III . Relations d'équivalence

① Déf et généralités

* déf : si $\mathcal{R}$ est une rel. binaire sur E, c'est une relation d'équivalence

si elle est
- → symétrique
- → réflexive
- → transitive

ex : sur $\mathbb{R}$ = $x \mathcal{R} y$ si $\lfloor x \rfloor = \lfloor y \rfloor$ | $\leqslant$ sur $\mathbb{R}$ ↓ rel. d'ordre.

sur $\mathbb{Z}$ $\equiv [n]$ (***)

sur les chaînes de caractères $m_1 \mathcal{R} m_2$ si $\text{long}(m_1) = \text{long}(m_2)$

si m_1, m_2 commencent par la même lettre

* déf : si $\mathcal{R}$ est une relation d'équivalence

on appelle classe d'équivalence de x $(x \in E)$ l'ensemble

$$\dot{x} = \{ y \in E \ ; \ x \mathcal{R} y \}$$

$y \mathcal{R} x$

$\dot{y}$

ex : sur $\mathbb{R}$ $x \mathcal{R} y$ si $\lfloor x \rfloor = \lfloor y \rfloor$

$$\dot{1{,}5} = \{ y \in \mathbb{R} \ ; \ 1{,}5 \ \mathcal{R} \ y \} = [1, 2[\ = \dot{1} = \dot{1{,}1} = \dot{1{,}25} \ \ldots$$

pas unique

$[1,2[\ \ni 1{,}1$

$\Updownarrow$

$1{,}1 \ \mathcal{R} \ 1{,}5$

Prop Les prop. suivantes sont équivalentes :

i) $y \in \dot{x}$

ii) $x \mathcal{R} y$ ---- (sym) $y \mathcal{R} x$ ⇢ iii)

iii) $x \in \dot{y}$

iv) $\dot{x} = \dot{y}$

i) ⇔ ii) ⇔ iii)

$x \in \dot{y} \iff y \in \dot{x}$

Prop $x \in \dot{x}$

dém : iii) $\Longrightarrow$ iv)

On suppose $\boxed{x \in \dot{y}}$ $\qquad$ $\dot{x} = \dot{y}$?

ég. ens $\rightsquigarrow$ double $\subseteq$

$\dot{x} \subseteq \dot{y}$?

Soit $\boxed{a \in \dot{x}}$ $\qquad$ $a \in \dot{y}$? $\Longleftrightarrow$ $a R y$?

$\Downarrow$

$a R x$

or $x \in \dot{y}$

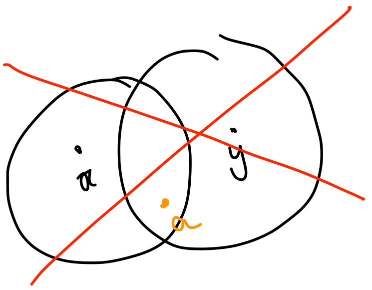
$\Longrightarrow x R y$

transitivité

$a R y$ ✓

$\dot{y} \subseteq \dot{x}$?

$\vdots$ faire la preuve ...



impossible

$\exists a \in \dot{x} \cap \dot{y}$

$\dot{x} \cap \dot{y} \neq \emptyset$

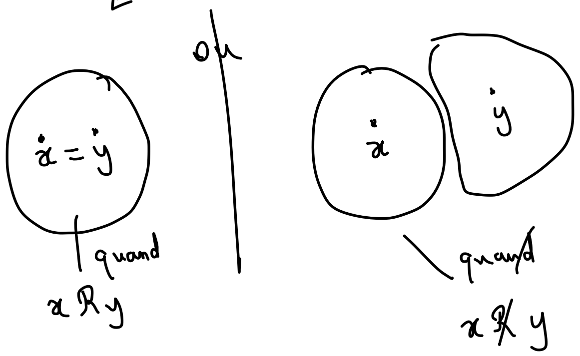
$\Downarrow$

$x R y \Longleftrightarrow \dot{x} = \dot{y}$

$\Longrightarrow a R x$ car $a \in \dot{x}$

$\Longrightarrow a R y$ car $a \in \dot{y}$

$\xRightarrow{\text{transitivité + symétrie}}$ $x R y \Longrightarrow \dot{x} = \dot{y}$

