

# Leçon 12 : Anneau $(\mathbb{Z}, +, \times)$ - Sous-groupes et idéaux - Egalité de Bézout - $ax + by = c$

**Prérequis :**  $(\mathbb{N}, +, \times, \leq)$  - Déf. d'un groupe, d'un anneau, d'un idéal et caractérisation d'un sous-groupe - Toute partie  $\neq \emptyset$  de  $\mathbb{N}$  admet un plus petit élément - Relation d'équivalence.

## 1 L'anneau $(\mathbb{Z}, +, \times)$

**Théorème 1.1.** *A un isomorphisme laissant fixes les éléments de  $\mathbb{N}$  près, il existe un unique anneau commutatif  $\mathbb{Z}$  contenant  $\mathbb{N}$  dont les lois d'addition et de multiplication prolongent celles de  $\mathbb{N}$  et qui est engendré par  $\mathbb{N}$ .*

*On a  $0_{\mathbb{Z}} = 0_{\mathbb{N}}$ ,  $1_{\mathbb{Z}} = 1_{\mathbb{N}}$ ,  $\mathbb{N} \cup (-\mathbb{N}) = \mathbb{Z}$ ,  $\mathbb{N} \cap (-\mathbb{N}) = \{0\}$ .  $\mathbb{Z}^* = \{-1, 1\}$  et  $\mathbb{Z}$  est intègre.*

**Théorème 1.2.** *Il existe une unique relation d'ordre sur  $\mathbb{Z}$  prolongeant celle de  $\mathbb{N}$  et compatible avec l'addition. Elle est totale et  $\mathbb{N}x = \mathbb{Z}|x \geq 0$ . En particulier,  $a \geq 0$  et  $b \geq 0 \implies ab \geq 0$*

**Théorème 1.3.**  $\forall x \in \mathbb{Z}, \{x, -x\} \cap \mathbb{N}$  est réduit à un seul élément. Cet élément s'appelle valeur absolue de  $x$  et se

$$\text{note } |x|. \text{ On a } \begin{cases} |x| = 0 \iff x = 0 \\ |x + y| \leq |x| + |y| \\ |xy| = |x||y| \end{cases}$$

**Théorème 1.4 (Division euclidienne).**

*Soit  $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$ . Alors*

$$\exists!(q, r) \in \mathbb{Z} \times \mathbb{N} \text{ tel que } a = bq + r \text{ et } 0 \leq r < |b|$$

## 2 Sous-groupes et idéaux

### 2.1 Sous-groupes de $(\mathbb{Z}, +)$

**Théorème 2.1.**  $(H, +)$  sous groupe de  $(\mathbb{Z}, +) \iff \exists a \in \mathbb{Z}$  tel que  $H = a\mathbb{Z}$ .

*Démonstration.*  $\Leftarrow$   $a\mathbb{Z}$  clairement sg de  $\mathbb{Z}$ .

$\Rightarrow$  Soit  $H$  un sg de  $\mathbb{Z}$ . Si  $H = \{0\}$ ,  $H = 0\mathbb{Z}$ .

Soit  $H \neq \{0\}$ . Posons  $H_+ = H \cap \mathbb{N}^*$ .  $H_+$  est un partie non vide de  $\mathbb{N}$  donc  $H_+$  admet un plus petit élément  $a$ .

Soit  $x \in H$ .  $x = aq + r$  avec  $0 \leq r < |a|$

$r = x - aq \in H$  or  $r < a$  donc  $r = 0$ ,  $x = aq$ ,  $H = a\mathbb{Z}$ .  $\square$

### 2.2 Idéaux de $(\mathbb{Z}, +, \times)$

**Théorème 2.2.**  $I$  idéal de  $A \iff \exists a \in \mathbb{Z}$  tel que  $I = a\mathbb{Z}$ .

## 3 Egalité de Bezout

### 3.1 PGCD

**Proposition 3.1.** *Soit  $a \in \mathbb{Z}$  et  $b \in \mathbb{Z}$ . Alors*

$a\mathbb{Z} + b\mathbb{Z} = \{x \in \mathbb{Z} | \exists (u, v) \in \mathbb{Z} \times \mathbb{Z} \text{ tq } x = au + bv\}$  est un sous-groupe de  $\mathbb{Z}$ .

