De la flêche $\mathbb{N}$ à la double flêche $\mathbb{Z}$

Alain Wazner

À chaque seconde qui passe
Achille divise par deux la distance qui le sépare de la tortue.
Achille va-t-il rattraper la tortue?

Préliminaires sur les ordinaux.

Dans tout l'article qui suit la théorie des ensembles est celle de Zermelo-Fraenkel. Nous utiliserons l'axiome du choix dépendant et appellerons ordinal tout ensemble o vérifiant les axiomes qui suivent :

- la relation $x \in y$ est sur o une relation d'ordre strict et toute partie de o admet un plus petit élément (on dit que $\in$ est un bon ordre).
- Si $P \in o$ alors $P \subset o$ (on dit que o est un ensemble transitif).

Segments initiaux d'un ordinal.

Soit o un ordinal et $x \in o$ nous appelons segment initial de sommet x de o l'ensemble $S(o,x) = \{y \in o | y \overset{\neq}{\in} x\}$.

Segments initiaux fermés d'un ordinal.

Un segment initial $S(o,x)$ d'un ordinal o est dit fermé s'il admet un plus grand élément pour la relation $\in$.

Des naturels.

Des ordinaux finis.

Nous appelons *axiome de l'infini* : la collection des ordinaux $\emptyset$, $\{\emptyset\}$, $\{\emptyset, \{\emptyset\}\}, \ldots$ est un ensemble bien ordonné par la relation $\in$, ce qui définit l'ensemble $\mathbb{N}$ des entiers naturels par

$0 \stackrel{déf}{=} \emptyset$

$1 \stackrel{déf}{=} \{\emptyset\}$

$2 \stackrel{déf}{=} \{\emptyset, \{\emptyset\}\}$

$\vdots$

$n+1 \stackrel{déf}{=} n \cup \{n\}$

$(n+1 \; est \; le \; suivant \; de \; n)$

$\vdots$

Définition des opérations et de la relation d'ordre sur $\mathbb{N}$ à partir d'opérations ensemblistes sur les ordinaux finis.

Si $n \neq 0 (= \emptyset)$ est un entier alors on définit $n-1$ le prédécesseur de n comme l'ordinal qui est le plus grand élément au sens de l'inclusion de n.
Le maximum des entiers m et n est défini par $Max(m,n) = m \cup n$, le minimum des entiers m et n est défini par $Min(m,n) = m \cap n$.
Addition : on définit $n+m$ l'addition récursivement par :
Si $m = 0$ alors n, sinon $n + (m-1) + 1$.

Multiplication : on définit $m \times n$ la multiplication de m par n récursivement par :
Si $m = 0$ alors 0 sinon, si $m = 1$ alors n sinon, $n \times (m-1) + n$.
Soustraction : si $n \subset m$ alors on définit $m - n$ récursivement par :
si $n = 0$ alors m sinon $(m-1) - (n-1)$ où $n-1$ et $m-1$ sont les plus grands éléments de n et de m.

Structuration de la collection des ordinaux successeurs de l'ensemble vide.

Opérateurs Add et Mult.

Supposant que nous disposions d'une fonction $Prec$ qui retourne le plus grand élément d'un ordinal fini alors nous définissons, sur la collection des ordinaux successeurs de l'ensemble vide, les opérateurs Add et $Mult$ par les fonctions récursives suivantes écrites en langage Python

$def \quad Add(m, n) :$
$\quad if\ n == \emptyset:$
$\quad\quad return\ m$
$\quad else\ return\ Add\,(m \cap \{m\}, Prec(n))$
$def \quad Mult(m, n) :$
$\quad if\ n == \emptyset:$
$\quad\quad return\ \emptyset$
$\quad else\ return\ Add\,(Mult\,(m, Prec(n))\,, n)$

Le théorème de fondement.

Si nous appelons ω_0 la collection des ordinaux successeurs de l'ensemble vide (c'est un ensemble d'après l'axiome de l'infini et ultérieurement nous le noterons $\mathbb{N}$) alors $(\omega_0, Add, Mult, \in)$ est un semi-anneau commutatif totalement ordonné dont les segments initiaux sont fermés.

Une preuve du théorème de fondement.

Parce qu'on nous l'a répété, souvent à partir du cours élémentaire, nous disons que $2+3 = 3+2$ ou que $2\times3 = 3\times2$, cependant la mathématique qui le prouve n'est pas aussi élémentaire, c'est pourquoi nous estimons qu'en rédiger une preuve est nécessaire et cela consistera à prouver qu'en codant Add et $Mult$ on arrive aux mêmes résultats si on inverse m et n. Pour la fonction Add imaginons que la nymphe Add gauchère se soit penchée au pied du berceau de l'immortelle Athèna et ait déposé n amphores de nectar à gauche et m amphores d'ambroisie à droite et lui ait dit : «À chacun de tes anniversaires tu boira une amphore de nectar à gauche, tu partira pour Troie guider Ulysse quand elles seront toutes vides et en t'attendant à chaque anniversaire de ton départ ton père $Zeus$ boira l'ambroisie à droite et tu reviendra quand il n'y aura plus d'ambroisie.» Si à présent la nymphe

Add est droitière et dépose n amphores de nectar à droite et m amphores d'ambroisie à gauche et lui dit : ≪À chacun de tes anniversaires tu boira une amphore de nectar à droite, tu partira pour Troie guider Ulysse quand elles seront toutes vides et en ton hommage à chaque anniversaire de ton départ ton père $Zeus$ boira l'ambroisie à gauche et tu reviendra quand elles seront toutes vides.≫ alors cela ne change rien à l'age d'Athéna à son retour.
Mais ce qu'ignore Athéna et savent les autres immortels de l'Olympe c'est que le jour de sa naissance la nymphe $Mult$ s'est penchée sur le berceau de l'immortel nouveau-né Hermès et a déposé à gauche de son berceau un damier de m lignes et n colonnes et lui a dit : ≪À chacun de tes anniversaires tu alignera mes n présents et un jour tu viendra chercher Ulysse pour le guider jusqu'à Troie, ton père $Zeus$ alignera mes n présents pour ton anniversaire et tu le retrouvera quand le damier sera rempli.≫ L'age d' Hermès à son retour ne changera pas si $Mult$ fait tourner le damier à angle droit et lui demande de déposer ses présents sur les colonnes.
Supposons que jusqu'à la date de départ d'Ulysse pour Troie, l'immortelle Athéna ai bu $Add(a, b)$ amphores de nectar, pendant le même temps l'immortel Hermès ai aligné $Mult(Add(a, b), n)$ pré-

sents sur son damier, soit d'abord $Mult(a, n)$ présents puis $Mult(b, n)$ présents. Ceci donne l'égalité

$$Mult(Add(a, b), n) = Add(Mult(a, n), Mult(b, n))$$

qui est la loi de distributivité de Add par rapport à $Mult$, ce qui se visualise - en notant $m+n$ pour $Add(m, n)$, $n \times m$ pour $Mult(n, m)$ et $n \leq m$ pour $n \in m$ à partir des deux lignes précédentes par

$$(a + b) \times n = a \times n + b \times n$$

Supposons qu'Athéna fête son $(a - 1)$-ième anniversaire lequel précède son $(b - 1)$-ième alors elle aura bu $a \leq b$ amphores de nectar...c années s'écoulent...au bout de ces c annés elle aura bu $a + c \leq b + c$ amphores de nectar, ce qui donne la relation $a \leq b \Rightarrow a + c \leq b + c$. Le jour du $(a - 1)$-ième anniversaire d'Athéna, Hermès aura aligné $a \times n \leq b \times n$ présents ce qui donne la relation $a \leq b \Rightarrow a \times n \leq b \times n$ et prouve que $(\omega_0, Add, Mult, \in)$ est un semi-anneau commutatif totalement ordonné et nous notons alors $\mathbb{N}$ pour ω_0.

