De la sonde $\mathbb{N}$ et du traît $\mathbb{Z}$

Alain Wazner

Boussole anc. Aiguille aimentée flottant horizontalement dans un bol d'eau.
In la circum-navigation terrestre ses radios.

Six éléments de vocabulaire

- Opérande : pour une opération (addition, multiplication, ...) ce qui est ajouté, par quoi on multiplie, ...
- Opération : dans tout le texte une opération aura 2 opérandes et seulement 2.
- Argument : ce dont quoi dépend une fonction informatique . *Une fonction informatique a une liste finie d'arguments.*
- Argument retourné : le résutat obtenu après exécution de la fonction informatique. *Une fonction ne retourne qu'un seul argument.*
- Fonction :
  - Informatique : voir Argument.
  - Mathématique : acte par lequel on fait correspondre *univoquement* à toute partie, appelée *domaine de la fonction* d'un ensemble appelé *ensemble de départ* une partie d'un ensemble appelé *ensemble d'arrivée*, *univoquement* signifiant qu'à tout élément du domaine, appelé *antécédent* on fait correspondre un seul élément appelé *image* (de

l'antécédent) *par la fonction*. L'usage est d'appeler *image du domaine*, l'ensemble des éléments images de l'ensemble d'arrivée, l'ensemble d'arrivée existe *par le shéma d'axiomes de compréhension* de la théorie Zermelo-Fraenkel des ensembles.

- Récursivité : possibilité pour une fonction informatique de décrire la liste de ses arguments dont l'un au moins est la fonction argumentée elle-même. Une fonction définie par récursivité est *finiment récursive* s'il est possible de l'exécuter en un nombre fini d'appels à elle-même. Les exemples de fonctions récursives donnés dans ce texte sont des fonctions finiment récursives.

Et des naturels et des 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 $\emptyset$, $\{\emptyset\}$, $\{\emptyset, \{\emptyset\}\}, \ldots$ est un ensemble bien ordonné par la relation $\in$.
On définit les naturels par :

$$0 = \emptyset$$

$$1 = \{\emptyset\}$$

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

$$n + 1 = n \cup \{n\}$$

$n+1 = n \cup \{n\}$ est le **suivant** de n et si $n \neq 0 (= \emptyset)$ alors on définit le précédent $n-1$ 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 $n+m$ par la fonction récursive add :
$add(n,m)$:
si $m = 0$ **alors** n **sinon** $n + (m-1) + 1$ /* $x+1$ est le suivant de x et $x-1$ est le prédécesseur de x*/
Multiplication : On définit la multiplication de $n \times m$ par la fonction récursive $mult$:
$mult(n,m)$:
si $m = 0$ **alors** 0 **sinonsi** $m = 1$ **alors** n **sinon** $n \times (m-1) + n$ /* $n-1$ 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 multi-

plication 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 $I_{a,b} =]a, b[= \{x \in \mathbb{I} / a \leq x \leq b\} \backslash \{a, b\}$ 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 $(u_n)_{n\in\mathbb{N}}$ 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 $I_n = Inf_{p\in A_n}(u_p)$, $S_n = Sup_{p\in A_n}(u_p)$ 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 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** $i = s$**.**
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

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

- 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 le maximum et le minimum de $f(b)$ et $f(a)$, 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 $b, a \in \mathbb{I}$ avec $0 < a < b$, considérons $G = \{x \in < a > / x \geq 0\}$, où $< a >$ est le groupe engendré par a (ses éléments sont les sommes finies d'opérande a ou $-a$). La partie G n'est pas majorée car, dans le cas contraire, il existe une borne supérieure S de G **dans** $\mathbb{I}$ et pour tout $\epsilon > 0 \in \mathbb{I}$ il y a dans $]S - \epsilon,\ S]$ un élément g de G (sinon S n'est pas la borne supérieure de G). Deux cas se présentent alors :

  - $G = \mathbb{I}$ alors $S + a \in G > S$ et S n'est pas une borne supérieure de I et si $b = na$ alors $na \geq b < (n+1)b$.
  - G est un sous-groupe propre de $\mathbb{I}$ alors il n'est pas dense dans $\mathbb{I}$ et $\exists \epsilon > 0 \in \mathbb{I}$, $[S - \epsilon,\ S[\cap G = \emptyset$ et comme $\exists g \in G,\ g \in]S - \epsilon, S]$ ceci n'est possible que si $S \in G$ mais alors $G \ni g + S > S$ et S n'est pas la borne supérieure de G.

