$a, b \in \mathbb{Z}$ et $n \in \mathbb{N}^*$.

1) $a \equiv b\,[n] \iff (\exists k \in \mathbb{Z},\ a = b + nk)$

$\iff n \mid (a-b)$

2) **Propriétés**

- $\forall a,\ a \equiv a\,[n]$
- $a \equiv b\,[n] \implies b \equiv a\,[n]$
- $\left.\begin{array}{l} a \equiv b\,[n] \\ b \equiv c\,[n] \end{array}\right\} \implies a \equiv c\,[n]$

c/c : $\equiv$ relat d'équiv sur $\mathbb{Z}$

Scanned with CamScanner

Soit R une relation d'équival sur E.

Soit $x \in E$.

$\rightarrow \bar{x}$: la classe d'équiva de x.

$\rightarrow \bar{x} = \{ y \in E \,/\, xRy \}$

$\rightarrow \bar{x} \subset E$ et $x \in E$

Prop

* $y \in \bar{x} \overset{\text{déf}}{\Longleftrightarrow} xRy \Leftrightarrow yRx$

$\Leftrightarrow \bar{x} = \bar{y} \Leftrightarrow y \in \bar{x}$

* $\forall x \in E,\ x \in \bar{x}$

* ⚠ $\bar{x} \neq \bar{y} \Longrightarrow \bar{x} \cap \bar{y} = \emptyset$

(à montrer)

L'ensemble $\mathbb{Z}/n\mathbb{Z}$

Prop : La congruence $\equiv$ est une relation d'équivalence s

NB :

— $\overline{a}$, la classe d'équivalence de a, est donnée par :

$x \in$)

$$\overline{a} = \{a + kn / k \in \mathbb{Z}\}$$

$x \in \overline{a} \iff x \equiv a[n] \iff (\exists k \in \mathbb{Z}, x = a + nk)$

— $\overline{a} = \overline{b} \Leftrightarrow a \equiv b[n]$

— $\overline{a} = \overline{0} \Leftrightarrow n/a$, par exemple :

$\forall k \in \mathbb{Z}, \overline{kn} = \overline{0}$; Dans $\mathbb{Z}/3\mathbb{Z}$, on a $\overline{3} = \overline{0}$ et $\overline{(-6)} = \overline{0}$

$n \in \mathbb{N}^*$.

Déf

$$\mathbb{Z}/n\mathbb{Z} = \{ \bar{a} \ / \ a \in \mathbb{Z} \}$$

Prop

$$\mathbb{Z}/n\mathbb{Z} = \{ \bar{0}, \bar{1}, \ldots, \overline{(n-1)} \}$$

càd

$$\mathbb{Z}/n\mathbb{Z} \overset{?}{=} \{ \bar{a} \ / \ 0 \leq a \leq n-1 \}$$

à savoir montrer

$A \subset B \Leftrightarrow (\forall x \in A, x \in B)$

Démo Par double inclusion

1) "$\supset$" évidente.

2) "$\subset$" M.q $\mathbb{Z}/n\mathbb{Z} \subset \{ \bar{a} \ / \ 0 \leq a \leq n-1 \}$

... (à finir) ! !

Scanned with CamScanner

$$\mathbb{Z}/6\mathbb{Z} = \{\overline{0}, \dots, \overline{5}\}$$

$$\overline{17} = \overline{?} \quad ; \quad \overline{7} = \overline{?} \quad ; \quad \overline{-2} = \overline{?}$$

$\mathbb{Z}/6\mathbb{Z} = \{\overline{0}, \dots, \overline{5}\}$

$\overline{17} = \overline{}$; $\overline{7} = \overline{1}$; $\overline{-2} = \overline{}$

$\overline{17} = \overline{\cancel{12}} + \overline{5} = \overline{5}$

$\overline{-2} = \overline{\cancel{-6}} + \overline{4} =$

...mme et le produit :

car $\overline{7} = \overline{\cancel{6}} + \overline{1} = \overline{1}$

$\overline{a} \times \overline{b}$

...ons les deux tableaux sui-

Prop : $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe abelien de neutre $\overline{0}$, et de cardinal n.

$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \dots, \overline{n-1}\}$. M.q ces sont 2 à 2 $\neq$.

à montrer

Sous-groupes

Soit $A \in M_n(\mathbb{R})$.

→ $\boxed{A \text{ est dite matrice } \underline{\text{orthogonale}} \text{ si et ssi : } \quad {}^tA \cdot A = I_n}$

→ $O(n)$ noté $O_n(\mathbb{R})$ est l'ens des matrices <u>orthogonales</u> :

→ $A \in O(n) \overset{déf}{\iff}$

<u>Exo</u> : M. que $O(n)$ est un <u>sous-groupe</u> de $(GL_n(\mathbb{R}), \times)$ (à travailler ⚠)

S!

<u>Vocab</u> : $(O(n), \times)$ est un groupe dit <u>groupe orthogonal</u> d'ordre n.