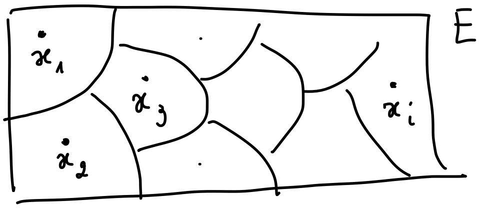


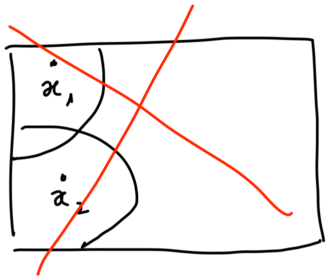
Prop

Si R est une relation d'équiv. sur E, les classes d'équivalence forment une partition de E ie :

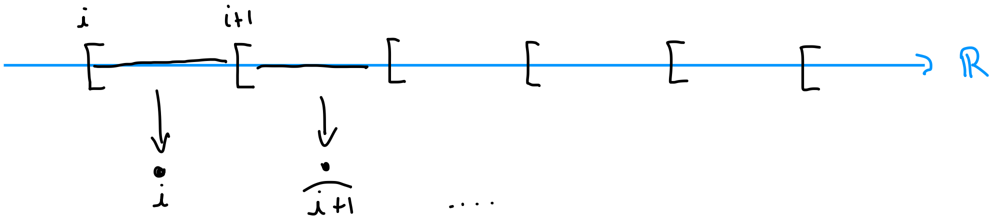
si $\dot{x}_i$ $\quad i \in I$ est une énumération des classes (comptées 1 seule fois)

partition $\Longleftrightarrow$
i) $E = \bigcup_{i \in I} \dot{x}_i$
ii) $\dot{x}_i \cap \dot{x}_j = \emptyset$ si $i \neq j$





ex: sur $\mathbb{R}$ $\quad x \mathcal{R} y$ si $\lfloor x \rfloor = \lfloor y \rfloor$



$\dot{1{,}5} = [1, 2[$
$\not\parallel$
$\dot{2{,}5}$
$\wr$
$\dot{2{,}5} = [2, 3[$
⋮

$\mathbb{R} = \bigcup$ classes $= \bigcup_{i \in \mathbb{Z}} [i, i+1[$

$[i, i+1[\cap [j, j+1[= \emptyset \quad i \neq j$

pb : ~~nommer~~ chaque classe de manière unique

$\Downarrow$

choisir 1 représentant par classe

$\dot{1} = [1, 2[= \dot{1{,}5}$
$\quad \shortparallel$
$\quad \dot{1{,}1} \quad ....$

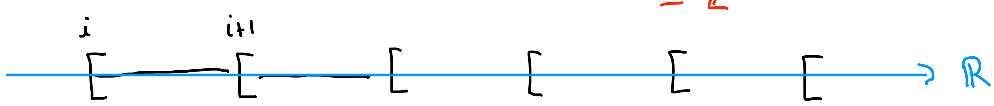
$\lfloor -\frac{1}{2} \rfloor = -1$

$\underbrace{\lfloor x \rfloor}_{\text{unique.}} \leq x < \lfloor x \rfloor + 1$

* **déf** : on appelle <u>ensemble quotient</u> de E par R (noté $E/_{\mathcal{R}}$)
l'ensemble des classes d'équivalence

ex : $\mathbb{R}/_{\mathcal{R}} = \{ \dot{i} = [i, i+1[\ ; i \in \mathbb{Z} \}$ $<$ ∞ discret $\simeq \mathbb{Z}$

$\mathbb{R} <$ ∞ continu



② <u>Cas de $\mathbb{Z}$ pour la congruence</u>

sur $\mathbb{Z}$ $\qquad \equiv [n]$ congruence modulo n $\rightsquigarrow$ rel. d'équivalence ex : $m = 5$ $\qquad R_5$ — $\equiv [5]$

$\dot{1} = \{ x \in \mathbb{Z} \text{ tq } \underbrace{x \, R_5 \, 1}_{\Leftrightarrow} \} = \{ 1, 6, 11, 16 \ldots, -4, -9, -14 \ldots \}$

$\overset{+5}{\frown}$: $1, 6, 11, 16 \ldots \longrightarrow 1 + 5k \quad k \geq 0$

