe donc $m, n \in \mathbb{N}$ tels que $x = i(m)$ et $y = i(n)$. On a ainsi $xy = i(m)i(n) = 1 = i(1)$. Ainsi $i(1) = (m)i(n) = i(mn)$. L'injectivité de i assure alors que $mn = 1$. La proposition 14 assure alors que $m = n = 1$ et donc $x = i(m) = 1$ et $y = i(n) = 1$.

Revenons sur l'objectif initial : l'objectif était de construire un nouvel ensemble de nombres dans lequel les équations $x + n = m$ pour $n, m \in \mathbb{N}$ auraient des solutions. Comme $(\mathbb{Z}, +)$ est un groupe, ces équations ont bien une solution plus précisément $x = i(m) - i(n)$ (c'est grâce à la structure de groupe qu'on peut donner un sens à $-$ pour tout $m, n \in \mathbb{N}$. On a même mieux puisqu'en fait, les équations $x + n = m$ ont une solution pour tous $m, n \in \mathbb{Z}$ et pas seulement $m, n \in \mathbb{N}$.

Chapitre 3

Nombres rationels et fractions

3.1 Construction des nombres rationnels

Maintenant que $\mathbb{Z}$ est construit et que toutes les équations de la forme $x+m=n$ ont une solutions, on s'intéresse aux équations de la forme $bx=a$ pour $a,b\in\mathbb{Z}$. La plupart d'entre-elle n'ont pas de solutions dans $\mathbb{Z}$; par exemple $2x=1$ (voir la remarque 32). On va appliquer le même principe que pour la construction de $\mathbb{Z}$: on considère l'ensemble des équations possibles et on identifie les équations qui « ont les mêmes sont solutions » [1] (voir le paragraphe d'introduction de la section 2.1). Il s'agit donc à présent de comprendre l'équivalence entre ces équations. Une première remarque est que si $b=0$ alors $a=0$ et alors tous les nombres peuvent être solution ce qu'on ne souhaite pas. Ainsi, on ne considère pas les équations avec $b=0$. Les équations qui nous intéressent sont celles de la forme $bx=a$ avec $a\in\mathbb{Z}$ et $b\in\mathbb{Z}\setminus\{0\}$. En utilisant la propriété 30 et plus spécifiquement l'intégrité de l'anneau $\mathbb{Z}$, on en déduit que les équations $bx=a$ et $mbx=ma$ sont équivalentes. Supposons que $bx=a$ et $dx=c$ sont deux équations sont équivalentes. Si $a=0$, on a $x=0$ et donc $c=0$ (et réciproquement) ainsi $ad=bc=0$. Si $a\neq 0$ (et donc $c\neq 0$) alors $dx=c$ et $bx=a$ sont équivalentes à $adx=ac$ et $bcx=ca$. Ainsi $bcx=adx$ donc $cb=ad$ (par intégrité de $\mathbb{Z}$ puisque $x\neq 0$). Réciproquement, on suppose que $bc=ad$. Si $a=0$, $c=0$ puisque $b\neq 0$ (et réciproquement) et donc $x=0$ et les équations $bx=a$ et $dx=c$ sont équivalentes. Si $a\neq 0$ alors $c\neq 0$ et les équations $bx=a$ et $dx=c$ sont équivalentes respectivement à $cbx=ac$ et $dax=ac$. Or ces équations n'en sont en fait qu'une seule puisque $bc=ad$. Ainsi $bx=a$ et $dx=c$ sont équivalentes à une même équation et donc sont équivalentes [2]. Une équation $bx=a$ pouvant se résumer au couple (a,b), on construit ainsi l'ensemble des nombres rationnels.

Proposition-Définition 33 – Définition des nombres rationnels. Sur l'ensemble $\mathbb{Z}\times\mathbb{Z}\setminus\{0\}$, la relation $\mathscr{S}$ définie par

$$(a,b)\mathscr{S}(c,d) \qquad \Longleftrightarrow \qquad ad=bc\,.$$

est une relation d'équivalence. On note $\mathbb{Q}$ l'ensemble quotient $(\mathbb{Q}\times\mathbb{Q})/\mathscr{S}$ et on l'appelle l'*ensemble des nombres rationnels*.

