

# La flèche $\mathbb{Z}$

Alain Wazner

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

## Les naturels et les relatifs

Dans tout ce qui suit la théorie des ensembles est la théorie de Zermelo-Fraenkel. Nous n'utiliseront ni l'axiome du choix, ni l'hypothèse du continu, ni leurs négations.

Nous rappelons **l'axiome de l'infini** : la collection des ordinaux  $\emptyset$ ,  $\{\emptyset\}$ ,  $\{\emptyset, \{\emptyset\}\}$ , ... est un ensemble bien ordonné par la relation  $\in$ . On définit les naturels par

- $0 = \emptyset$
- $1 = \{\emptyset\}$
- $2 = \{\emptyset, \{\emptyset\}\}$
- ⋮
- 
- $n + 1 = n \cup \{n\}$  :  $n + 1$  est le suivant de  $n$ .
- ⋮
- 

Si  $n \neq 0 (= \emptyset)$  alors on définit le précédent de  $n - 1$  de  $n$  comme l'ordinal qui est le plus grand élément (au sens de l'inclusion) de  $n$ .

Le maximum de  $m$  et  $n$  est défini par  $Max(m, n) = m \cup n$ , le minimum de  $m$  et  $n$  est défini par  $Min(m, n) = m \cap n$ .

**addition** : On définit l'addition de  $n + m$  par la fonction récursive : si  $m = 0$  alors  $n$  sinon  $n + (m - 1) + 1$  (où  $x + 1$  désigne le suivant de  $x$  et  $x - 1$  le prédécesseur de  $x$ ).

**Multiplication** : On définit la multiplication de  $m \times n$  par la fonction récursive : si  $m = 0$  alors  $0$  sinon si  $m = 1$  alors  $n$  sinon  $n \times (m - 1) + n$  (où  $n - 1$  est le prédécesseur de  $n$ ).

**Soustraction** : Si  $n \leq m$  alors on définit  $m - n$  par la fonction récursive : si  $n = 0$  alors  $m$  sinon  $(m - 1) - (n - 1)$  où  $n - 1$  et  $m - 1$  sont les prédécesseurs de  $n$  et de  $m$ . Ainsi structurés, les naturels forment un semi-groupe (et même un semi-anneau), on définit le groupe des relatifs comme le symétrisé du semi-groupe des naturels, puis l'anneau des relatifs en appliquant à la multiplication la règle des signes.

### **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  $I_{a,b} = ]a, b[ = \{x \in \mathbb{I} / a \leq x \leq b\} \setminus \{a, b\}$  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  $M = \text{Max}_{\{i \leq N\}} (|u_i|) + \varepsilon$ .

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  $S_n = \text{Sup}_{p \in A_n}(u_p)$  et  $I_n = \text{Inf}_{p \in A_n}(u_p)$  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  $u = \text{Sup}_{n \in \mathbb{N}}(u_n)$ . 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  $u = \lim_{n \rightarrow \infty} u_n$ .

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  $i = \lim_{n \rightarrow \infty} I_n$  et  $s = \lim_{n \rightarrow \infty} S_n$ .**

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 équivalente 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 du gendarme 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

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

- 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  $f : [a, b] \rightarrow \mathbb{I}$  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  $E = \{x \in \langle a \rangle / x \geq 0\}$ , où  $\langle a \rangle$  est le groupe engendré par  $a$  (les éléments de  $E$  sont les sommes répétées de  $a$ ). Si la partie  $E$  est majorée, alors elle ad-

met une borne supérieure  $S$ . Soit l'intervalle  $I = ]S - a, S[$ , alors  $\langle a \rangle \supset I \cap E \neq \emptyset$  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  $x + a > S$ ,  $x + a \in \langle a \rangle$  et  $S$  n'est pas la borne supérieure de  $E$ .  $E$  n'est donc pas bornée et  $(\forall b > a) (\exists x \in \langle a \rangle / x > b)$ .



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.

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

**Tout  $a \in \mathbb{I} \setminus \{0\}$  est d'ordre 0 (donc  $\langle a \rangle$  n'est pas fini et donc non plus  $\mathbb{I}$  :** comme  $a$  et  $-a$  sont deux éléments non-nuls de signes opposés et  $\langle a \rangle = \langle -a \rangle$ , 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  $\mathbb{Z}_a \stackrel{\text{déf}}{=} \langle a \rangle$ .**

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 :

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

et donc  $|\alpha - x| < \varepsilon$  et puisque  $x \in \langle c \rangle$ , on a  $x + c \in \langle c \rangle \subset G$  tout élément  $\alpha \in \mathbb{I}$  peut être approché à  $\varepsilon$  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 mini-

mum 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  $\varepsilon$ . 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  $\exists x \in \langle a \rangle$  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

$$G = \langle a \rangle = \mathbb{Z}_a$$

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

- soit  $\mathbb{Z}_a = \langle a \rangle$  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 raison-

nement 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  $G = \mathbb{I}$  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  $\langle a \rangle$ , défini comme l'ensemble des sommes répétées 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  $a \in \mathbb{I} \setminus \{0\}$  et  $b \in \mathbb{I}$ , on dira que  $a$  est un diviseur de  $b$  si  $b$  est somme répétée 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 répétée de  $a$  alors toute somme répétée de  $b$  est somme répétée 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 répétée 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  $\mathbb{Z}_a + \mathbb{Z}_b = \mathbb{Z}_c$  où  $c \in \mathbb{I}$ . On a le