Soit un segment initial $S(o, x)$ de ω_0 alors nous choisissons un élément $x_0 \in S(o, x)$ si x_0 n'est pas le plus grand élément de $S(o, x)$ alors nous choisissons x_1 tel que $x_0 \overset{\neq}{\in} x_1$...nous construisons ainsi une suite croissante d'éléments de $S(o, x)$, cette

suite est finie car $S(o,x)$ est un ordinal fini. Le dernier élément de la suite est alors le plus grand élément de $S(o,x)$.

Groupe ordonné.

Jusqu'à la fin des préliminaires $(\mathbb{I},+,\leq)$ est un groupe abélien totalement ordonné non trivial et possédant la propriété de la borne supérieure. La topologie sera la topologie définie par la métrique $d(x,y)=|x-y|=x-y$ si $y\leq x$, $y-x$ sinon.
Cette topologie est séparée et il revient au même de définir cette topologie en définissant les voisinages $V(c)$ de $c\in\mathbb{I}$ comme les intervalles $I_{a,b}=]a,b[=\{x\in\mathbb{I}/a\leq x\leq b\}\backslash\{a,b\}$ avec $a\neq b$ et $c\in I_{a,b}$.
Donnons quelques propriétés :

- un groupe totalement ordonné et possédant la propriété de la borne supérieure est complet.

  Preuve :

  Toute suite $(u_n)_{n\in\mathbb{N}}$ qui est de Cauchy est bornée si $\varepsilon>0\in\mathbb{I}$ alors, puisque $(u_n)_{n\in\mathbb{N}}$ est de Cauchy, $\exists N\in\mathbb{N}$ tel que $(q>p>N)\Rightarrow|u_q-u_p|<\varepsilon$. $(u_n)_{n\in\mathbb{N}}$

est alors bornée par $M = Max_{\{i \leq N\}}(|u_i|) + \varepsilon$. Selon la propriété de la borne supérieure la partie U de $\mathbb{I}$ égale à l'ensemble des valeurs prises par la suite de Cauchy, $(u_n)_{n\in\mathbb{N}}$ admet une borne supérieure u_+, elle admet aussi une borne inférieure $u_- \leq u_+$ (en effet la suite $(u_n)_{n\in\mathbb{N}}$ étant bornée, on peut appliquer la propriété de la borne supérieure à la suite de Cauchy $(-u_n)_{n\in\mathbb{N}}$). Pour $n \in \mathbb{N}$, les parties A_n de $\mathbb{I}$, définies par $\{u_p / p \geq n\}$ sont majorées par u_+, minorées par u_-, et décroissantes par inclusion, par la propriété de la borne supérieure les suites $S_n = Sup_{p\in A_n}(u_p)$ et $I_n = Inf_{p\in A_n}(u_p)$ sont bien définies et de plus $u_- \leq I_n \leq S_n \leq u_+ (\forall n \in \mathbb{N})$ par définition des bornes inférieures et supérieures. De plus, comme les parties A_n sont décroissantes par inclusion, $(S_n)_{n\in\mathbb{N}}$ est décroissante et $(I_n)_{n\in\mathbb{N}}$ est croissante.

Une suite croissante et majorée converge vers la borne supérieure de ses valeurs : soit $(u_n)_{n\in\mathbb{N}}$ une telle suite, nous posons $u = Sup_{n\in\mathbb{N}}(u_n)$. Soit $\varepsilon > 0$, alors $\exists N \in \mathbb{N}$ tel que $u_N + \varepsilon > u$, et pour tout $n > N$ on a par propriété de croissance et de la borne supérieure $u_N < u_n < u$. Sachant que $u_N + \varepsilon > u$, ceci entraîne que $|u - u_n| = u - u_n < u - u_N < \varepsilon$

soit $u = \lim_{n\to\infty} u_n$.
Si $(u_n)_{n\in\mathbb{N}}$ est décroissante et minorée alors la suite $(-u_n)_{n\in\mathbb{N}}$ est convergente comme suite croissante majorée, son opposée $(u_n)_{n\in\mathbb{N}}$ converge vers la borne inférieure de ses valeurs. Nous en déduisons qu'il existe $i \leq s$ tels que $i = lim_{n\to\infty} I_n$ et $s = lim_{n\to\infty} S_n$.
Soit $\varepsilon > 0$, alors du fait que $(u_n)_{n\in\mathbb{N}}$ est de Cauchy, $\exists N \in \mathbb{N}$ tel que $p > q > N \Rightarrow |u_p - u_q| < \varepsilon$, de $||u_p| - |u_q|| \leq |u_p - u_q|$ il suit que $||u_p| - |u_q|| < \varepsilon$. Dans l'assertion qui précède, on peut choisir tous les p tels que $p \geq N + 1$ et tous les q tels que $q \geq N + 2$ et, par passage aux bornes inférieures et÷ supérieures $|S_{N+1} - I_{N+2}| \leq \varepsilon$. Nous faisons à présent tendre N vers $+\infty$, il s'en suit que $(\forall \varepsilon > 0)\ 0 \leq |s - i| \leq \varepsilon$.
Cette assertion est équivallente à l'assertion la borne supérieure de la suite $(v_n)_{n\in\mathbb{N}}$ où $(\forall n \in \mathbb{N})\ v_n = |s - i|$ est 0 et comme cette suite est constante ceci entraîne que $s = i$.
Nous terminons la preuve en remarquant que le théorème des gendarmes s'applique à la suite $(u_n)_{n\in\mathbb{N}}$ puisqu'on a l'assertion $(\forall n \in \mathbb{N})$ $I_n \leq u_n \leq S_n$ avec

$$s = lim_{n\to\infty} S_n = lim_{n\to\infty} I_n = i$$

- Si $\mathbb{I}$ est un groupe totalement ordonné et possédant la propriété de la borne supérieure alors le théorème des valeurs intermédiaires s'applique, c'est à dire : soit $f : [a, b] \to \mathbb{I}$ une application continue, alors pour tout u compris entre $f(a)$ et $f(b)$, il existe c compris entre a et b tel que $f(c) = u$.
  Preuve : Supposons par exemple $f(a) \leq u \leq f(b)$, et notons X le sous-ensemble de l'intervalle $[a, b]$ constitué des $x \in \mathbb{I}$ qui vérifient $f(x) \leq u$.

  Cet ensemble est non vide (il contient a) et majoré (par b).

  Notons c sa borne supérieure et prouvons que $f(c) = u$.

  Comme c est une limite d'éléments de X, on a (par passage à la limite dans les inégalités) $f(c) \leq u$.
  Il reste à prouver que $f(c) \geq u$.
  Si $c = b$, c'est vrai par hypothèse.
  Si au contraire l'intervalle $]c, b]$ est non vide, comme ses éléments x vérifient tous $f(x) > u$, on obtient (à nouveau par passage à la limite) $f(c) \geq u$.