On note $\pi'\colon \mathbb{Z}\times\mathbb{Z}\setminus\{0\}\to\mathbb{Q}$ l'application qui à (a,b) fait correspondre sa classe d'équivalence [3]. Cependant plutôt que de noter $\pi'(a,b)$ la classe d'équivalence de (a,b) on note a/b. Ainsi a/b désigne une classe d'équivalence et $a/b=c/d$ signifie $ad=bc$.

Preuve. Montrons que $\mathscr{S}$ est une relation d'équivalence.

Comme $ab=ba$ (puisque la multiplication sur $\mathbb{Z}$ est commutative), on a bien $(a,b)\mathscr{S}(a,b)$. Ainsi $\mathscr{S}$ est réflexive.

Supposons que $(a,b)\mathscr{S}(c,d)$ (c'est-à-dire $ad=bc$) et montrons que $(c,d)\mathscr{S}(a,b)$ (c'est-à-dire $cb=da$). Cela découle immédiatement de la commutativité de la multiplication dans $\mathbb{Z}$. Ainsi $\mathscr{S}$ est symétrique.

Supposons que $(a,b)\mathscr{S}(c,d)$ et $(c,d)\mathscr{S}(e,f)$. On a donc $ad=bc$ et $cf=de$. En multipliant la première relation par f et la deuxième par b, on obtient $adf=bcf=bde$. Ainsi $adf=bde$. Comme

1. Cette expression est bien sûr abusive puisqu'on ne dispose pas encore des nombres rationels et que $2x=1$ n'a pas de solution, mais on y pense en terme d'équivalence d'équations.

2. Le raisonnement ci-dessus reste purement heuristique puisque la relation d'équivalence sur les équations n'a pas été proprement définie et il n'a pas été montré une quelconque propriété de transitivité qui serait utilisée ici. Cependant, ce raisonnement heuristique permet de mettre en évidence la relation à considérer pour construire l'ensemble des rationnels

3. Cela signifie que $\pi'(a,b)=\pi'(c,d)$ si et seulement si $ad=bc$.

la multiplication est commutative, que $d \neq 0$ et que $\mathbb{Z}$ est intègre, on en déduit que $af = be$. Ainsi $(a,b)\mathscr{S}(e,f)$ et la relation $\mathscr{S}$ est transitive.

3.1.1 Lien entre les entiers relatifs et les nombres rationnels

On a construit un nouvel ensemble de nombres $\mathbb{Q}$. Il s'agit dans un premier temps de voir que c'est un ensemble qui « contient » le précédent. Évidemment cette notion de « contient » est abusive les éléments de $\mathbb{Q}$ sont des classes d'équivalence de couples. Cependant, on va construire une application $j\colon \mathbb{Z} \to \mathbb{Q}$ injective. Et c'est toujours grâce à cette application qu'on pourra considérer que $\mathbb{Z}$ « est » un sous-ensemble de $\mathbb{Q}$.

Proposition 34 – La relation entre $\mathbb{Z}$ et $\mathbb{Q}$. L'application

$$j\colon \begin{cases} \mathbb{Z} \longrightarrow \mathbb{Q} \\ n \longmapsto \pi'(n,1) = n/1 \end{cases}$$

est injective et permet ainsi d'identifier $\mathbb{Z}$ a un sous-ensemble de $\mathbb{Q}$.

Preuve. Supposons $j(n) = j(n')$. On a ainsi $n/1 = n'/1$ et donc $n1 = 1n'$ ce qui donne $n = n'$ puisque 1 est élément neutre pour la multiplication.