**Définition 3.2.** Soit  $a \in \mathbb{Z}$  et  $b \in \mathbb{Z}$ . On appelle pgcd de  $a$  et  $b$  l'unique entier  $d \geq 0$  tel que  $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ .  $d$  est noté  $a \wedge b$ .

**Définition 3.3.** Soit  $a \in \mathbb{Z}$  et  $b \in \mathbb{Z}$ . On dit que  $a$  divise  $b$  si  $\exists k \in \mathbb{Z}$  tel que  $b = ak$ . On note  $a|b$ .

**Conséquence.**  $a|b \iff b\mathbb{Z} \subset a\mathbb{Z}$

**Proposition 3.4.** *Soit  $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ .*

$$a \wedge b = d \iff \begin{cases} d|a, d|b, d \geq 0 \\ \forall d' \text{ tq } d'|a \text{ et } d'|b \text{ alors } d'|d \end{cases}$$

*Démonstration.*  $\Rightarrow$  On sait que  $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ .

$a\mathbb{Z} \subset d\mathbb{Z} \implies d|a$  et  $b\mathbb{Z} \subset d\mathbb{Z} \implies d|b$ .

Si  $d'|a$ ,  $a\mathbb{Z} \subset d'\mathbb{Z}$  et si  $d'|b$ ,  $b\mathbb{Z} \subset d'\mathbb{Z}$

$\implies a\mathbb{Z} + b\mathbb{Z} \subset d'\mathbb{Z} \implies d\mathbb{Z} \subset d'\mathbb{Z} \implies d'|d$

$\Leftarrow$  On sait que  $d|a$ ,  $d|b$  et que si  $d'|a$  et  $d'|b$ ,  $d'|d$ .

Mq  $a\mathbb{Z} + b\mathbb{Z} \subset d\mathbb{Z}$ .

Si  $x \in a\mathbb{Z} + b\mathbb{Z}$ ,  $x = au + bv$ . Comme  $d|a$  et  $d|b$ ,  $x = a'du + b'dv = d(\dots) \in d\mathbb{Z}$ .

Mq  $d\mathbb{Z} \subset a\mathbb{Z} + b\mathbb{Z}$ .

$a\mathbb{Z} + b\mathbb{Z}$  sg de  $\mathbb{Z}$  donc  $= c\mathbb{Z}$ . Or  $\left. \begin{matrix} a\mathbb{Z} \subset c\mathbb{Z} \implies c|a \\ b\mathbb{Z} \subset c\mathbb{Z} \implies c|b \end{matrix} \right\} \implies$

$c|d \implies d\mathbb{Z} \subset c\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$   $\square$

**Propriétés 3.5.**  $a \wedge 1 = 1$

$a \wedge 0 = a$

$a \wedge b = b \wedge a$

$a|b \iff a \wedge b = |a|$

**Définition 3.6.** Soit  $(a, b) \in \mathbb{Z} \wedge \mathbb{Z}$ . On dit que  $a$  et  $b$  sont premiers entre eux (ou étrangers) si  $a \wedge b = 1$ .

### 3.2 Egalité de Bézout

**Lemme 3.7.** *Soit  $(a, b) \in \mathbb{Z} \times \mathbb{Z}$*

$a \times b = d \implies \exists (u, v) \in \mathbb{Z} \times \mathbb{Z}$  tel que  $au + bv = 1$ .