Cette inégalité et la précédente prouvent l'égalité voulue.

- Un groupe $\mathbb{I}$ totalement ordonné et possédant la propriété de la borne supérieure est archimédien :
  Soient $a, b \in \mathbb{I}$ avec $0 < a < b$, considérons $E = \{x \in < a > / x \geq 0\}$, où $< a >$ est le groupe engendré par a (les éléments de E sont les sommes répétées de a). Si la partie E est majorée, alors elle admet une borne supérieure S. Soit l'intervalle $I =]S - a, S[$, alors $< a > \supset I \cap E \neq \emptyset$ car dans le cas contraire $S - a$ est un majorant de E plus petit que S qui n'est pas alors une borne supérieure, soit $x \in I \cap E$ alors par définition de I on a $x + a > S$, $x + a \in < a >$ et S n'est pas la borne supérieure de E.
  E n'est donc pas bornée et $(\forall b > a)$ $(\exists x \in < a > / x > b)$.

Nous avons prouvé le résultat suivant : si $(\mathbb{I}, +, \times, \leq)$ est un groupe totalement ordonné vérifiant la propriété de la borne supérieure alors

- la norme naturelle sur $\mathbb{I}$ définit une topologie séparée sur $\mathbb{I}$ pour laquelle $\mathbb{I}$ est complet, archimédien, vérifie le théorème des valeurs intermédiaires.
- Il existe des preuves de ces théorèmes n'utilisant pas l'axiome du choix général.

Les sous-groupes de $\mathbb{I}$.

Tout $a \in \mathbb{I}\backslash\{0\}$ est d'ordre 0 (donc $< a >$ n'est pas fini et donc non plus $\mathbb{I}$: comme a et $-a$ sont deux éléments non-nuls de signes opposés et $< a >=< -a >$, on peut supposer $a > 0$. Si x est somme répétée de $a > 0$, comme $\mathbb{I}$ est groupe ordonné on a $x > 0$: a est donc d'ordre 0.
On pose alors $\mathbb{Z}_a \overset{déf}{=} < a >$.
Si G est un sous-groupe additif propre de $\mathbb{I}$ et si G n'est pas $\{0\}$, alors on peut trouver $x \in G$ avec $x \neq 0$, la partie de $\mathbb{I} \supset G^+ = \{g \in G | g > 0\}$ n'est pas vide puisque x ou $-x$ appartiennent à G^+, G^+ est donc minorée par 0 et admet alors une borne inférieure $a \geq 0$.

- Si $a = 0$ alors G est dense dans $\mathbb{I}$. En effet : $\forall \varepsilon > 0,\ \exists c \in G | 0 < c < \varepsilon$. $\mathbb{I}$ est archimédien

  $$(\forall \alpha \in \mathbb{I})\ (\exists x \in < c >) x \leq \alpha < x + c$$

  et donc $|\alpha - x| < \varepsilon$ et puisque $x \in < c >$, on a $x + c \in < c > \subset G$ tout élément $\alpha \in \mathbb{I}$ peut être approché à ε près par un élément de G qui est alors dense dans $\mathbb{I}$.

- Si $a > 0$ alors $a \in G^+$ car dans le cas contraire tout voisinage $V(a)$ de a contient des éléments de G^+ différents de a, il n'en contient pas un nombre fini car dans le cas contraire le minimum de ces éléments est la borne supérieure de

G^+ et elle est plus grande que a, soit à présent $\varepsilon > 0$ alors l'intervalle $]a, a+\varepsilon[$ contient au moins deux éléments distincts de G^+ et dont la différence positive toujours dans G^+ est plus petite que ε. Ceci étant vrai pour tout $\varepsilon > 0$ on a alors $a = 0$ ce qui est contradictoire. Soit à présent $g \in G$ alors comme $\mathbb{I}$ est archimédien $\exists x \in < a >$ tel que $x \leq g < x + a$ on a donc $0 \leq g - x < a$ et comme a est la borne inférieure de G^+ ceci entraîne que $g = x$ (sinon $g - x \in G^+$ est plus petit que a). Inversement tout $x \in a$ est dans G : on a donc

$$\mathbb{Z}_a =< a >= G$$

.

On peut déduire de la propriété de la borne supérieure la classification suivante : tout sous-groupe additif de $\mathbb{I}$ est :

- soit $\mathbb{Z}_a =< a >$ avec $a \in \mathbb{I}$.
- Soit dense dans $\mathbb{I}$.

Lemme des deux ouverts : si $\mathcal{O}_1$ et $\mathcal{O}_2$ sont deux ouverts denses de $\mathbb{I}$ alors $\mathcal{O}_1 \cap \mathcal{O}_2$ est un ouvert dense de $\mathbb{I}$.
Preuve : soit I un intervalle ouvert de $\mathbb{I}$ alors, comme $\mathcal{O}_1$ est un ouvert dense de $\mathbb{I}$, l'ouvert $I \cap \mathcal{O}_1$ contient un intervalle $I \cap \mathcal{O}_1 \supset I_1$, mais

$\mathcal{O}_2$ est un ouvert dense de $\mathbb{I}$ et par le même raisonnement l'ouvert $I_1 \cap \mathcal{O}_2$ contient un intervalle $I_1 \cap \mathcal{O}_2 \supset I_2$. Tout intervalle I contient un intervalle I_2 inclus dans $\mathcal{O}_1 \cap \mathcal{O}_2$ qui est un ouvert dense de $\mathbb{I}$ et nous pouvons en déduire que
Tout sous-groupe propre et dense de $\mathbb{I}$ n'est pas ouvert : si G est dense dans $\mathbb{I}$ alors supposons le ouvert, en se donnant un élément x de $\mathbb{I}$, son translaté $x + G$ est encore un ouvert dense dans $\mathbb{I}$ et en se donnant un autre élément y de $\mathbb{I}$: l'intersection $(y + G) \cap (x + G)$ est un ouvert dense de $\mathbb{I}$ par le lemme des deux ouverts. En particulier cette intersection n'est pas vide. Ceci prouve que le groupe quotient $\mathbb{I}/G$ ne contient qu'un élément qui ne peut-être que son neutre et donc que $\mathbb{I} = G$ n'est pas un sous-groupe propre de $\mathbb{I}$ (en effet les éléments de $\mathbb{I}/G$ sont les classes $x + G$ qui forment une partition de $\mathbb{I}$).

Des nombres entiers.

Dans tout ce qui suit $\mathbb{I}$ est un groupe abélien non trivial, totalement ordonné et possédant la propriété de la borne supérieure. On suppose de plus que $\mathbb{I}$ n'admet pas de sous-groupe propre et dense.
Nous utilisons dans tout ce qui suit la

convention suivante : on note $\mathbb{Z}_a$ le groupe $< a >$, défini comme l'ensemble des sommes finies de a ou de $-a$ où a est la borne inférieure des éléments positifs et non-nuls de $\mathbb{Z}_a$ (a est alors le plus petit élément positif et non-nul de $\mathbb{Z}_a$).

Diviseurs et p.g.c.d.

Diviseurs et multiples.