**Lemme :**  $\forall a, b \in \mathbb{I}^+$  on a l'alternative :

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

**Preuve :**  $\forall a, b \in \mathbb{I}^+$ ,  $\mathbb{Z}_a + \mathbb{Z}_b$  est un sous-groupe de  $\mathbb{I}$ . Si c'est un sous-groupe propre alors c'est  $\mathbb{Z}_c$ .

**Définitions :** Si  $a, b \in \mathbb{I}^+$  et si  $\mathbb{Z}_a + \mathbb{Z}_b = \mathbb{Z}_c$  alors on appelle  $c$  le p.g.c.d (plus grand commun diviseur) de  $a$  et  $b$ . On a de plus  $a, b \in \langle c \rangle$ . Si  $\mathbb{Z}_a + \mathbb{Z}_b = \mathbb{I}$  seront dits premiers entre eux.

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

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

**Preuve :**

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

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

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

On a prouvé que si  $i|a$  et  $i|b$  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  $a$  et  $b$  au sens de la relation d'ordre  $\leq$  alors  $\mathbb{Z}_a \subset \mathbb{Z}_c$  et  $\mathbb{Z}_b \subset \mathbb{Z}_c$  et donc  $\mathbb{Z}_a + \mathbb{Z}_b \subset \mathbb{Z}_c$ . Si **le groupe  $\mathbb{Z}_a + \mathbb{Z}_b$  est dense dans  $\mathbb{I}$  alors  $\mathbb{I} = \mathbb{Z}_a + \mathbb{Z}_b$  d'où  $\mathbb{I} = \mathbb{Z}_a + \mathbb{Z}_b = \mathbb{Z}_c$ . Si **le groupe  $\mathbb{Z}_a + \mathbb{Z}_b$  n'est pas dense dans  $\mathbb{I}$  alors  $\mathbb{Z}_a + \mathbb{Z}_b = \mathbb{Z}_d$****

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

#### L'élément unité

*Afin d'une plus grande commodité, nous désignerons par  $\mathbf{a}, \mathbf{b}, \mathbf{c}, \dots$  c'est à dire **en caractères gras et minuscules** les relatifs et les naturels construits à partir de l'axiome de l'in-*



fini, et pour  $x \in \mathbb{I}$  et  $\mathbf{n}$  naturel  $\mathbf{n}x$  signifiera répéter  $x$  « en comptant  $\mathbf{n}$  sur les ordinaux ». On se servira de la notion de **module** pour faire du calcul algébrique sur  $\mathbb{I}$ . On remarque si  $x \in \mathbb{I}$  alors  $\mathbf{0}x = 0$  et  $(\mathbf{n}+\mathbf{1})x = \mathbf{n}x + x$  et on pose  $\mathbf{n}.x \stackrel{\text{def}}{=} \mathbf{n}x$ . On peut, **des règles d'addition et de multiplication des naturels** déduire les règles :

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

où  $x, y \in \mathbb{I}$  et  $\mathbf{n}$  et  $\mathbf{m}$  sont des naturels. Ces règles s'étendent pour  $\mathbf{n}$  et  $\mathbf{m}$  relatifs si en définissant  $\mathbf{n}.x$  par  $\mathbf{n}x$  si le relatif  $\mathbf{n}$  est un naturel (s'il est de signe positif) et  $\mathbf{n}.x$  par  $-\mathbf{n}.(-x)$  si le relatif  $\mathbf{n}$  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  $(\mathbf{a} \neq 0) \wedge (\mathbf{a}x = \mathbf{a}y) \Rightarrow x = y$ ).

Eléments premiers, éléments unaires

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

**Eléments 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.ad.* *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  $\mathbb{Z}_p \not\subset \mathbb{Z}_d$  car sinon  $\mathbb{Z}_p = \mathbb{Z}_d$  et  $d = p$ . Mais si  $\mathbb{Z}_p \not\subset \mathbb{Z}_d$  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  $u_1$  et  $u_2$  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  $G = \mathbb{Z}_{u_1} \cap \mathbb{Z}_{u_2}$  :

- Si  $G = \mathbb{Z}_d$  alors de  $\mathbb{Z}_d \subset \mathbb{Z}_{u_1}$  et  $\mathbb{Z}_d \subset \mathbb{Z}_{u_2}$ , 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  $(1) d = \mathbf{m}u_1 = \mathbf{n}u_2$ .

