Chapitre 5

Relations d'équivalence, congruence

1°) Relations d'équivalences

Définition : Soit E un ensemble, une relation sur E est une application

$$R : E \times E \longrightarrow \{\text{Vrai}, \text{Faux}\}$$
$$(x, y) \longmapsto R(x, y).$$

Nous écrivons parfois $x R y$ au lieu de $R(x, y)$. Il s'agit donc d'un booléen.

Cette définition est très générale et s'applique à de nombreuses situations.

Exemples :

1°) Soit E l'ensemble des villes du monde. Si x et y sont deux villes, nous dirons qu'elles sont en relation si elles sont à moins de 100 km

On a donc :

$$x \mathcal{R} y \iff \text{distance}(x,y) \leq 100 \text{ km}.$$

2°) Soit $E = \mathbb{C}$ l'ensemble des nombres complexes.
Nous dirons que x et y sont en relation s'ils ont même module :

$$x \mathcal{R} y \iff |x| = |y|.$$

3°) Soit E l'ensemble des êtres humains.
Nous dirons que x et y sont en relation si x est un descendant de y.

Remarque : définition alternative.

Une relation sur un ensemble E est souvent définie comme "une partie de $E \times E$".
Les deux définition sont équivalente :
À toute partie A de $E \times E$ on associe la relation

$$\begin{aligned} \mathcal{R}_A : \quad E \times E &\longrightarrow \{\text{Vrai}, \text{Faux}\} \\ (x,y) &\longrightarrow \text{Vrai ssi } (x,y) \in A \end{aligned}$$

et à toute relation R on associe la partie $A_R = \{ (x,y) \in E \times E,\ x R y \text{ est vrai} \}$.

Certains types de relations sont particulièrement important. On a déjà parlé des "relation d'ordre". Rappelons ici la définition de "relation d'équivalence":

Définition: Soit E un ensemble. Une relation d'équivalence sur E est une relation $R : E \times E \longrightarrow \{\text{Vrai}, \text{Faux}\}$ telle que:

i) R est réflexive: $\forall x \in E,\ x R x$

ii) R est symétrique:

$$\forall (x,y) \in E \times E,\quad x R y \Longleftrightarrow y R x$$

iii) R est transitive:

$$\forall (x,y,z) \in E \times E,$$
$$((x R y) \text{ et } (y R x)) \Longrightarrow x R z$$

Exemples :

Reprenons nos trois exemples précédent.

i) Les villes du monde.

R est reflexive et symétrique, mais elle n'est pas transitive.

On a par exemple pour

$x =$ Montpellier

$y =$ Avignon

$z =$ Aix-en-Provence

$(x R y)$ et $(y R z)$, mais pas $(x R z)$.

ii) Modules de nombres complexes.

C'est bien une relation d'équivalence.

iii) Être humains et descendance.

Ce n'est pas une relation d'équivalence car elle n'est pas symétrique ! En revanche, c'est une relation d'ordre.

Définitions : Soit E un ensemble muni d'une relation d'équivalence $\mathcal{R}$.

i) Pour tout $x \in E$, on appelle **classe d'équivalence de x** l'ensemble des éléments de E en relation avec x. On note $\bar{x}$ cet ensemble (ou parfois $\bar{x}^{\mathcal{R}}$ si on souhaite préciser la relation $\mathcal{R}$).

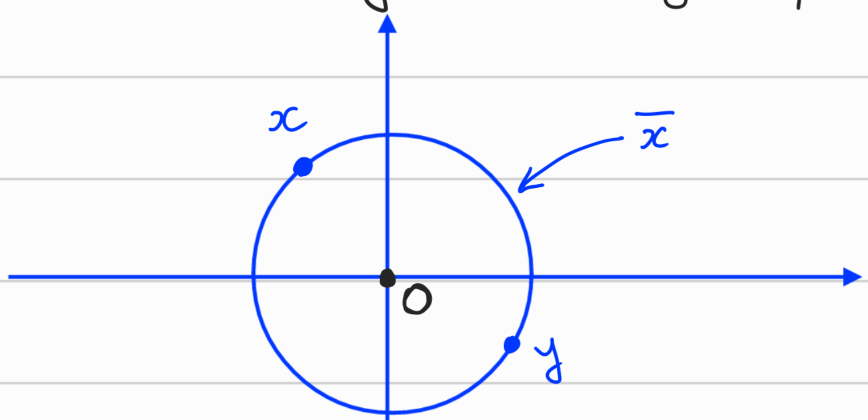
$$\bar{x} = \{ y \in E,\ x \mathcal{R} y \}.$$

ii) Un partie A de E est appelée **classe d'équivalence** de $\mathcal{R}$, s'il existe $x \in E$ tel que $A = \bar{x}$.

iii) Soit $A \subset E$ une classe d'équivalence de $\mathcal{R}$, tout élément y de A est appelé **représentant** de A.