Définitions : Soit $a \in \mathbb{I}\backslash\{0\}$ et $b \in \mathbb{I}$, on dira que a est un diviseur de b si b est somme finie de a ou de $-a$, on dira aussi que b est multiple de a. *On convient que* 0 *est multiple de* 0*, ce qui revient à dire que* 0 *est diviseur de* 0.
On remarque que 0 ne divise jamais $a \neq 0$, ce qui revient à dire que $a \neq 0$ n'est jamais multiple de 0.
Propriété : soient $a > 0$, $b \geq 0$ deux éléments de $\mathbb{I}$ alors a est un diviseur de b si et seulement si $b \neq 0$ et $\mathbb{Z}_b \subset \mathbb{Z}_a$ (ce qui entraîne que $0 < a \leq b$).
Preuve : si b est somme finie de a alors toute somme finie de b est somme finie de a, ce qui équivaut à $\mathbb{Z}_b \subset \mathbb{Z}_a$. Si $\mathbb{Z}_b \subset \mathbb{Z}_a$ alors $b \in \mathbb{Z}_a$, soit si b est somme finie de a et donc multiple de a, soit a est un diviseur de b.
Conséquence : si $a \geq 0$ est un diviseur de $b > 0$

alors $0 < a \leq b$, on en déduit que

$$(a \geq 0) \wedge (b > 0) \wedge (\mathbb{Z}_b \subset \mathbb{Z}_a) \wedge (\mathbb{Z}_a \subset \mathbb{Z}_b) \Rightarrow (a = b > 0)$$

Notation : si $a, b > 0$ on note $a|b$ pour *a est un diviseur de b*, ce qui précède peut alors s'écrire

$$(a|b) \wedge (b|a) \Rightarrow (b = a)$$

Soit si a est diviseur de b et b est diviseur de a alors $b = a$.
Propriété : sur $\mathbb{I}^+ = \{i \in \mathbb{I} / i > 0\}$ la relation $a|b$ est une relation d'ordre.
Preuve : en effet $(a|b) \Leftrightarrow \mathbb{Z}_a \supset \mathbb{Z}_b$.

P.g.c.d.

Soient $a, b \in \mathbb{I}^+$ alors $\mathbb{Z}_a + \mathbb{Z}_b$ est un sous-groupe de $\mathbb{I}$. Si ce groupe est dense alors il n'est pas un sous-groupe propre de $\mathbb{I}$ c'est donc $\mathbb{I}$. Sinon $\mathbb{Z}_b + \mathbb{Z}_a = \mathbb{Z}_c$ où $c \in \mathbb{I}$. On a le
Lemme : $\forall a, b \in \mathbb{I}^+$ on a l'alternative :

- $\exists c \in \mathbb{I} / \ \mathbb{Z}_b + \mathbb{Z}_a = \mathbb{Z}_c$
- $\mathbb{Z}_b + \mathbb{Z}_a = \mathbb{I}$

Preuve : $\forall a, b \in \mathbb{I}^+$, $\mathbb{Z}_b + \mathbb{Z}_c$ est un sous-groupe de $\mathbb{I}$. Si c'est un sous-groupe propre alors c'est $\mathbb{Z}_c$.
Définitions : si $b, a \in \mathbb{I}^+$ et si $\mathbb{Z}_b + \mathbb{Z}_a = \mathbb{Z}_c$ alors on appelle c le p.g.c.d. (plus grand commun diviseur) de b et a. On a de plus

$b, a \in < c >$. Si $\mathbb{Z}_b + \mathbb{Z}_a = \mathbb{I}$ seront dits premiers entre eux.

Preuve : comme $\mathbb{Z}_b + \mathbb{Z}_c = \mathbb{Z}_c$ on a $\mathbb{Z}_c \supset \mathbb{Z}_a$ et $\mathbb{Z}_c \supset \mathbb{Z}_a$ il suit que $b \in < c >$, $a \in < c >$, mais comme $b, a > 0$ il suit que $c > 0$ (si $c = 0$ alors $b = a = c = 0$ puisque $< 0 >= \{0\}$).

Propriété : soient $b, a \in \mathbb{I}^+$, s'il existe c le p.g.c.d de b et a alors c'est le plus grand diviseur commun à b et a au sens *des deux relations d'ordres* $\leq$ et $|$.

Preuve :

- supposons que $\mathbb{Z}_b + \mathbb{Z}_a = \mathbb{Z}_c$ alors $\mathbb{Z}_b \subset \mathbb{Z}_c$ et $\mathbb{Z}_a \subset \mathbb{Z}_c$: c est donc un diviseur commun à b et a. La partie $D = \{i \in \mathbb{I}^+ / (i|b) \wedge (i|a)\}$ contient c et est majorée par le maximum de b et a elle admet une borne supérieure S.

  On a $S = c$: si $i|b$ alors $\mathbb{Z}_b \subset \mathbb{Z}_i$. Si $i|a$ alors $\mathbb{Z}_a \subset \mathbb{Z}_i$. Il suit que

  $$\mathbb{Z}_i + \mathbb{Z}_i = \mathbb{Z}_i \supset \mathbb{Z}_c = \mathbb{Z}_b + \mathbb{Z}_a$$

  On a prouvé que si $i|b$ et $i|a$ alors $i \leq c$ mais, puisque $c \in D$, on a alors $c = S$ qui est alors le plus grand élément de D.

  Réciproquement si c est le plus grand diviseur commun de b et a au sens de la relation d'ordre $\leq$ alors $\mathbb{Z}_b \subset \mathbb{Z}_c$ et $\mathbb{Z}_c \subset \mathbb{Z}_c$ et donc $\mathbb{Z}_b + \mathbb{Z}_a \subset \mathbb{Z}_c$. Si le groupe $\mathbb{Z}_b + \mathbb{Z}_a$ est dense dans $\mathbb{I}$ alors $\mathbb{I} = \mathbb{Z}_b + \mathbb{Z}_a$ d'où $\mathbb{I} = \mathbb{Z}_b + \mathbb{Z}_a = \mathbb{Z}_c$. Si **le**

groupe $\mathbb{Z}_b + \mathbb{Z}_a$ n'est pas dense dans $\mathbb{I}$ alors $\mathbb{Z}_b + \mathbb{Z}_a = \mathbb{Z}_d$ où $d \in \mathbb{I}^+$: d est d'après ce qui précède le plus grand diviseur commun de b et a au sens de la relation d'ordre $\leq$ on a donc $c = d$ par unicité du plus grand élément d'une partie.

- Au sens de la théorie des groupes la relation $\mathbb{Z}_b + \mathbb{Z}_a = \mathbb{Z}_c$ est équivallente à $\mathbb{Z}_c$ **est le plus petit sous-groupe $G \subset \mathbb{I}$ tel que** $G \supset \mathbb{Z}_b + \mathbb{Z}_a$. On a alors l'alternative suivante :
  - $\mathbb{Z}_b + \mathbb{Z}_a$ n'est contenu dans aucun sous-groupe propre de $\mathbb{I}$ alors $(\mathbb{Z}_c =) \mathbb{Z}_b + \mathbb{Z}_a = \mathbb{I}$: il n'y a qu'un seul d tel que $\mathbb{Z}_b \supset \mathbb{Z}_d$ et $\mathbb{Z}_a \supset \mathbb{Z}_d$ c'est c tel que $\mathbb{Z}_c = \mathbb{I}$, c'est donc le plus grand pour la relation $|$.
  - $\mathbb{Z}_b + \mathbb{Z}_a$ est contenu au moins un sous-groupe propre de $\mathbb{I}$ soit un $\mathbb{Z}_d$: le plus petit sous-groupe qui contient $\mathbb{Z}_b + \mathbb{Z}_a$ est nécessairement un sous-groupe propre de $\mathbb{I}$ donc $\mathbb{Z}_c$ **est le plus petit sous-groupe $\mathbb{Z}_d \subset \mathbb{I}$ tel que** $\mathbb{Z}_d \supset \mathbb{Z}_b + \mathbb{Z}_a$ soit c **est le plus grand diviseur commun à b et a au sens de la relation $|$.**

L'élément unité.