3.2 Structure de corps sur l'ensemble des rationnels

On souhaite à présent définir sur $\mathbb{Q}$ une addition et une multiplication. On souhaite évidemment que ces applications « prolongent » les addition et multiplication de $\mathbb{Z}$ et donc on va les construire à partir de celle de $\mathbb{Z}$. La relation d'équivalence $\mathscr{S}$ reposant sur la multiplication, il n'est pas très étonnant que la multiplication sur $\mathbb{Q}$ soient définie très simplement à partir de celle de $\mathbb{Z}$. Pour l'addition les choses sont plus complexes : on aimerait poser, par simplicité que la somme de a/b et c/d est $(a+c)/(b+d)$. Cependant, il a deux obstacles profonds à cette raison. Le premier est que cette addition ne prolonge pas celle de $\mathbb{Z}$: en effet la somme de $j(n) = n/1$ et $j(m) = m/1$ sera alors $(n+m)/2$ qui est différent [4] de $j(n+m) = (m+n)/1$. Le deuxième obstacle, tout aussi problématique est que la somme ainsi ne sera pas bien définie. En effet, si on calcule avec cette formule la somme de $2/3$ et $1/2$, on obtient $3/5$. Mais $2/3 = 4/6$ et la somme vaudrait alors aussi $5/8$. Mais $3/5 \neq 5/8$ puisque $3 \times 8 \neq 5 \times 5$.

Essayons d'expliquer d'où vient la formule de l'addition. On souhaite ajouter a/b et c/d. Pour cela, le but est d'essayer de se ramener à $\mathbb{Z}$. Grâce à la multiplication par b, on peut ramener a/b dans $\mathbb{Z}$ (ou plutôt dans $j(\mathbb{Z})$). De même, en multipliant par d, on peut ramener c/d dans $\mathbb{Z}$. Le problème est qu'on a multiplier par b d'un côté et par d de l'autre et que cela n'est pas tellement compatible avec les propriétés de l'addition. L'idée est alors de multiplier par bd chacun des deux termes pour les ramener simultanément dans $\mathbb{Z}$ et d'ensuite les ajouter. On obtient ainsi d'un côté ad et de l'autre cb. Ainsi en multipliant la somme par bd, on obtient $ad + bc$ (par distributivité) ce qui donne bien la formule classique pour la somme $(ad+bc)/bc$.

Proposition 35 – Le corps des nombres rationnels. Il existe sur $\mathbb{Q}$ une loi $+$ et une loi $\times$ définies par

$$+\colon \begin{cases} \mathbb{Q}^2 \longrightarrow \mathbb{Q} \\ \left(\frac{a}{b}, \frac{c}{d}\right) \longmapsto \dfrac{ad+bc}{bd} = \pi'(ad+bc, bd) \end{cases}$$

et

$$\times\colon \begin{cases} \mathbb{Q}^2 \longrightarrow \mathbb{Q} \\ \left(\frac{a}{b}, \frac{c}{d}\right) \longmapsto \dfrac{ac}{bd} = \pi'(ac, bd)\,. \end{cases}$$

L'ensemble $(\mathbb{Q}, +, \times)$ est un corps dont l'élément neutre pour $+$ est $j(0) = 0/1$ et l'élément neutre pour $\times$ est $j(1) = 1/1$. De plus, l'application $j\colon \mathbb{Z} \to \mathbb{Q}$ est un morphisme d'anneaux unitaires.

Ces deux dernières phrases signifient que

(i) la loi $+$ est associative, commutative, qu'elle admet un élément neutre et que tout élément de $\mathbb{Q}$ admet un inverse pour $+$

4. sauf si $m + n = 0$

(*ii*) la loi $\times$ est associative, commutative, distributive par rapport à $+$ admet un élément neutre et que tout élément non nul de $\mathbb{Q}$ est inversible pour $\times$.

(*iii*) Pour tous $(n,m) \in \mathbb{Z}$, on a $j(n+m) = j(n) + j(m)$ et $j(nm) = j(n)j(m)$ et $j(1)$ est élément neutre pour $\times$.

Preuve. Le point délicat est de vérifier que ces deux applications sont bien définies ; les propriétés découlant des propriétés de la multiplication et de l'addition dans $\mathbb{Z}$.