**Théorème 3.8 (de Bézout).**  $a \wedge b = 1 \iff \exists (u, v)$  tels que  $au + bv = 1$ .

*Démonstration.*  $\Leftarrow$  Soit  $c \in \mathbb{Z}$  tel que  $c|a$  et  $c|b$ . Donc  $c|au$  et  $c|bv$ , donc  $c|au + bv \implies c|1 \implies c = \pm 1$ . Donc  $a \wedge b = 1$ .  $\square$

**Théorème 3.9 (de Gauss).** *Soit  $a, b, c \in \mathbb{Z}$  tels que  $a|bc$  et  $a \wedge b = 1$ . Alors  $a|c$ .*

## 4 Eq. diophantienne $ax + by = c$

### 4.1 Existence de solutions

**Théorème 4.1.**  $ax + by = c$  admet une solution si et seulement si  $(a \wedge b)|c$

Dans la suite, on note  $d = a \wedge b$  et  $c = \gamma d$ .

*Démonstration.*  $\Leftarrow$   $d = a \wedge b \implies \exists u$  et  $v$  tel que  $au + bv = d$  donc  $\gamma u$  et  $\gamma v$  sont solutions.

$\Rightarrow$  Supposons qu'il existe une solution, càd  $\exists x$  et  $y$  tels que  $ax + by = c$ .  $c \in a\mathbb{Z} + b\mathbb{Z}$  donc  $c \in d\mathbb{Z} \implies d|c$ .  $\square$

### 4.2 Recherche de solutions

#### 4.2.1 Solution particulière

**Algorithme d'Euclide :** On effectue la division euclidienne de  $a$  par  $b$  :  $a = bq_1 + r_1$   $0 \leq r_1 < |b|$

Les diviseurs communs à  $a$  et à  $b$  sont ceux communs à  $b$  et à  $r_1$  donc  $a \wedge b = b \wedge r_1$ .

Si  $r_1 = 0$ ,  $a \wedge b = b$  et  $x = 0$  et  $y = \gamma$  sont solutions.

Si  $r_1 \neq 0$ , on effectue la division euclidienne de  $b$  par  $r_1$  :  $b = q_2 r_1 + r_2$   $0 \leq r_2 < r_1$ . En répétant, on obtient une suite finie strictement décroissante d'élément de  $\mathbb{N}$  telle que  $r_n = 0$ . On a donc  $a \wedge b = b \wedge r_1 = \dots = r_{n-1} \wedge r_n = r_{n-1}$ . Cet algorithme permet de trouver le pgcd. Ensuite, dans chaque division euclidienne, on isole  $r_i$  en fonction de  $r_{i-1}$  et  $r_{i-2}$ , ce qui permet d'écrire  $d$  en fonction de  $a$  et  $b$ .

#### 4.2.2 Solution générale

**Théorème 4.2.** *Soit l'équation  $ax + by = c$  (1). Si  $(u_0, v_0)$  est une solution particulière de  $ax + by = d$ , alors les solutions de (1) sont :*

$$\begin{cases} x = \frac{c}{d}u_0 - \frac{b}{d}k \\ y = \frac{c}{d}v_0 - \frac{a}{d}k \end{cases} \quad k \in \mathbb{Z}$$

*Démonstration.* On sait que  $\gamma u_0$  et  $\gamma v_0$  sont solutions, donc  $a\gamma u_0 + b\gamma v_0 = ax_0 + by_0 = c$ . Si  $(x, y)$  est une solution de (1),  $ax + by = c$  et  $ax_0 + by_0 = c$

donc  $a(x - x_0) = -b(y - y_0) \implies \frac{a}{d}(x - x_0) = -\frac{b}{d}(y - y_0)$  (2)

Or  $\frac{a}{d} \wedge \frac{b}{d} = 1$  et  $\frac{a}{d} | -\frac{b}{d}(y - y_0) \implies \frac{a}{d} | y - y_0 \implies \exists k$  tel que  $k \frac{a}{d} = y - y_0 \implies y = \frac{a}{d}k + y_0$ .

En remplaçant dans (2) :  $x = -\frac{b}{d}k + x_0$ . D'où le résultat.  $\square$