Afin d'une plus grande commodité, nous désignerons par ***a,b,c****,... c'est à dire* ***en caractères gras et minuscules*** *les relatifs et les naturels construits à partir de l'axiome de l'infini, et pour* $x \in \mathbb{I}$ *et* $\boldsymbol{n}$ *naturel* $\boldsymbol{n}x$ *signifiera* $Mult(n, x)$ *c'est à dire le résultat de l'éxécution en langage non typé Python de la fonction* $Mult$ *qui dépend des fonctions* Add *et* $Prec$*. On se servira de la notion de* ***module*** *pour faire du calcul algébrique sur* $\mathbb{I}$*. On remarque si* $x \in \mathbb{I}$ *alors* $\boldsymbol{0}.x = 0$ *et* $(\boldsymbol{n+1}).x = \boldsymbol{n}.x + x$ *où on a posé* $\boldsymbol{n}.x \stackrel{déf}{=} \boldsymbol{n}x$*. On peut,* ***des règles d'addition et de multiplication des naturels*** *déduire les règles :*

- *(i)* $\boldsymbol{0}.x = \boldsymbol{0}$
- *(ii)* $(\boldsymbol{n}+\boldsymbol{m}).x = \boldsymbol{n}.x + \boldsymbol{m}.x$
- *(iii)* $\boldsymbol{n}.(x + y) = \boldsymbol{n}.x + \boldsymbol{n}.y$
- *(iv)* $\boldsymbol{n}.(\boldsymbol{m}.x) = (\boldsymbol{n} \times \boldsymbol{m}).x$

où $x, y \in \mathbb{I}$ *et* $\boldsymbol{n}$ *et* $\boldsymbol{m}$ *sont des naturels. Ces règles s'étendent pour* $\boldsymbol{n}$ *et* $\boldsymbol{m}$ ***relatifs*** *si en définissant* $\boldsymbol{n}x$ *par* $\boldsymbol{n}.x$ *si le relatif* $\boldsymbol{n}$ *est un naturel (s'il est de signe positif) et* $\boldsymbol{n}.x$ *par* $\boldsymbol{-n}.(-x)$ *si le relatif* $\boldsymbol{n}$ *n'est pas un naturel (s'il est de signe négatif). Ainsi muni de l'opération*

externe . sur les relatifs le groupe $\mathbb{I}$ *devient un module sur les relatifs. Ce module est de plus* ***intègre****, il suit qu'il est régulier (c'est à dire* $(\boldsymbol{a}\neq 0) \wedge (\boldsymbol{a}y = \boldsymbol{a}x) \Rightarrow y = x$*).*

Éléments premiers, éléments unaires.

Éléments premiers. **Définition :** $p \in \mathbb{I}^+$ est premier si et seulement si $(\mathbb{Z}_p \supset \mathbb{Z}_p + \mathbb{Z}_a) \Rightarrow (\mathbb{Z}_p \supset \mathbb{Z}_a)$.

Éléments unaires. **Définition :** $u \in \mathbb{I}^+$ est unaire si et seulement si $(\mathbb{Z}_u \supset \mathbb{Z}_a) \Rightarrow (u = a)$, soit u est unaire s'il n'a pas d'autre diviseur que lui-même.

Propriétés.

- Soit $a, p \in \mathbb{I}^+$ où p est premier alors :
  - Soit p divise a.
  - Soit a et p sont premiers entre eux.
- Tout élément unaire est premier.
- Tout diviseur d'un élément premier autre que lui-même est unaire.
- S'il existe au moins un élément premier dans $\mathbb{I}^+$ alors il n'existe qu'un et un seul élément unaire noté $1_{\mathbb{I}}$. **On a alors** $\mathbb{I} = \mathbb{Z}_{1_{\mathbb{I}}}$ (*c.a.d. qu'à un isomorphisme près on a* $\mathbb{I} = \mathbb{Z}$).

Preuve :

- – Soit p premier, si $\mathbb{Z}_p \supset \mathbb{Z}_p + \mathbb{Z}_a$ alors $\mathbb{Z}_p \supset \mathbb{Z}_a$, soit p divise a.
  – Si $\mathbb{Z}_p + \mathbb{Z}_a = \mathbb{I}$ alors p est premier avec a.

- Soit u unaire et $a \in \mathbb{I}^+$, si $\mathbb{Z}_u \supset \mathbb{Z}_u + \mathbb{Z}_a$ alors, $a + u \in \mathbb{Z}_u$ et par différence $a \in \mathbb{Z}_u$ soit $u|a$ soit $\mathbb{Z}_u \supset \mathbb{Z}_a$. u est un élément premier.

- Soit p premier et $d \neq p$ tel que $\mathbb{Z}_d \supset \mathbb{Z}_p$ alors $\mathbb{Z}_p \not\supset \mathbb{Z}_d$ car sinon $\mathbb{Z}_p = \mathbb{Z}_d$ et $d = p$. Mais si $\mathbb{Z}_p \not\supset \mathbb{Z}_d$ alors p ne divise pas d et donc $\mathbb{Z}_d + \mathbb{Z}_p = \mathbb{I}$, mais puisque $\mathbb{Z}_d \supset \mathbb{Z}_p$ il vient $\mathbb{Z}_d + \mathbb{Z}_p = \mathbb{Z}_d = \mathbb{I}$: d est diviseur de tout élément de $\mathbb{I}^+$, il est donc unaire.

- S'il existe au moins un élément p premier dans $\mathbb{I}^+$: s'il n'admet pas de diviseur plus petit que lui, il est alors unaire, sinon p est unaire. S'il existe au moins un élément p premier alors il existe dans $\mathbb{I}^+$ au moins un élément u unaire et donc premier.
  S'il existe *au moins deux* éléments unaires alors, appelant u_2 et u_1 deux unaires distincts, ils sont premiers : aucun d'eux ne divise l'autre car alors ils sont égaux comme unaires, sinon nous considérons le groupe $G = \mathbb{Z}_{u_2} \cap \mathbb{Z}_{u_1}$:
  – Si $G = \mathbb{Z}_d$ alors de $\mathbb{Z}_d \subset \mathbb{Z}_{u_2}$ et $\mathbb{Z}_d \subset \mathbb{Z}_{u_1}$, on déduit qu'il existe deux naturels $\mathbf{m}$ et $\mathbf{n}$ tels que $d = \mathbf{m}u_1 = \mathbf{n}u_2$:

ceci entraîne alors la relation

$$\boxed{(1)\ d = \mathbf{m}u_1 = \mathbf{n}u_2}$$

Les éléments unaires distincts sont premiers entre eux et de $\mathbb{Z}_{u_1} + \mathbb{Z}_{u_2} = \mathbb{I}$ on déduit que $\boxed{(2)\exists \mathbf{a}, \mathbf{b}\ d = \mathbf{a}u_1 + \mathbf{b}u_2}$ où $\mathbf{a}$ et $\mathbf{b}$ sont des relatifs.