Commençons par $+$. On suppose que $a/b = a'/b'$ et $c/d = c'/d'$. L'objectif est de montrer que $(ad+bc, bd)\mathscr{S}(a'd'+b'c', b'd')$. Pour cela, on calcule (par distributivité de $\times$ sur $+$ dans $\mathbb{Z}$ et commutativité de $\times$ dans $\mathbb{Z}$)

$$b'd'(ad+bc) = ab'dd' + bb'cd'$$

Comme $ab' = ba'$ et $cd' = dc'$, on obtient

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

La commutativité de $\times$ dans $\mathbb{Z}$ et la distributivité de $\times$ sur $+$ dans $\mathbb{Z}$ donne alors

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

ce qui est l'égalité souhaitée.

Passons à présent à $\times$. On suppose que $a/b = a'/b'$ et $c/d = c'/d'$. L'objectif est de montrer que $(ac, bd)\mathscr{S}(a'c', b'd')$ Pour cela, en utilisant la commutativité de la multiplication dans $\mathbb{Z}$ et les relations $ab' = ba'$ et $cd' = dc'$, on obtient

$$ac\,b'd' = ab'\,cd' = ba'\,dc' = a'c'\,bd$$

ce qui donne le résultat souhaité.

Remarque 36 – Retour sur l'objectif initial. On souhaitait construire des solutions aux équations $bx = a$ où $a \in \mathbb{Z}$ et $b \in \mathbb{Z} \setminus \{0\}$ et x est l'inconnue. Or en posant $x = j(a) \times j(b)^{\times} = a/b$. On a bien $j(b)a/b = j(a)$. En fait, on a même mieux : toute équation de la forme $rx = r'$ avec $r \in \mathbb{Q}$ et $r' \in \mathbb{Q} \setminus \{0\}$ admet une unique solution qui est $r'r^{-1}$ [5].

3.3 Relation d'ordre sur les nombres rationnels

On souhaite à présent définir un ordre sur l'ensemble $\mathbb{Q}$, ordre qui bien entendu « prolonge » [6] l'ordre sur $\mathbb{Z}$. Pour cela, on va procéder en construisant un ensemble de nombres rationnels P (auquel on va penser comme les nombres rationnels positifs (d'où le nom de l'ensemble) et on définit ensuite la relation d'ordre sur $\mathbb{Q}$ par $r \leqslant r'$ lorsque $r' - r \in \mathrm{P}$. Les propriétés de P permettent alors de s'assurer que la relation ainsi construite est bien une relation d'ordre. Elles permettent aussi de montrer que cet ordre est total et se comporte bien vis-à-vis de l'addition et de la multiplication.

Proposition-Définition 37 – La partie P. On note $\mathrm{P} = \{x \in \mathbb{Q}, \quad \exists (a,b) \in \mathbb{N} \times \mathbb{N} \setminus \{0\}\,, x = a/b\}$ [7].

On a $\mathrm{P} + \mathrm{P} \subset \mathrm{P}$, $\mathrm{PP} \subset \mathrm{P}$, $\mathbb{Q} = \mathrm{P} \cup -\mathrm{P}$ et $\mathrm{P} \cap -\mathrm{P} = \{0\}$.

Preuve. Si $x, y \in \mathrm{P}$, il existe $a, a' \in \mathbb{N}$ et $b, b' \in \mathbb{N} \setminus \{0\}$ tel que $x = a/b$ et $y = a'/b'$. On a alors $x+y = (ab'+a'b)/bb'$. Comme $ab'+a'b \in \mathbb{N}$ et $bb' \in \mathbb{N} \setminus \{0\}$ [8]. On obtient $x+y \in \mathrm{P}$ et donc $\mathrm{P}+\mathrm{P} \subset \mathrm{P}$.

On a aussi $xy = (aa')/(bb')$. Comme $aa' \in \mathbb{N}$ et $bb' \in \mathbb{N} \setminus \{0\}$, on obtient que $xy \in \mathrm{P}$ et donc $\mathrm{PP} \subset \mathrm{P}$.