$\overset{-5}{\frown}$: $-4, -9, -14 \ldots \longrightarrow 1 + 5k \quad k < 0$

$x = 1 + 5.k$, $k \in \mathbb{Z}$

$\{\ldots\} = \dot{6} = \dot{11} = \dot{-4} \ldots\ldots$

$\dot{2} \notin \dot{1}$

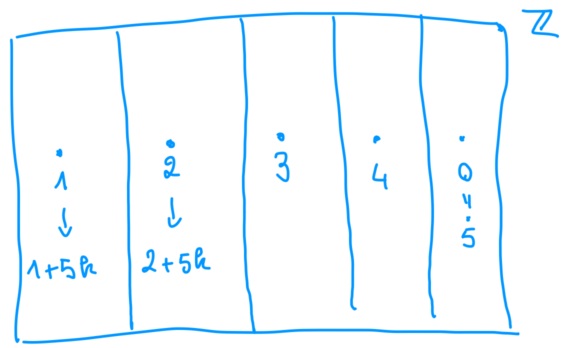
$\Downarrow$

$\dot{2} \cap \dot{1} = \emptyset$

$\dot{2} = \{ x \in \mathbb{Z} \, ; \, x \equiv 2 \, [5] \}$

$\downarrow$

$x = 2 + 5k$



5 classes distinctes

$\dot{7} = \dot{2}$

$\dot{127} = \dot{2}$

$\underline{m = 5q + r} \quad 0 \leq r < 5 \qquad$ div. eucl. par 5

$\downarrow$

$\dot{m} = \dot{r}$

$\uparrow$ plus petit représentant de la classe ...

on a autant de classes que de restes possibles $\sim \underbrace{\dot{0} \ldots \dot{m-1}}_{\dot{r}}$ avec $0 \leq r < m$

ensemble des 5 classes d'équiv.

$\mathbb{Z}/R_5 = \{ \dot{0}, \dot{1}, \dot{2}, \dot{3}, \dot{4} \} = \{ \dot{-2}, \dot{-1}, \dot{0}, \dot{1}, \dot{2} \}$

$\dot{-2} = \dot{3}$, $\dot{-1} = \dot{4}$

ensemble quotient

énumération la + simple et fréquente

Prop. si R_n est la congruence modulo n

i) $\mathbb{Z}$ comporte n classes pour R_n

ii) on les énumère comme : $\dot{0}, \dots, \dot{\overline{n-1}}$

iii) donc $\underbrace{\mathbb{Z}/R_n}_{\text{notée } \mathbb{Z}/n\mathbb{Z}} = \{\dot{0} \dots \dot{\overline{n-1}}\}$ ← ensemble fini à n élts

$\mathbb{Z}$ — ∞

ex: $\equiv [9]$ $\quad \dot{256}$?

$\dot{256} = \dot{4}$

$$\begin{array}{r|l} 256 & 9 \\ \hline 18 & 28 \\ 76 & \\ 72 & \\ \hline 4 & \end{array}$$

$\mathbb{Z}/n\mathbb{Z}$ fini — n éléments

Th. info
- → ens — alphabet fini
- → arithmétique $+, \times, /, \dots$ → complexité ....

$$\begin{array}{ccccc} \mathbb{Z} & x+y & & y & + \\ \downarrow & \downarrow & \searrow & \downarrow & \downarrow \\ \mathbb{Z}/n\mathbb{Z} & \dot{x} & \dot{\overline{x+y}} & \dot{y} & \oplus \end{array}$$

$\dot{\overline{x+y}} \overset{\text{déf}}{=} \dot{x} \oplus \dot{y}$

↓

opération quotient → facile à définir
→ pas toujours bien définie ...

* **déf:** opération quotient

sur $\mathbb{Z}$ → opération $*$ ($+$, $\times$, $-$, ...)

sur $\mathbb{Z}/n\mathbb{Z}$ → opération quotient $\circledast$ définie par

$$\underbrace{\dot{x} \circledast \dot{y}}_{\text{pas toujours bien définie}} = \dot{\overline{x * y}} \qquad (x*y \in \mathbb{Z})$$

($\oplus$, $\ominus$, $\otimes$, ...)

ex: $\mathbb{Z}/5\mathbb{Z}$ $\longrightarrow$ $\oplus$? bien défini

$\dot{x}$ $\dot{y}$

$$\dot{x} \oplus \dot{y} \overset{\text{déf}}{=} \overset{\bullet}{\overline{x+y}}$$

ex $\rightsquigarrow$ $\dot{1} \oplus \dot{4} = \overset{\bullet}{\overline{\underset{\in \mathbb{Z}}{1+4}}} = \dot{5} = \dot{0}$

$4+5k'$

$1+5k$

$\dot{1} = \dot{6} = \overset{\bullet}{-4}$

$\dot{4} = \overset{\bullet}{-1} = \dot{9} \vdots$

pour d'autres représentants $\rightsquigarrow$ même résultat ?

$$\forall k, k' \quad \overset{\bullet}{\overline{(1+5k)+(4+5k')}} \overset{!}{=} \dot{0} \qquad = \overset{\bullet}{\overline{5+5(k+k')}} = \dot{0}$$

__Prop.__ dans $\mathbb{Z}/n\mathbb{Z}$ $\oplus$, $\otimes$ sont bien définies