En répétant (2) $\mathbf{bm}$ fois on a (3) $\mathbf{bm}d = \mathbf{abm}u_1 + \mathbf{b}\times\mathbf{b}\times\mathbf{m}\ u_2$ et comme (1) répétée $\mathbf{ab}$ fois devient $\mathbf{abm}u_1 = \mathbf{abn}u_2$, (4) devient (5) $\mathbf{bm}d = (\mathbf{abn} + \mathbf{b}\times\mathbf{b}\times\mathbf{m})u_2$ puis (6) $\mathbf{bm}\mathrm{d} = \mathbf{b}\times(\mathbf{an}+\mathbf{bm})u_2$.

En répétant (2) $\mathbf{an}$ fois on a (7) $\mathbf{an}d = \mathbf{a}\times\mathbf{a}\times\mathbf{n}u_1 + \mathbf{anb}\ u_2$ et comme (1) répétée $\mathbf{ab}$ fois devient $\mathbf{abm}u_1 = \mathbf{abn}u_2$, (7) devient (8) $\mathbf{an}d = (\mathbf{a}\times\mathbf{a}\times\mathbf{n}+\mathbf{abm})u_1$ puis (9) $\mathbf{an}\mathrm{d} = \mathbf{a}\times(\mathbf{an}+\mathbf{bm})u_1$.

* Si $\exists \mathbf{a} \neq 0, \mathbf{b} \neq 0\ d = \mathbf{a}u_1 + \mathbf{b}u_2$ alors par régularité (6) et (9) deviennent $(S)\ \begin{cases} \mathbf{m}d = (\mathbf{an}+\mathbf{bm})u_2 \\ \mathbf{n}d = (\mathbf{an}+\mathbf{bm})u_1 \end{cases}$.
  En utilisant la relation $\mathbf{m}u_1 = \mathbf{n}u_2$ on a $(\mathbf{an}+\mathbf{bm})u_2 = \mathbf{m}(\mathbf{a}u_1 + \mathbf{b}u_2) = \mathbf{m}d$ et $(\mathbf{an}+\mathbf{bm})u_1 = \mathbf{n}(\mathbf{a}u_1 + \mathbf{b}u_2) = \mathbf{n}d$, on obtient donc $d = \mathbf{m}d = \mathbf{n}d$. Sachant que $d = \mathbf{m}u_1 = \mathbf{n}u_2$, il vient par différence $\mathbf{m}(d - u_1) = 0$ et $\mathbf{n}(d - u_2) = 0$. $\mathbf{m}$ et $\mathbf{n}$ ne peuvent être simultanément non nuls,

sinon les deux égalités qui précèdent entraînent $d = u_1$ et $d = u_2$ soit $u_1 = u_2$ ce que l'on n'a pas supposé. On a donc $\mathbf{m} = 0$ ou $\mathbf{n} = 0$: ce qui entraîne alors $d = 0$.

* Si $\forall \mathbf{a}, \mathbf{b}$ la relation $d = \mathbf{a}u_1 + \mathbf{b}u_2$ entraîne $\mathbf{a} = 0$ ou $\mathbf{b} = 0$ alors comme $d = \mathbf{m}u_1 = \mathbf{n}u_2$ c'est que $\mathbf{m} = 0$ ou $\mathbf{n} = 0$ soit $d = 0$.

On a prouvé que si $\mathbb{I}$ a deux éléments unaires u_1 et u_2 alors $\mathbb{Z}_{u_1} \cap \mathbb{Z}_{u_2} = \mathbb{Z}_0 = \{0\}$. Comme $\mathbb{Z}_{u_1} + \mathbb{Z}_{u_2} = \mathbb{I}$ on a donc $\mathbb{I} = \mathbb{Z}_{u_1} \oplus \mathbb{Z}_{u_2}$. Nous prouvons que cette relation est impossible grâce aux lemmes qui suivent :

lemme 1 : si $\mathbb{I} = \mathbb{Z}_{u_1} \oplus \mathbb{Z}_{u_2}$ alors pour tout $x \in \mathbb{I}$ il existe un unique couple $(\mathbf{a}, \mathbf{b})$ de relatifs tels que $x = \mathbf{a}u_1 + \mathbf{b}u_2$.

Preuve : puisque $I = \mathbb{Z}_{u_1} \oplus \mathbb{Z}_{u_2}$ c'est que pour tout $x \in \mathbb{I}$ il existe un couple de $(\mathbf{a}, \mathbf{b})$ de relatifs tels que $x = \mathbf{a}u_1 + \mathbf{b}u_2$. *Nous prouvons l'unicité de ce couple en prouvant que si les relatifs* $\boldsymbol{a}$, $\boldsymbol{b}$ *sont tels que* $\boldsymbol{a}u_1 + \boldsymbol{b}u_2 = 0$ *alors* $\boldsymbol{a} = \boldsymbol{b} = \boldsymbol{0}$. En effet si $\mathbf{a}u_1 + \mathbf{b}u_2 = 0$ alors $x = \mathbf{a}u_1 = -\mathbf{b}u_2 \in \mathbb{Z}_{u_1} \cap \mathbb{Z}_{u_2}$, donc $x = 0$ et puisque $0 = x = \mathbf{a}u_1 = -\mathbf{b}u_2$ ceci

entraîne que $\mathbf{a} = \mathbf{b} = \mathbf{0}$.

Lemme 2 :*pour tout relatif* $\boldsymbol{a}$, $u_1 + \boldsymbol{a}u_2$ *est unaire :* s'il existe un naturel $\mathbf{n}$ et $x \in \mathbb{I}$ tel que $u_1 + \mathbf{a}u_2 = \mathbf{n}x$ alors; si $(\mathbf{c}, \mathbf{b})$ est l'unique couple de relatifs tel que $x = \mathbf{b}u_1 + \mathbf{c}u_1$ alors $\mathbf{nb}u_1 + \mathbf{nc}u_2 = u_1 + \mathbf{a}u_2$ et par unicité de la décomposition sur u_1 et u_2 on a alors $\begin{cases} \mathbf{nb} = \mathbf{1} \\ \mathbf{nc} = \mathbf{a} \end{cases}$. L'équation aux naturel et relatif $\mathbf{nb} = \mathbf{1}$ a pour unique solution

$\mathbf{n} = \mathbf{b} = 1$, il suit que l'équation $\mathbf{nc} = \mathbf{a}$ devient l'égalité $\mathbf{c} = \mathbf{a}$: on a donc prouvé que si $\mathbf{n}x = u_1 + \mathbf{a}u_2$ alors $\mathbf{n} = \mathbf{1}$ et $x = u_1 + \mathbf{a}u_2$; $u_1 + \mathbf{a}u_2$ est donc unaire.

En particulier les deux éléments distincts $u_1 + u_2$ et $u_1 - u_2$ sont unaires et donc $\mathbb{I} = \mathbb{Z}_{u_1+u_2} \oplus \mathbb{Z}_{u_1-u_2}$: il existe un unique couple de relatifs $(\mathbf{a}, \mathbf{b})$ tels que

$$\begin{aligned} u_1 &= \mathbf{a}(u_1 + u_2) + \mathbf{b}(u_1 - u_2) \\ &= (\mathbf{a} + \mathbf{b})u_1 + (\mathbf{a} - \mathbf{b})u_2 \end{aligned}$$

ce qui entraîne que $\begin{cases} \mathbf{a} + \mathbf{b} = \mathbf{1} \\ \mathbf{a} - \mathbf{b} = \mathbf{0} \end{cases}$. On a alors : $\begin{cases} \mathbf{2a} = \mathbf{1} \\ \mathbf{a} = \mathbf{b} \end{cases}$ et comme l'équation aux relatifs $\mathbf{2a} = \mathbf{1}$ n'a pas de solution, ceci entraîne que le couple $(\mathbf{a}, \mathbf{b})$ ne peut

pas exister, ce qui est contradictoire.