Soit $x \in \mathbb{Q}$. On écrit $x = a/b$ avec $a \in \mathbb{Z}$ et $b \in \mathbb{Z} \setminus \{0\}$. On a alors quatre cas possibles d'après la remarque 29 : soit $a, b \in \mathbb{N}$, $a \in -\mathbb{N}$ et $b \in \mathbb{N}$, soit $a \in -\mathbb{N}$ et $b \in \mathbb{N}$ soit $a, b \in -\mathbb{N}$.

Par ailleurs, pour tout $c, d \in \mathbb{Z} \times \mathbb{Z} \setminus \{0\}$, on a $c/d = -c/-d$ puisque $c(-d) = (-c)d = -(cd)$. Ainsi dans le premier et le quatrième cas, on a $x \in \mathrm{P}$; on en déduit aussi que le troisième cas, se ramène au deuxième. Dans ce cas, x peut s'écrire sous la forme $(-a)/b$ avec $a, b \in \mathbb{N}$. Or, on a vu que $(-a)/b = -(a/b)$ dans la preuve de la proposition 35. Finalement, $x \in -\mathrm{P}$.

5. On peut donner un sens à r^{-1} puisque r est non nul dans $\mathbb{Q}$

6. Une fois encore, cette notion de prolongement se fait au travers de l'application injective j.

7. En respectant les notations utilisées pour le lien entre $\mathbb{N}$ et $\mathbb{Z}$, il vaudrait mieux écrire $x = i(a)/i(b)$ mais on a fait le choix de ne plus écrire ce i

8. Le fait que bb' ne soit pas nul résulte des propriétés de la multiplication dans $\mathbb{Z}$

On suppose à présent que $x \in \mathrm{P} \cap -\mathrm{P}$. Il existe donc $a, a' \in \mathbb{N}$ et $b, b' \in \mathbb{N} \setminus \{0\}$ tel que $x = a/b = -(a'/b') = (-a')/b'$. On a ainsi $ab' = -a'b \in \mathbb{N} \cap -\mathbb{N} = \{0\}$. Comme $b' \neq 0$ les propriétés de la multiplication dans $\mathbb{Z}$ assure que $a = 0$ et donc $x = 0$. Réciproquement, on a $0 = 0/1 = -0/1 \in \mathrm{P} \cap -\mathrm{P}$. Ainsi $\mathrm{P} \cap -\mathrm{P} = \{0\}$.

On peut à présent définir simplement l'ordre sur $\mathbb{Q}$.

Proposition-Définition 38 Soit $x, y \in \mathbb{Q}$, la relation $\leqslant$ définie par $x \leqslant y$ si $y - x \in \mathrm{P}$ est une relation d'ordre totale sur $\mathbb{Q}$. Elle vérifie les propriétés suivantes

(i) L'application $j \colon \mathbb{Z} \to \mathbb{Q}$ est strictement croissante [9].
(ii) $\forall (x, y) \in \mathbb{Q}^2, \quad x \leqslant y \iff -y \leqslant -x$;
(iii) $\forall (x, y, z) \in \mathbb{Q}^3, \quad x \leqslant y \iff x + z \leqslant y + z$;
(iv) $\forall (x, y, z) \in \mathbb{Q}^3, \quad x \leqslant y \iff x - z \leqslant y - z$;
(v) $\forall (x, y, z) \in \mathbb{Q} \times \mathbb{Q} \times \mathrm{P}, \quad x \leqslant y \implies xz \leqslant yz$;
(vi) $\forall (x, y, z) \in \mathbb{Q} \times \mathbb{Q} \times \mathrm{P}, \quad x \leqslant y \implies yz \leqslant xz$;
(vii) $\forall (x, y, z) \in \mathbb{Q} \times \mathbb{Q} \times (\mathrm{P} \setminus \{0\}), \quad xz \leqslant yz \implies x \leqslant y$;
(viii) $\forall (x, y, z) \in \mathbb{Q} \times \mathbb{Q} \times -(\mathrm{P} \setminus \{0\}), \quad xz \leqslant yz \implies y \leqslant x$;
(ix) L'ensemble $\mathbb{Q}$ n'admet ni plus grand, ni plus petit élément.
(x) $\forall x, y \in (\mathrm{P} \setminus \{0\}) \times (\mathrm{P} \setminus \{0\})$, il existe $n \in \mathbb{N}$ tel que $y < nx$.

