L'anneau $\mathbb{Z}$, sous-groupes additifs de $\mathbb{Z}$. Les idéaux de $\mathbb{Z}$ sont principaux, égalité de Bezout. Résolution dans $\mathbb{Z}$ des équations de la forme $ax + by = c$.

Pré-requis:
- ◇ $\mathbb{N}$: Les lois $+$ et $\cdot$, sa structure d'ordre.
- ◇ La division euclidienne.

0.1 L'anneau $\mathbb{Z}$.

Il s'agit ici de symétriser l'opération d'addition sur $\mathbb{N}$ afin de pouvoir résoudre les équations de la forme

$$a + x = b \text{ où } (a, b) \in \mathbb{N}^2$$

qui admet une unique solution dès lors que $b \geq a$.

Proposition 0.1.1.
La relation $\mathcal{R}$ définie sur $\mathbb{N} \times \mathbb{N}$ par

$$(a, b)\mathcal{R}(a', b') \text{ si, et seulement si } a + b' = a' + b$$

est une relation d'équivalence.

Démonstration. $a + b = a + b$ implique que $(a, b)\mathcal{R}(a, b)$.

La commutativité de l'addition donne immédiatement que $(a, b)\mathcal{R}(a', b') \Leftrightarrow (a', b')\mathcal{R}(a, b)$.

Si $(a, b)\mathcal{R}(a', b')$ et $(a', b')\mathcal{R}(a'', b'')$ alors $a + b' = b + a'$ et $a' + b'' = a'' + b'$ donc $a = b + a' - b'$ et $b'' = b' + a'' - a'$ d'où $a + b'' = b + a''$ c'est-à-dire $(a, b)\mathcal{R}(a'', b'')$. ■

Définition 0.1.2.
L'ensemble quotient $\mathbb{N} \times \mathbb{N}/\mathcal{R}$ sera appelé l'ensemble des entiers relatifs que l'on notera $\mathbb{Z}$. $\overline{(a, b)}$ sera la classe d'équivalence contenant (a, b).

On va maintenant munir $\mathbb{Z}$ d'une structure de groupe abélien en définissant l'opération:

$$\overline{(a, b)} + \overline{(a', b')} = \overline{(a + a', b + b')}$$

en remarquant qu'elle ne dépend pas du représentant choisit.

On définit de même une multiplication sur $\mathbb{Z}$ de la manière suivante:

$$\overline{(a, b)} \times \overline{(a', b')} = \overline{(aa' + bb', ab' + ba')}$$

qui ne dépend pas non plus du choix du représentant.

Ces deux opérations confèrent à $\mathbb{Z}$ une structure d'anneau commutatif unitaire.

Si on considère le plongement

$$\begin{array}{rccc} \varphi : & \mathbb{N} & \longrightarrow & \dfrac{\mathbb{Z}}{(n, 0)} \\ & n & \longmapsto & \end{array} \quad (\varphi \text{ est bien injective})$$

on peut voir $\mathbb{N}$ comme une partie de $\mathbb{Z}$ et on peut identifier n et la classe de $(n,0)$.

D'après l'opération $+$ définie sur $\mathbb{Z}$, l'opposé de n et la classe de $(0,n)$ et sera noté $-n$.

De ces notations on déduit $\overline{(a,b)} = a-b$.

Les éléments de $\mathbb{N}$ seront les éléments positifs de $\mathbb{Z}$. D'où la relation d'ordre sur $\mathbb{Z}$ qui prolonge celle de $\mathbb{N}$ que l'on notera $\leq$:

$$x \leq y \Leftrightarrow x - y \in \mathbb{N}.$$

Proposition 0.1.3.
Cette relation est compatible avec la structure d'anneau de $\mathbb{Z}$:

$$x \leq y \Leftrightarrow x+z \leq y+z \text{ pour tout } z \in \mathbb{Z}$$

et

$$x \leq y \Leftrightarrow xz \leq yz \text{ pour tout } z \in \mathbb{N}^*$$

Remarque: la relation $\leq$ est un ordre total.