Conclusions. *S'il existe au moins un élément premier alors il admet un diviseur unaire unique soit* $1_{\mathbb{I}}$ *et* ***on a alors*** $\mathbb{I} = \mathbb{Z}_{1_{\mathbb{I}}}$. *S'il n'existe aucun élément premier alors tout* $u > 0 \in \mathbb{I}$ *admet un diviseur plus petit et différent de lui-même et ce diviseur n'est pas premier : tout nombre de* $\mathbb{I}$ *est alors infiniment divisable, nous montrons dans ce qui suit que cela contredit que* $\mathbb{I}$ *est un groupe totalement ordonné possédant la propriété de la borne supérieure sans sous-groupe propre et dense.*

Peut-il n'exister aucun élément premier?

Nous supposons donc dans cette partie que tout élément de $u > 0 \in \mathbb{I}$ admet un diviseur différent et plus petit que lui-même.
Soient x, y deux éléments de $\mathbb{I}$ *distincts positifs et non nuls* et soit $G = \mathbb{Z}_x \cap \mathbb{Z}_y$ alors $\mathbb{I} \supsetneq G$ car dans le cas contraire $\mathbb{Z}_y = G = \mathbb{Z}_x$ et $x = y$ unaire.

$$\boxed{(\forall x, y \in \mathbb{I}_+^*)\,(\exists z \in \mathbb{I}_+^*)\ \ \mathbb{Z}_z = \mathbb{Z}_y \cap \mathbb{Z}_x}$$

- Si $\mathbb{Z}_x + \mathbb{Z}_y = \mathbb{I}$ de $\mathbb{Z}_z \subset \mathbb{Z}_x$ et $\mathbb{Z}_z \subset \mathbb{Z}_x$, on déduit qu'il existe deux naturels $\mathbf{m}$ et $\mathbf{n}$ tels que $\boxed{(1)\ z = \mathbf{m}x = \mathbf{n}y}$. Les éléments positifs non-nuls et distincts x, y sont premiers entre

eux, on en déduit que $\boxed{(2)\exists \mathbf{a},\mathbf{b}\ z=\mathbf{a}x+\mathbf{b}y}$ où $\mathbf{a}$ et $\mathbf{b}$ sont des relatifs. En substituant u_1 par x, u_2 par y et d par z au calcul de la page 18, on en déduit que :

$$(S_1)\ \begin{cases} \mathbf{bm}z &= \mathbf{b}\times(\mathbf{an}+\mathbf{bm})y \\ \mathbf{an}z &= \mathbf{a}\times(\mathbf{an}+\mathbf{bm})x \end{cases}$$

Le produit $\mathbf{ab}$ n'est pas 0 : s'il était alors $\mathbf{a}$ et $\mathbf{b}$ seraient *simultanément* nuls -puisque si un seul naturel parmi $\{\mathbf{a},\mathbf{b}\}$ est non nul alors $x|y$ ou $y|x$ ce qui contredit que $\mathbb{Z}_x+\mathbb{Z}_y=\mathbb{I}$- et on aurait $z=0$. Un naturel non nul étant régulier on a

$$(S_1)\Longleftrightarrow(S_2)\ \begin{cases} \mathbf{m}z &= \mathbf{an}+\mathbf{bm}y \\ \mathbf{n}z &= \mathbf{an}+\mathbf{bm}x \end{cases}$$

Par substitution de u_1 par x, u_2 par y et d par z au système (S) on obtient (S_2) et puisque $(S)\ \Rightarrow\ (d=0)$ on en déduit que $(S_2)\Rightarrow(z=0)$ ce qui contredit que $z\neq 0$.

- Si $\mathbb{Z}_x+\mathbb{Z}_y=\mathbb{Z}_w$ avec $w\in\mathbb{I}_*^+$ alors il existe deux relatifs $\mathbf{m}$ et $\mathbf{n}$ tels que $w=\mathbf{m}x+\mathbf{n}y$. w est le p.g.c.d. de x et y il existe donc des naturels $\mathbf{t}$ et $\mathbf{s}$ tels que $x=\mathbf{t}w$ et $x=\mathbf{s}w$. Puisque $\mathbb{Z}_z=\mathbb{Z}_y\cap\mathbb{Z}_x$, z est un multiple commun de x et y, il existe deux naturels $\mathbf{e}$ et $\mathbf{f}$ tels que $z=\mathbf{e}x=\mathbf{f}y$.
  Pour tout $x,y\in\mathbb{I}_+^*$ *où* $x\neq y$ *il existe*

$z, w \in \mathbb{I}_+^*$, quatre naturels $\boldsymbol{t}$, $\boldsymbol{s}$, $\boldsymbol{e}$, $\boldsymbol{f}$ et deux relatifs $\boldsymbol{m}$ et $\boldsymbol{n}$ tels que

$$(S_3)\begin{cases} w &= \mathbf{m}x + \mathbf{n}y \\ x &= \mathbf{t}w \\ y &= \mathbf{s}w \\ z &= \mathbf{e}x \\ z &= \mathbf{f}y \end{cases}$$

On a $0 = z - z = \mathbf{e}x - \mathbf{f}y = (\mathbf{e} \times \mathbf{t} - \mathbf{f} \times \mathbf{s})d$

$$\begin{aligned} 0 &= w - \mathbf{m}x - \mathbf{n}y \\ &= (\mathbf{1} - \mathbf{m} \times \mathbf{t} - \mathbf{n} \times \mathbf{s})w \end{aligned}$$

Comme w et d ne sont pas nuls ceci entraîne que $\begin{cases} \mathbf{e} \times \mathbf{t} - \mathbf{f} \times \mathbf{s} = \mathbf{0} \\ \mathbf{m} \times \mathbf{t} + \mathbf{n} \times \mathbf{s} = \mathbf{1} \end{cases}$ En substituant à la deuxième égalité la somme de $\mathbf{n}$ fois la première et de $\mathbf{f}$ fois la deuxième, on obtient $\begin{cases} \mathbf{e} \times \mathbf{t} - \mathbf{f} \times \mathbf{s} = \mathbf{0} \\ (\mathbf{fm} + \mathbf{ne}) \times \mathbf{t} = \mathbf{f} \end{cases}$ soit

$$(S_4)\begin{cases} \mathbf{e} \times \mathbf{t} = \mathbf{s} \times \mathbf{f} \\ (\mathbf{fm} + \mathbf{en}) \times \mathbf{t} = \mathbf{f} \end{cases}$$