Nous en déduisons que G n'est pas minoré : si G etait minoré alors $-G = G$ serait majoré. Nous choisissons alors $g_1 \in G$ tel que $g_1 > b > 0$ et considérons l'ensemble $G_1 = \{h \in G / h <= g_1\}$, nous choisissons $g_2 \in G$ tel que $g_2 < b$ et considérons l'ensemble $G_2 = \{h \in G / h >= g_2\}$ alors $G_1 \cup G_2 = G$ et $H = G_1 \cap G_2 = [g_2, g_1] \cap G$ puis nous considérons l' ensemble $H_1 = \{h \in H \ h < b\}$ cet ensemble a une borne supérieure $h_1 \in \mathbb{I}$ et comme H_1 **est fini** c'est le plus grand élément de H_1 et $G \ni h_1 < g$, $h_1 + a$ n'est alors pas dans H_1, sinon h_1 ne serait pas son plus grand élément et donc $h_1 + a >= b$ ce qui prouve que $\mathbb{I}$ est archimédien.

,

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 $a \in \mathbb{I}\backslash\{0\}$ 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 finie de l'opérande $a > 0$, 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 $c + x \in < c > \subset G$ 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 $x = g$ (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 dense dans $\mathbb{I}$.**
- **soit $\mathbb{Z}_a =< a >$ avec $a \in \mathbb{I}$.**

Lemme des deux ouverts : si $\mathcal{O}_1$ et $\mathcal{O}_2$ sont deux ouverts denses de $\mathbb{I}$ alors $\mathcal{O}_2 \cap \mathcal{O}_1$ est un ouvert dense de $\mathbb{I}$.

Preuve : soit I un intervalle ouvert de $\mathbb{I}$ alors, comme $\mathcal{O}_2$ est un ouvert dense de $\mathbb{I}$, l'ouvert $I \cap \mathcal{O}_2$ contient un intervalle $I_2 \subset I \cap \mathcal{O}_2$; mais

$\mathcal{O}_1$ est un ouvert dense de $\mathbb{I}$ et par le même raisonnement l'ouvert $I_1 \cap \mathcal{O}_2$ contient un intervalle $I_1 \subset \mathcal{O}_2 \cap I$. Tout intervalle I contient un intervalle $I_2 \cap I_1$ inclus dans $\mathcal{O}_2 \cap \mathcal{O}_1$ 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 d'opérande a ou $-a$ 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 d'opérande a ou $-a$, 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 d'opérande a alors toute somme finie d'opérande b est somme finie d'opérande 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 d'opérande a et donc multiple de a, soit a est un diviseur de b.

Conséquence : Si $b > 0$ est un multiple de $a \geq 0$ alors $0 \leq a < b$, on en déduit que

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

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

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

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

P.g.c.d.

Soient $b, a \in \mathbb{I}^+$ alors $\mathbb{Z}_b + \mathbb{Z}_a$ 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 : $\forall b, a \in \mathbb{I}^+$ 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 : $\forall b,\ a \in \mathbb{I}^+$, $\mathbb{Z}_b + \mathbb{Z}_a$ est un sous-groupe non réduit à $\{0\}$ de $\mathbb{I}$. Si c'est un sous-groupe propre alors c'est un $\mathbb{Z}_c$ et on peut choisir $c > 0$.
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 $\mathbb{Z}_b + \mathbb{Z}_a = \mathbb{Z}_c$ on a $\mathbb{Z}_c \supset \mathbb{Z}_b$ 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 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 de 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

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

  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 rela-

tion d'ordre $\leq$ alors $\mathbb{Z}_c \supset \mathbb{Z}_b$ et $\mathbb{Z}_c \supset \mathbb{Z}_a$ 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 $d = c$ 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 équivalente à $\mathbb{Z}_c$ **est le plus petit sous-groupe** $G \subset \mathbb{I}$ **tel que** $\mathbb{Z}_b + \mathbb{Z}_a \subset G$. 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 $\mathbb{Z}_d \subset \mathbb{Z}_b$ et $\mathbb{Z}_d \subset \mathbb{Z}_a$ 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 répéter* x *« en comptant* $\boldsymbol{n}$ *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* $\boldsymbol{0}x = 0$ *et* $(\boldsymbol{n+1})x = \boldsymbol{n}x + x$ *et on pose* $\boldsymbol{n}.x \overset{déf}{=} \boldsymbol{n}x$*. 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* $(\boldsymbol{a}\neq 0) \wedge (\boldsymbol{a}.x = \boldsymbol{a}.y) \Rightarrow x = y$*).*

Eléments unaires et éléments premiers

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

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

Propriétés

(i) Soit $p, a \in \mathbb{I}^+$ où p est premier alors
   - Soit p divise a.
   - Soit p et a sont premiers entre eux.

(ii) Tout élément unaire est premier.

(iii) Tout diviseur d'un élément premier autre que lui-même est unaire.