Munit de cette relation d'ordre, $\mathbb{Z}$ est archimédien: Si $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$ alors il existe $n \in \mathbb{Z}$ tel que $nb \geq a$.

Ainsi, $\mathbb{Z}$ est un anneau unitaire intègre commutatif totalement ordonné et archimédien.

0.2 Sous-groupes et idéaux de $\mathbb{Z}$.

Théorème 0.2.1.
Les sous-groupes de $(\mathbb{Z},+)$ sont exactement les ensembles

$$n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}, n \in \mathbb{N}.$$

Démonstration. Tout d'abord $n\mathbb{Z}$ est bien un sous-groupe de $(\mathbb{Z},+)$.

Soit G un sous-groupe de $(\mathbb{Z},+)$:

- ◇ Si $G = \{0\}$, alors $G = 0 \cdot \mathbb{Z}$.
- ◇ Si $G \neq \{0\}$, alors il existe g dans G strictement positif (positif et non nul) car G est un groupe. Soit alors

$$n = \min\{g : g \in G \setminus \{0\} \text{ et } g \geq 0\}.$$

  - $n\mathbb{Z} \subset G$ (car $n+n+n+\ldots \in G$);
  - Montrons que $G \subset n\mathbb{Z}$: Soit $a \in G$, effectuons la division euclidienne de a par n, alors il existe q et r dans $\mathbb{Z}$ tels que:

$$|a| = nq + r \text{ et } 0 \leq r < n \text{ où } |a| = \begin{cases} a & \text{si } a \geq 0 \\ -a & \text{sinon} \end{cases}.$$

Or $r = |a| - nq \in G$ et $r < n$ ce qui contredit le fait que n soit le plus petit élément non nul de G donc $r = 0$, ainsi $|a| = nq$ c'est-à-dire $a = \pm nq$ donc $a \in n\mathbb{Z}$.

■

Exercice: Soit G un sous-groupe de $\mathbb{Z}$, montrer qu'il existe un unique $n \in \mathbb{N}$ tel que $G = n\mathbb{Z}$.

Théorème 0.2.2.

1. Tout idéal de l'anneau $\mathbb{Z}$ est principal.
2. $\mathbb{Z}$ est principal.

Démonstration. Même démonstration que le théorème précédent en remplaçant G par I et $n\mathbb{Z} \subset I$ découle du fait que I est un idéal. ■

Exercice: Déterminer les idéaux de $\mathbb{Z}$ contenant $24\mathbb{Z}$.

0.3 Théorème de Bezout et équation du type $au + bv = c$, $a, b, c \in \mathbb{Z}$.

Proposition 0.3.1.
Soit $(a, b) \in \mathbb{N}^2$. L'ensemble

$$a\mathbb{Z} + b\mathbb{Z} = \{au + bv : (u, v) \in \mathbb{Z}^2\}$$

est un sous-groupe de $\mathbb{Z}$ et il existe un unique d dans $\mathbb{N}$ tel que:

$$a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}.$$

On dira que d est le plus grand commun diviseur de a et b et on notera $d = (a, b) = a \wedge b = \text{pgcd}(a, b)$.

Corollaire 0.3.2.
$d = (a, b)$ si, et seulement si $d|a$, $d|b$ et pour tout d' dans $\mathbb{N}$ vérifiant $d'|a$ et $d'|b$, $d'|d$.

Théorème 0.3.3.
(Théorème de Bezout)
Soient a et b dans $\mathbb{N}$.

$$(a, b) = 1 \Leftrightarrow \exists (u, v) \in \mathbb{Z}^2,\ au + bv = 1.$$

Démonstration. Si $(a, b) = 1$ alors $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$, en particulier, $1 \in a\mathbb{Z} + b\mathbb{Z}$ donc il existe $(u, v) \in \mathbb{Z}^2$ tel que $au + bv = 1$.