Preuve. Comme $0 \in \mathrm{P}$, on a $x - x \in \mathrm{P}$ et donc $x \leqslant x$ et la relation est réflexive.

Supposons que $x \leqslant y$ et $y \leqslant x$. On a ainsi $y - x \in \mathrm{P}$ et $x - y \in \mathrm{P}$ c'est-à-dire $x - y \in \mathrm{P} \cap -\mathrm{P}$. La proposition-définition 37 dit que $\mathrm{P} \cap -\mathrm{P} = \{0\}$. Ainsi $x - y = 0$ et $x = y$. La relation $\leqslant$ est donc antisymétrique.

Supposons que $x \leqslant y$ et $y \leqslant z$. On a ainsi $y - x \in \mathrm{P}$ et $z - y \in \mathrm{P}$. On a alors $z - x = (z - y) + (y - x) \in \mathrm{P} + \mathrm{P}$; La proposition-définition 37 assure que $\mathrm{P} + \mathrm{P} \subset \mathrm{P}$. On en déduit que $x \leqslant z$ et la relation $\leqslant$ est transitive.

Soit $(x, y) \in \mathbb{Q}$, comme $\mathbb{Q} = \mathrm{P} \cup -\mathrm{P}$, on a $x - y \in \mathrm{P}$ ou $y - x \in \mathrm{P}$. Ainsi $y \leqslant x$ ou $x \leqslant y$. L'ordre sur $\mathbb{Q}$ est donc total.

Montrons à présent les propriétés.

(i) Soient $(m, n) \in \mathbb{Z}^2$ tel que $m \leqslant n$. On a alors $n - m \in \mathbb{N}$. Comme $j(n) - j(m) = j(n - m) = (n - m)/1$ [10], on en déduit que $j(n) - j(m) \in \mathrm{P}$ (puisque $n - m \in \mathbb{N}$ et $1 \in \mathbb{N}$). Ainsi j est croissante. L'injectivité de j assure alors la stricte croissante de j. En effet si $m < n$ alors $n - m \neq 0$ et $j(n - m) \neq 0$ (par injectivité de j). On a ainsi $j(n - m) = j(n) - j(m) \neq 0$ et par croissance $j(m) \leqslant j(n)$. Ainsi $j(m) < j(n)$.

(ii) On a $y - x = (-x) - (-y)$, la relation $y - x \in \mathrm{P}$ est équivalente à $(-x) - (-y) \in \mathrm{P}$

(iii) Comme $y - x = (y + z) - (x + z)$, la relation $y - x \in \mathrm{P}$ est équivalente à $(y + z) - (x + z) \in \mathrm{P}$.

(iv) Cette propriété est équivalente à la précédente car soustraire z revient à ajouter $-z$. On peut aussi la démontrer directement comme la précédente en remarquant que $y - x = (y - z) - (x - z)$.

(v) On a $y - x \in \mathrm{P}$. Or $yz - xz = (y - x)z \in \mathrm{PP}$. Comme $\mathrm{PP} \subset \mathrm{P}$ d'après la proposition-définition 37, on obtient le résultat souhaité.

(vi) On a $y - x \in \mathrm{P}$ et $z = -z'$ avec $z' \in \mathrm{P}$. On a alors $xz - yz = (x - y)z = (y - x)(-z) = (y - x)z' \in \mathrm{PP}$. Comme $\mathrm{PP} \subset \mathrm{P}$ d'après la proposition-définition 37, on obtient le résultat souhaité.

(vii) On suppose que $xz \leqslant yz$. Comme $z \in \mathrm{P}$, il existe $a, b \in \mathbb{N}$ tel que $z = a/b$. De plus, $z \neq 0$ ainsi $a \neq 0$ et on a donc $z^{-1} = b/a \in \mathrm{P}$. On applique alors le point (v) en multipliant l'inégalité $xz \leqslant yz$ par z^{-1} pour obtenir la relation $x \leqslant y$.