Exemple : $E = \mathbb{C}$, $R =$ "égalité des modules".

Les classes d'équivalences sont les cercles centrés à l'origine, de rayon positif ou nul.



y est un représentant de $\overline{x}$.

Lemme : Soit E un ensemble muni d'une relation d'équivalence R.
Soit $A \subset E$ une classe d'équivalence de R et $y \in A$ un représentant de A.

Alors $A = \overline{y}$.

Preuve :

Par définition d'une classe d'équivalence, il existe $x \in E$ tel que :

$$A = \overline{x} = \{ z \in E \,,\; x R z \}.$$

Posons par ailleurs, $B = \overline{y} = \{z \in E,\ y R z\}$.

<u>$A \subset B$</u> : Soit $z \in A$, on sait que $x R z$.

Puisque $y \in A = \overline{x}$, on a aussi : $x R y$

Par symétrie, $x R y \Rightarrow y R x$.

On a donc :

$(y R x)$ et $(x R z)$ ce qui implique

$y R z$ par transitivité, donc

$z \in \overline{y} = B$.

<u>$B \subset A$</u> : Là encore on procède par transitivité ;

Soit $z \in B$, on a $y R z$.

Puisque $y \in \overline{x}$, on a $x R y$, donc

$(x R y)$ et $(y R z)$ implique $(x R z)$

par transitivité, et $z \in A$.

$\square$

<u>Remarque</u> : Le lemme précédent montre pourquoi la symétrie et la transitivité sont nécessaires.

La reflexivité permet par ailleurs d'affirmer que si $A = \overline{x}$ est une classe d'équivalence alors $x \in A$. En effet on a $x \mathcal{R} x$ par réflexivité.

Une relation d'équivalence permet de regrouper les éléments d'un ensemble E en sous-ensemble d'éléments équivalents.

Définition. Soit E un ensemble non vide, $\mathcal{P}(E)$ l'ensemble des parties de E, et $X \subset \mathcal{P}(E)$.

On dit que X est une partition de E si :

i) $\forall A \in X, \quad A \neq \emptyset$

ii) $E = \bigcup_{A \in X} A$

iii) $\forall (A, B) \in X^2, \quad A \cap B \neq \emptyset \Longrightarrow A = B$.

Exemple : $E = \mathbb{C}$

$X = \{$ ensemble des cercles centrés à l'origine, de rayon $\geq 0 \}$.

alors X est une partition de $\mathbb{C}$.

Proposition : Soit E un ensemble non vide muni d'une relation d'équivalence R. L'ensemble des classes d'équivalences de R forme une partition de E.

Preuve : Soit X l'ensemble des classes d'équivalences de E, vérifions les points i) à iii) de la définition d'une partition.

i) Soit $A \in X$.

Par définition d'une classe d'équivalence il existe $x \in A$ tel que $\bar{x} = A$, et $x \in A$ par reflexivité, donc $A \neq \emptyset$.

ii) Soit $A, B \in X$.

Soit $x \in A \cap B$. L'élément x est un représentant de A et de B. D'après le lemme ci-dessus, $A = \bar{x}$ et $B = \bar{x}$, donc $A = B$.

iii) On a la suite d'inclusions :

$$E = \bigcup_{x \in E} \{x\} \subset \bigcup_{x \in E} \bar{x} = \bigcup_{A \in X} A.$$

Donc $E = \bigcup_{A \in X} A$. $\square$

Définition : Soit E un ensemble non vide muni d'une relation d'équivalence R. L'ensemble des classes d'équivalence de R est appelé ensemble quotient de E par R. On le note parfois E/R.

Exemple : Si $E = \mathbb{C}$ et $R =$ "égalité des modules", l'ensemble quotient $\mathbb{C}/R$ est l'ensemble des cercles unités de rayons positifs ou nul. Il est en bijection avec $\mathbb{R}^+$:

$$\begin{array}{ccc} \mathbb{R}^+ & \longrightarrow & \mathbb{C}/R \\ r & \longmapsto & \text{cercle de centre } 0 \text{ et rayon } r. \end{array}$$

2°) Relations de congruence

Définition : Soit $n \in \mathbb{Z}$, soit $(a, b) \in \mathbb{Z}^2$, on dit que a et b sont congrus modulo n si n divise $(a-b)$.
On note $a \equiv b\ [n]$ cette relation.