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

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

En répétant (2)  $\mathbf{a}\mathbf{n}$  fois on a  
 (7)  $\mathbf{a}\mathbf{n}d = \mathbf{a} \times \mathbf{a} \times \mathbf{n}u_1 + \mathbf{a}\mathbf{n}\mathbf{b} u_2$  et comme (1)

répétée  $\mathbf{ab}$  fois devient  $\mathbf{abmu}_1 = \mathbf{abnu}_2$ ,  
(7) devient (8)  $\mathbf{and} = (\mathbf{a} \times \mathbf{a} \times \mathbf{n} + \mathbf{abm})u_1$   
puis (9)  $\mathbf{and} = \mathbf{a} \times (\mathbf{an} + \mathbf{bm})u_1$ .

– Si  $\exists \mathbf{a} \neq 0, \mathbf{b} \neq 0$   $d = \mathbf{au}_1 + \mathbf{bu}_2$  alors par  
régularité (6) et (9) deviennent

$$(S) \begin{cases} \mathbf{md} = (\mathbf{an} + \mathbf{bm})u_2 \\ \mathbf{nd} = (\mathbf{an} + \mathbf{bm})u_1 \end{cases}.$$

En utilisant la relation  $\mathbf{mu}_1 = \mathbf{nu}_2$  on a  
 $(\mathbf{an} + \mathbf{bm})u_2 = \mathbf{m}(\mathbf{au}_1 + \mathbf{bu}_2) = \mathbf{md}$  et  
 $(\mathbf{an} + \mathbf{bm})u_1 = \mathbf{n}(\mathbf{au}_1 + \mathbf{bu}_2) = \mathbf{nd}$ , on  
obtient donc  $d = \mathbf{md} = \mathbf{nd}$ . Sachant que  
 $d = \mathbf{mu}_1 = \mathbf{nu}_2$ , 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 en-  
traînent  $d = u_1$  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  $d = \mathbf{au}_1 + \mathbf{bu}_2$  entraîne  
 $\mathbf{a} = 0$  ou  $\mathbf{b} = 0$  alors comme  
 $d = \mathbf{mu}_1 = \mathbf{nu}_2$  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 impos-**

sible grâce aux lemmes qui suivent :

**lemme** : 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  $\mathbf{a}, \mathbf{b}$  sont tels que  $\mathbf{a}u_1 + \mathbf{b}u_2 = 0$  alors  $\mathbf{a} = \mathbf{b} = \mathbf{0}$ . 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  $\mathbf{a} = \mathbf{b} = \mathbf{0}$ .

*Pour tout relatif  $\mathbf{a}$ ,  $u_1 + \mathbf{a}u_2$  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 tels que  $x = \mathbf{b}u_1 + \mathbf{c}u_2$  alors  $\mathbf{n}\mathbf{b}u_1 + \mathbf{n}\mathbf{c}u_2 = u_1 + \mathbf{a}u_2$  et par unicité de la décomposition sur  $u_1$  et  $u_2$  on a alors 
$$\begin{cases} \mathbf{n}\mathbf{b} = \mathbf{1} \\ \mathbf{n}\mathbf{c} = \mathbf{a} \end{cases}$$
. L'équation aux naturel et relatif  $\mathbf{n}\mathbf{b} = \mathbf{1}$  a pour unique solution  $\mathbf{n} = \mathbf{b} = 1$ , il suit que l'équation  $\mathbf{n}\mathbf{c} = \mathbf{a}$  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 divisible, 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  $\mathbb{I} \not\supseteq G$  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  $\mathbb{Z}_z \subset \mathbb{Z}_y$ , 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 :

$$(S_1) \begin{cases} \mathbf{b}mz = \mathbf{b} \times (\mathbf{a}n + \mathbf{b}m)y \\ \mathbf{a}nz = \mathbf{a} \times (\mathbf{a}n + \mathbf{b}m)x \end{cases}$$

Le produit  $\mathbf{a}\mathbf{b}$  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

$$(S_1) \iff (S_2) \begin{cases} \mathbf{m}z = \mathbf{a}n + \mathbf{b}my \\ \mathbf{n}z = \mathbf{a}n + \mathbf{b}mx \end{cases}$$

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  $y = \mathbf{s}w$ . 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  $\mathbf{t}, \mathbf{s}, \mathbf{e}, \mathbf{f}$  et deux relatifs  $\mathbf{m}$  et  $\mathbf{n}$  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

$$\begin{cases} \mathbf{e} \times \mathbf{t} - \mathbf{f} \times \mathbf{s} = \mathbf{0} \\ (\mathbf{fm} + \mathbf{ne}) \times \mathbf{t} = \mathbf{f} \end{cases} \quad \text{soit}$$

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

$\mathbf{f}$  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

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

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  $\alpha$  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!

## Équivalence 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,  $(\infty)$  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  $\mathbb{I}$

Etant donnée 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  $\theta : G \rightarrow \mathbb{Z}$  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  $\theta$  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 il vérifie les «axiomes de Peano». Comme l'axiome de l'infini est l'un des axiomes de Zermelo-Fraenkel les «axiomes de Peano» s'en déduisent. Si les axiomes de Zermelo-Fraenkel sont consistants définir  $\mathbb{Z}$  par les «axiomes de Peano» est équivalent à le définir à un isomorphisme près par «les axiomes de groupe  $(\mathcal{G})$ ».**