(iv) 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* $\mathbb{Z} = \mathbb{I}$).

Preuve :

(i) – 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.

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

(iii) 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 $\mathbb{Z}_p + \mathbb{Z}_d = \mathbb{I}$, mais puisque $\mathbb{Z}_p \subset \mathbb{Z}_d$ il vient $\mathbb{Z}_p + \mathbb{Z}_d = \mathbb{Z}_d = \mathbb{I}$: d est diviseur de tout élément de $\mathbb{I}^+$ est donc unaire.

(iv) Nous supposons qu'il existe au moins un élément p premier dans $\mathbb{I}^+$ **et prouverons** *a posteriori* **que c'est bien le cas**.
Si p n'admet pas de diviseur plus petit que lui alors il est unaire *sinon* tout diviseur de 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 distincts** u_2 **et** u_1 dans $\mathbb{I}^+$ alors ils sont premiers et aucun d'eux ne divise l'autre car alors ils seraient égaux puisque unaires.
Si $\exists d > 0$ $\mathbb{Z}_{u_2} + \mathbb{Z}_{u_1} = \mathbb{Z}_d$ alors d est dans $\mathbb{I}$ un diviseur commun de u_2 et u_1 unaires donc $d = u_2$ **et** $d = u_1$ soit $u_1 = u_2$ qui est contra-

dictoire, ce qui prouve qu'alors $\mathbb{Z}_{u_2} + \mathbb{Z}_{u_1} = \mathbb{I}$. Si $\mathbb{Z}_{u_2} \cap \mathbb{Z}_{u_1} = \mathbb{I}$ alors $\mathbb{Z}_{u_2} = \mathbb{Z}_{u_1} = \mathbb{I}$ et en particulier $\mathbb{Z}_{u_1} = \mathbb{Z}_{u_2}$ soit $u_2|u_1$ et $u_1|u_2$ et donc $u_1 = u_2$ qui est contradictoire, ce qui prouve qu'alors $\mathbb{Z}_{u_2} \cap \mathbb{Z}_{u_1} = \mathbb{Z}_m$ avec $m \in \mathbb{I}$ et comme $\mathbb{Z}_{-m} = \mathbb{Z}_m$ on peut choisir $m \geq 0$ et comme $\mathbb{Z}_{u_2} \supset \mathbb{Z}_m$ il existe un **relatif a** tel que $\mathbf{a}.u_2 = m$ et comme m et u_2 ont même signe ce relatif est un **naturel**. De même, comme $\mathbb{Z}_{u_1} \supset \mathbb{Z}_m$ il existe un **relatif b** tel que $\mathbf{b}.u_1 = m$ et comme m et u_1 ont même signe ce relatif est aussi un **naturel**.

On peut choisir les naturels **b** et **a** premiers entre eux : si **c** est un diviseur commun à **b** et **a** soit **b=cb'** et **a=ca'** alors comme le $\mathbb{Z}$-module $(\mathbb{I}, +, .)$ est régulier

$\mathbf{b}.u_1 = \mathbf{a}.u_2 \Rightarrow \mathbf{cb'}.u_1 = \mathbf{ca'}.u_2 \Rightarrow \mathbf{b'}.u_1 = \mathbf{a'}.u_2$

On peut trouver deux relatifs **m** et **n** tels que $\mathbf{na}+\mathbf{mb}=1$ et on a $\begin{cases} u_1 &= \mathbf{na}u_1 + \mathbf{mb}u_1 \\ &= \mathbf{na}u_1 + \mathbf{ma}u_2 \\ &= \mathbf{a}.(\mathbf{n}u_1 + \mathbf{m}u_2) \end{cases}$

u_1 est unaire soit sans autre diviseur que lui-même, ceci entraîne que **a=1** et $\mathbf{n}u_1+\mathbf{m}u_2 = u_1$, la relation $\mathbf{a}.u_2 = \mathbf{b}.u_1$ devient $u_2 = \mathbf{b}.u_1$ u_2 unaire a pour diviseur u_1 donc $u_2 = u_1$ et nous concluons.

Il ne peut pas exister dans $\mathbb{I}$ deux nom-

bres unaires u_2 et u_1 distincts.

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.

Nous allons montrer, par des lemmes dûs à **Emmy Noether** (♪Erlangen 1882 🍃Bryn Mawr 1935) que tout élément non nul de $\mathbb{I}$ a un plus petit diviseur.

Nous rappelons les définitions et les lemmes- sans les démontrer- qui suivent :

- Un idéal $I \subset A$ est de type fini s'il est engendré par un nombre fini d'éléments de A.