(viii) On applique le résultat précédent à $-z$ et on utilise (ii).

(ix) Comme $1 = 1/1 \in \mathrm{P}$, on en déduit que pour tout $x \in \mathbb{Q}$, on a $x < x + 1$ et $x - 1 < x$ ce qui montre que $\mathbb{Q}$ n'a pas de plus petit ni de plus grand élément.

(x) Comme $x \in \mathrm{P}$, on a vu que $x^{-1} \in \mathrm{P}$ (voir (vii)), ainsi $yx^{-1} \in \mathrm{PP} \subset \mathrm{P}$. On écrit alors $yx^{-1} = a/b$ avec $(a, b) \in \mathbb{N} \times \mathbb{N} \setminus \{0\}$. Comme $b \neq 0$, l'exemple 20 montre que la suite des multiples de b est strictement croissante. La proposition 19 montre alors qu'il existe tel que $nb > a$. En appliquant les points (v) (avec $z = b^{-1}$) on obtient $n \geqslant a/b$ (mais si $n = a/b$ alors en multipliant par b, on obtient $nb = a$. NON). Ainsi $n > a/b$. On obtient ainsi $n > yx^{-1}$. Toujours avec (v) (en prenant

9. Cela est équivalent au fait de dire que l'ordre sur $\mathbb{Q}$ prolonge l'ordre défini au chapitre 2.2 sur $\mathbb{Z}$
10. À savoir démontrer à partir de la relation $j(n + m) = j(n) + j(m)$ pour tous $n, m \in \mathbb{Z}$

$z = x$), on en déduit que $nx \geqslant y$. De plus si $nx = y$ alors en multipliant par x^{-1}, on aurait $n = yx^{-1}$. NON. Ainsi $nx > y$ comme souhaité.

Remarque 39 Avec cette définition, on a $\mathrm{P} = \{x \in \mathbb{Q},\ x \geqslant 0\}$ puisque $x - 0 \in \mathrm{P}$ est équivalent à $x \in \mathrm{P}$ puisque $x - 0 = x$.

Remarque 40 – Une partie non vide majorée sans plus grand élément ni borne supérieure. L'ordre sur $\mathbb{Q}$ est bien différent de l'ordre sur $\mathbb{Z}$. En effet, un ensemble non vide et majoré n'a pas forcément de plus grand élément ni même de borne supérieure.

Par exemple, considérons l'ensemble $\mathrm{U} = \{x \in \mathrm{P}, x^2 < 2\}$. Il est majoré par 2 non vide En effet, si U n'était pas majoré par 2 alors il existerait $x \in \mathrm{U}$ tel que $x > 2$. Mais, en multipliant par $x > 0$, on aurait $x^2 > 2x$. Or en multipliant la relation $x > 2$ par $2 > 0$, on a $2x \geqslant 4$. Ainsi, on aurait $2 > x^2 > 2x > 4$. NON.

Montrons qu'il n'admet pas de plus grand élément. Soit $m/n \in \mathrm{U} \setminus \{0\}$. Montrons que $4mn/(2n^2 + m^2) \in \mathrm{U}$ [11] et vérifie $m/n < 4mn/(2n^2 + m^2)$.

Comme $n \neq 0$, on a $2n^2 + m^2 > 0$. Ainsi $4mn/(2n^2 + m^2)$ existe.

Par ailleurs, on a $2(2n^2+m^2)^2 = 8n^4+8m^2n^2+2m^4$. Ainsi $2(2n^2+m^2)^2-(4mn)^2 = 8n^4-8m^2n^2+2m^4 = 2(2n^2-m^2)^2 \geqslant 0$. De plus, comme $(m/n)^2 < 2$, on a $2n^2-m^2 > 0$. Ainsi $2(2n^2+m^2)^2-(4mn)^2 > 0$ et donc $4mn/(2n^2 + m^2) \in \mathrm{U}$.