S'il existe $(u, v) \in \mathbb{Z}^2$ tel que $au+bv = 1$, soit alors $d = (a, b)$; $d|a$ et $d|b$ donc $d|au+bv = 1$ donc $d = 1$ $(d \geq 0)$. ■

Théorème 0.3.4.
(Théorème de Gauss)
Soit $(a, b, c) \in \mathbb{Z}^3$ tel que $a|bc$ et $(a, b) = 1$ alors $a|c$.

Démonstration. $a|bc$ donc il existe k dans $\mathbb{Z}$ tel que $ka = bc$. Puisque $(a, b) = 1$, il existe $(u, v) \in \mathbb{Z}^2$ tel que $au + bv = 1$ d'où $acu + bcv = c$ donc $a(cu + kc) = c$ c'est-à-dire $a|c$. ■

Résolution dans $\mathbb{Z}$ de l'équation

$$\text{(E)} \quad ax + by = c.$$

Soit $d = (a, b)$,

- ◇ Si $d \nmid c$ alors d'après le théorème de Bezout (E) n'a pas de solution.
- ◇ Di $d|c$ alors l'équation (E) est équivalente à:

$$\text{(E')} \quad \frac{a}{d}x + \frac{b}{d}y = \frac{c}{d} \text{ avec } \left(\frac{a}{d}, \frac{b}{d}\right) = 1.$$

D'après le théorème de Bezout, il existe $(x_0, y_0) \in \mathbb{Z}^2$ tel que $\frac{a}{d}x_0 + \frac{b}{d}y_0 = 1$ ainsi $\left(\frac{c}{d}x_0, \frac{c}{d}y_0\right)$ est solution particulière de (E').
Soit (x, y) une autre solution de l'équation (E'), alors:

$$\frac{c}{d}\left(\frac{a}{d}x_0 + \frac{b}{d}y_0\right) = \frac{a}{d}x + \frac{b}{d}y \quad \Rightarrow \quad \frac{a}{d}\left(\frac{cx_0}{d} - x\right) = \frac{b}{d}\left(y - \frac{cy_0}{d}\right).$$

donc

$$\frac{a}{d} \,\Big|\, \frac{b}{d}\left(y - \frac{cy_0}{d}\right) \text{ et } \left(\frac{a}{d}, \frac{b}{d}\right) = 1$$

alors d'après le théorème de Gauss $\frac{a}{d} \,\big|\, \left(y - \frac{cy_0}{d}\right)$ donc il existe $k \in \mathbb{Z}$ tel que $y - \frac{cy_0}{d} = k\frac{a}{d}$ donc $y = \frac{cy_0}{d} + k\frac{a}{d}$. Donc

$$\frac{a}{d}\left(\frac{cx_0}{d} - x\right) = \frac{b}{d}\left(\frac{cy_0}{d} + k\frac{a}{d} - \frac{cy_0}{d}\right)$$

d'où

$$\frac{cx_0}{d} - x = \frac{b}{d}k$$

et par conséquent

$$x = \frac{cx_0}{d} - k\frac{b}{d}.$$

Reste à vérifier que les solutions trouvées sont aussi des solutions de (E):

$$a\left(\frac{cx_0}{d} - \frac{kb}{d}\right) + b\left(\frac{cy_0}{d} + \frac{ka}{d}\right) = c\left(\frac{a}{d}x_0 + \frac{b}{d}y_0\right) = c$$

donc

$$\mathcal{S}(\text{E}) = \left\{\left(c\frac{x_0}{d} - k\frac{b}{d}, c\frac{y_0}{d} + k\frac{a}{d}\right) : k \in \mathbb{Z}\right\}.$$

Exercice: Une troupe d'hommes et de femmes a dépensé $1000E$ dans une auberge.
Les hommes ont payé $19E$ chacuns
Les femmes ont payé $13E$ chacunes.
Combien y avait-t'il d'hommes et de femmes?