- Un anneau A est noethérien si tout idéal $I \subset A$ est de type fini.
- Tout anneau principal est noethérien.
- Si l'anneau A est noethérien alors les propositions qui suivent sont équivalentes :
  (i) Tout idéal de A est de type fini.
  (ii) Toute suite croissante d'idéaux de A est stationnaire.
  (iii) Tout ensemble non vide d'idéaux de A a un élément maximal pour l'inclusion.
- Un A-module M est noethérien s'il satisfait aux conditions équivalentes suivantes :
  (i) Toute suite croissante de sous-modules de M est stationnaire.
  (ii) Tout sous-module de M est de type fini.

Soit $z \in \mathbb{I}\backslash\{0\}$ alors, puisque z est infiniment divisable, on peut, par utilisation de *l'axiome du choix dépendant*, construire une suite $(\mathbb{Z}_{z_n})_{n\in\mathbb{N}}$, strictement croissante au sens de l'inclusion, de sous -modules du $\mathbb{Z}$-module noethérien $(\mathbb{I}, +, .)$ (ses sous-modules sont les groupes $\mathbb{Z}_i,\ i \in \mathbb{I}$ qui sont de type fini). Par l'utilisation du lemme de Noether appliqué aux modules cette suite est stationnaire... ce qui contredit qu'elle est strictement croissante.

Équivalence de la définition de $\mathbb{Z}$ comme groupe normé totalement ordonné vérifiant la propriété de la borne supérieure sans sous-groupe dense et de celle par les axiomes de Le Peano

Une définition de $\mathbb{N}$ est donnée par «les axiomes de Le 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.
- Les entiers forment un semi-groupe de neutre 0 en définissant l'addition $a+b$ par la fonction finiment récursive $add(a,b)$.

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 $(\mathbb{I},+,\leq)$ normé et totalement ordonné.
- Les entiers relatifs possèdent la propriété de la borne supérieure.
- Tout sous-groupe propre de $\mathbb{I}$ n'est pas dense dans $\mathbb{I}$.

- Le demi-groupe des entiers relatifs supérieur ou égaux à l'élément neutre de $\mathbb{I}$.

Étant données deux collections d'axiomes $(\mathcal{C})$ et $(\mathcal{A})$, $(\mathcal{C}) \wedge (\mathcal{A})$ désignera la réunion des collections d'axiomes de $(\mathcal{C})$ et $(\mathcal{A})$.
Soit $(\mathcal{C})$ la collection $(\mathcal{P} \wedge (\infty))$ et $(\mathcal{A})$ la collection $(\mathcal{G} \wedge (\infty))$.
Des axiomes de la collection $(\mathcal{C})$ nous avons déduit que le demi-groupe $G^+ = \{g \in G / 0 \prec g\}$ où $\prec$ est la relation d'ordre totale définie par

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

et la donnée d'un isomorphisme $\theta : \quad G \to \mathbb{Z}$, autrement dit θ est un isomorphisme de groupe totalement ordonné, vérifie les axiomes de la collection $(\mathcal{A})$, en effet :

- les sous-groupes propres de $\mathbb{Z}$ étant les $n\mathbb{Z}$ avec $n \in \mathbb{N}\backslash\{1\}$ les sous-groupes propres de G sont $\theta^{-1}(n\mathbb{Z})$ et 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 $\theta^{-1}(\mathbb{Z})$ au sens de $\prec$.
- G est normé par la l'ordre $\prec$ qui permet de construire une valeur absolue par différence positive ou nulle au sens de $\prec$.

- G^+ vérifie la propriété de la borne supérieure. Soit H une partie majoré de G, elle est totalement ordonné alors $\theta(H)$ est une partie totalement ordonné et majorée de $\theta(G) = \mathbb{Z}$ et admet une borne supérieure S et comme θ^{-1} est un isomorphisme de groupe totalement ordonné $\theta^{-1}(S) \in \mathbb{I}$ est la borne supérieure de $H = \theta^{-1}(\theta(H))$.
- Soit H un sous-groupe propre de G alors $\theta(H)$ est un sous-groupe propre de H c'est un $n\mathbb{Z}$ avec $n > 1$ qui n'est pas dense dans $\mathbb{Z}$ donc $\theta^{-1}(n\mathbb{Z}) = H$ n'est pas dense dans $\theta^{-1}(\mathbb{Z}) = \mathbb{I}$.

Des axiomes de la collection $(\mathcal{C})$ nous avons déduit les axiomes de la collection $(\mathcal{A})$ et des axiomes de la collection $(\mathcal{A})$ nous avons déduit les axiomes de la collection $(\mathcal{C})$ ce qui prouve l'équivalence

$$(\mathcal{P}) \wedge (\infty) \longleftrightarrow (\mathcal{G}) \wedge (\infty)$$

Fini à Eybens le 23 Janvier 2019, 8h 42 locale