$\mathbf{f}$ et $\mathbf{t}$ sont à même proportion donc

$$\mathbf{s} \times (\mathbf{fm} + \mathbf{en}) = \mathbf{e}$$

et en reportant $\mathbf{e}$ à la première ligne de (S_4) :

$$\mathbf{t} \times (\mathbf{fm} + \mathbf{en}) = \mathbf{f}$$

puis $\mathbf{f}$ dans (S_3)

$$\begin{cases} w &= \mathbf{m}x + \mathbf{n}y \\ x &= \mathbf{t}w \\ y &= \mathbf{s}w \\ z &= \mathbf{st} \times (\mathbf{fm} + \mathbf{en})w \end{cases}$$

Mais z est le plus petit élément du groupe des multiples commun à x et y dont $\mathbf{st}w$ est un élément, z est donc égal à $\mathbf{st}w$ et $\mathbf{fm} + \mathbf{en}$ à $\mathbf{1}$! Et de ce qui précède $\mathbf{s} = \mathbf{e}$, $\mathbf{t} = \mathbf{f}$, $\mathbf{tm} + \mathbf{sn} = \mathbf{1}$ ainsi que

$$\begin{cases} w &= \mathbf{m}x + \mathbf{n}y \\ x &= \mathbf{t}w \\ y &= \mathbf{s}w \\ z &= \mathbf{st} \times w \end{cases}$$

donc $\mathbf{s}x - \mathbf{t}y = (\mathbf{st} - \mathbf{ts}y)w = 0$ et $\mathbf{s}x + \mathbf{t}y = (\mathbf{st} + \mathbf{ts})w = \mathbf{2}z = \mathbf{2m}x + \mathbf{2n}y$ donne

$$(S_5) \begin{cases} \mathbf{s}x & - & \mathbf{t}y & = & 0 \\ (\mathbf{s} - \mathbf{2m})x & + & (\mathbf{t} - \mathbf{2n})y & = & 0 \end{cases}$$

dont la deuxième égalité est

$$((\mathbf{s} - \mathbf{2m})\mathbf{t} + (\mathbf{t} - \mathbf{2n})\mathbf{s})\, w = 0$$

Puisque $w \neq 0$ c'est que $(\mathbf{s} - \mathbf{2m})\mathbf{t} = (\mathbf{2n} - \mathbf{t})\mathbf{s}$
$\mathbf{t}$ divise $(\mathbf{2n} - \mathbf{t})\mathbf{s}$, il est premier avec $\mathbf{s}$ puisque $\mathbf{tm}+\mathbf{sn} = \mathbf{1}$, il divise donc $(\mathbf{2n}-\mathbf{t})$ et donc divise $\mathbf{2n}$ qui est égal à $\mathbf{at}$.
$\mathbf{s}$ divise $(\mathbf{s} - \mathbf{2m})\mathbf{t}$, il est premier avec $\mathbf{t}$ puisque

$\mathbf{tm} + \mathbf{sn} = \mathbf{1}$, il divise donc $(\mathbf{s} - \mathbf{2m})$ et donc divise $\mathbf{2m}$ qui est égal à $\mathbf{bs}$.
$(\mathbf{s} - \mathbf{2m})\mathbf{t} = (\mathbf{2n} - \mathbf{t})\mathbf{s}$ devient $(\mathbf{s} - \mathbf{bs})\mathbf{t} = (\mathbf{at} - \mathbf{t})\mathbf{a}$ soit $\mathbf{1} - \mathbf{b} = \mathbf{a} - \mathbf{1}$ soit $\mathbf{a} + \mathbf{b} = \mathbf{2}$. Il vient

$$\mathbf{2}w = \mathbf{2m}x + \mathbf{2n}y = \mathbf{bs}x + \mathbf{at}y = (\mathbf{a} + \mathbf{b})z = \mathbf{2}z$$

et donc $z = w$. Comme z est un multiple commun à x et y positifs et non nuls et w un diviseur qui leur est commun (le plus petit) on $x = y$. Ceci étant vrai pour tout $x, y > 0$ ceci prouve que le semi-groupe $\mathbb{I}^+$ **non trivial** n'a que deux éléments, et donc que $\mathbb{I}$ a trois éléments $-\alpha, 0, \alpha$ où α désigne l'unique élément positif non nul.
Mais alors $\mathbf{2}\alpha = \alpha + \alpha > 0$ et donc $\alpha = \alpha + \alpha$ soit $\alpha = 0$ ce qui est contradictoire!

Équivallence de la définition de $\mathbb{Z}$ comme groupe totalement ordonné et par les axiomes de Peano.

Une définition de $\mathbb{N}$ est donnée par «les axiomes de Peano»:

- l'élément appelé zéro et noté 0 est un entier naturel.
- Tout entier naturel n a un unique successeur noté $s(n)$.
- Aucun entier naturel n'a 0 pour successeur.

- Deux entiers naturels ayant même successeur sont égaux.
- Si un ensemble d'entiers naturels contient 0 et contient le successeur de chacun de ses éléments, alors cet ensemble est égal à $\mathbb{N}$.

Nous appelons $(\mathcal{P})$ la collection de ces d'axiomes, (∞) l'axiome de l'infini, et $(\mathcal{G})$ la collection des axiomes suivants :

- Les entiers relatifs forment un groupe commutatif $\mathbb{I}$ totalement ordonné.
- Les entiers relatifs possèdent la propriété de la borne supérieure.
- Tout sous-groupe propre de $\mathbb{I}$ n'est pas dense dans $\mathbb{I}$.

Étant données deux collections d'axiomes $(\mathcal{A})$ et $(\mathcal{B})$, $(\mathcal{A}) \wedge (\mathcal{B})$ désignera la réunion des collections d'axiomes de $(\mathcal{A})$ et de $(\mathcal{B})$.
Nous avons prouvé que si un groupe G vérifie la collection d'axiomes $(\mathcal{G}) \wedge (\infty)$ alors G et $\mathbb{Z}$ sont isomorphes.
D'autre part si un groupe G est isomorphe à $\mathbb{Z}$ par $\theta : G \to \mathbb{Z}$ alors il est totalement ordonné par la relation $\prec$ définie par

$$(\forall g_1, g_2 \in G)(g_1 \prec g_2) \Leftrightarrow (\theta(g_1) \leq \theta(g_2))$$

ces sous-groupes propres sont isomorphes aux sous-groupes propres de $\mathbb{Z}$ qui sont les $n\mathbb{Z}$ avec $n \in \mathbb{N}$, ce sont donc les $\theta^{-1}(n\mathbb{Z})$: ils ne sont pas denses dans G puisque la propriété qu'entre deux éléments de $n\mathbb{Z}$ il n'y en a aucun de $n\mathbb{Z}$ entraîne alors qu'entre deux éléments de $\theta^{-1}(n\mathbb{Z})$ il n'y en a aucun de $\theta^{-1}(n\mathbb{Z})$. L'isomorphisme θ permet de plus que $(G, +, \prec)$ vérifie la propriété de la borne supérieure. $G^+ = \{g \in G | 0 \prec g\}$ est alors isomorphe à $\mathbb{N}$ et vérifie les axiomes de Peano.
On a prouvé que si un groupe G est isomorphe à $\mathbb{Z}$ alors son demi-groupe des positifs vérifie les axiomes de Peano. Comme l'axiome de l'infini est l'un des axiomes de Zermelo-Fraenkel les axiomes de Peano se déduisent des axiomes de Zermelo-Fraenkel. Si les axiomes de Zermelo-Fraenkel sont consistants définir $\mathbb{Z}$ par les axiomes de Peano est équivallent à le définir à un isomorphisme près par les axiomes de groupe $(\mathcal{G})$.