Montrons que $m/n < 4mn/(2n^2 + m^2)$. Cette relation est équivalente à $4mn^2 - m(2n^2 + m^2) > 0$. Or $4mn^2 - m(2n^2 + m^2) = m(2n^2 - m^2) > 0$ car $m \neq 0$ et $m/n \in \mathrm{U}$ (et donc $2n^2 > m^2$). Ainsi, à partir d'un élément non nul de U, on peut en construire un strictement plus grand. On en déduit que U ne peut avoir de plus grand élément.

Montrons qu'il n'y a pas de borne supérieure à U. Si $x = m/n$ est un majorant de U. Montrons que $(m^2 + 2n^2)/(2nm)$ [12] est un majorant de U strictement plus petit que x.

Commençons par montrer que $(m^2 + 2n^2)/(2nm) < m/n$. Cette relation est équivalente à $2nm^2 - nm^2 - 2n^3 > 0$. Or $2nm^2 - nm^2 - 2n^3 = n(m^2 - 2n^2)$. Comme m/n est un majorant de U, on ne peut avoir $m/n \in \mathrm{U}$ puisque U n'a pas de plus grand élément. Comme $m/n \in \mathrm{P}$ et que l'ordre est total on a $(m/n)^2 \geqslant 2$ et donc $m^2 - 2n^2 \geqslant 0$. Or on sait qu'il n'existe pas (m, n) tel que $m^2 = 2n^2$ [13]. Ainsi $m^2 - 2n^2 > 0$ et comme $n > 0$, on a $(m^2 + 2n^2)/(2nm) < m/n$.

Par ailleurs, on a bien sûr $(m^2 + 2n^2)/(2nm) > 0$ (puisque $n > 0$). Pour montrer que $(m^2 + 2n^2)/(2nm)$ est un majorant de U, il suffit de montrer que $((m^2 + 2n^2)/(2nm))^2 > 2$. En effet, pour $y \in \mathrm{U}$, on aura alors $y^2 < 2 < ((m^2 + 2n^2)/(2nm))^2$ et si on avait $(m^2 + 2n^2)/(2nm) \leqslant y$ alors en multipliant cette inégalité par $y \geqslant 0$ et par $(m^2+2n^2)/(2nm) > 0$, on aurait $((m^2+2n^2)/(2nm))^2 \leqslant y^2$. Or l'inégalité $((m^2 + 2n^2)/(2nm))^2 > 2$ est équivalente à $(m^4 + 4m^2n^2 + 4n^2) - 8m^2n^2 > 0$. Comme $(m^4+4m^2n^2+4n^2)-8m^2n^2 = (m^4-4m^2n^2+4n^2) = (m^2-2n^2)^2 \geqslant 0$. De plus, comme $(m^2-2n^2) \neq 0$ [14], on a $(m^2 - 2n^2)^2 > 0$ ce qui est l'inégalité souhaitée. Ainsi, U n'admet pas de plus petit majorant et donc pas de borne supérieure.

C'est l'une des raisons du besoin de construire les nombres réels.

---

11. Cette formule est donnée par la méthode de Héron d'Alexandrie : la suite définie par récurrence par $u_0 = x > 0$ et $u_{n+1} = u_n/2 + 1/u_n$ converge en décroissant (à partir du rang 1) vers $\sqrt{2}$ par valeurs supérieures et la suite $v_n = 2/u_n$ converge en croissant (à partir du rang 1) vers $\sqrt{2}$ par valeurs inférieures
12. Cette formule est encore donnée par la relation d'Héron d'Alexandrie.
13. On utilise ici l'irrationalité de $\sqrt{2}$
14. Toujours par irrationalité de $\sqrt{2}$

Bibliographie

[A-F] J.-M. Arnaudiès et H. Fraysse. *Cours de Mathématiques - 1, algèbre*. Dunod Université, 1992.

[ZEK] Édouard Zeckendorf. Représentation des nombres naturels par une somme de nombres de fibonacci ou de nombres de lucas. *Bull. Soc. R. Sci. Liège*, 41 :179–182, 1972.