Proposition : La congruence modulo n est une relation d'équivalence sur $\mathbb{Z}$.

Preuve :

Réflexivité : Soit $a \in \mathbb{Z}$, n divise $(a-a) = 0$.

Symétrie : Soit $(a, b) \in \mathbb{Z}^2$, n divise $(a-b)$ ssi n divise $(b-a)$.

Réflexivité, Soient $(a, b, c) \in \mathbb{Z}^3$.
Si $n \mid (a-b)$ et $n \mid (b-c)$, alors $n \mid ((a-b)+(b-c)) = (a-c)$ donc $a \equiv c\ [n]$.

$\square$

Proposition : Soit $(a,b) \in \mathbb{Z}^2$ et $n \in \mathbb{N}^*$, on a :
a est congru à b modulo n si et seulement les restes des divisions euclidiennes de a et b par n sont les mêmes.

Preuve :

Ecrivons les divisions euclidiennes de a et b par n :

$$a = qn + r \qquad \text{où } 0 \leq r, r' < n.$$
$$b = q'n + r'$$

On a :

$$a \equiv b\ [n] \iff n \text{ divise } (a-b)$$
$$\iff n \text{ divise } (q-q')n + (r-r')$$
$$\iff n \text{ divise } (r-r')$$

or $0 \leq |r-r'| < n$

donc ceci équivaut à $r - r' = 0$. $\square$

Notons $\equiv_n$ la relation de congruence modulo n.

<u>Notation</u> : L'ensemble quotient de $\mathbb{Z}$ par la relation de congruence modulo n est noté : $\mathbb{Z}/n\mathbb{Z}$.

Rappelons aussi que, si $a \in \mathbb{Z}$, la classe d'équivalence de a pour $\equiv_n$ est notée $\bar{a}$. Si l'entier n doit être précisé, on la notera $\bar{a}^n$.

On a donc :

$$\bar{a}^n = \bar{a} = \{ b \in \mathbb{Z} \,/\, n \text{ divise } b-a \}$$
$$= \{ a + kn \,;\, k \in \mathbb{Z} \}.$$

<u>Proposition</u> : Soit $n \in \mathbb{N}^*$, l'ensemble $\mathbb{Z}/n\mathbb{Z}$ est de cardinal n et :

$$\mathbb{Z}/n\mathbb{Z} = \{ \bar{0}, \bar{1}, \dots, \overline{n-1} \}.$$

Preuve : Montrons d'abord que si $0 \leq a < b < n$, alors

$$\bar{a} \neq \bar{b}.$$

en effet, si $\bar{a} = \bar{b}$ alors a et b sont congrus modulo n, donc

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

mais, puisque $0 \leq a, b < n$, $|a-b| < n$.

donc $a - b = 0$ et $a = b$, ce qui est exclu.

Ainsi les classe $\bar{0}, \bar{1}, \dots, \overline{n-1}$ sont toutes distinctes, et l'ensemble

$A = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$ est de cardinal n.

Puisque les éléments de A sont des classes d'équivalence, on a : $A \subset \mathbb{Z}/n\mathbb{Z}$.

Il ne reste qu'à montrer que $\mathbb{Z}/n\mathbb{Z} \subset A$:

Soit $x \in \mathbb{Z}/n\mathbb{Z}$; x est une classe d'équivalence et on peut en choisir un représentant $a \in \mathbb{Z}$.

On a donc : $x = \bar{a}$.

Effectuons la division euclidienne de

a par n : $a = qn + r$.

alors $a - r$ est divisible par n donc $a \equiv r\ [n]$. Par suite $\bar{a} = \bar{r}$ donc $x = \bar{r}$ avec $0 \leq r < n$, donc $x \in \{\bar{0}, .., \overline{n-1}\}$. $\square$

Exemples :

Si $n = 0$: Soit $(a, b) \in \mathbb{Z}^2$.

$$a \equiv b\ [0] \iff 0 \text{ divise } (a-b)$$
$$\iff (a-b) = 0 \iff a = b.$$

Ainsi, $\mathbb{Z}/_{0\mathbb{Z}} = \mathbb{Z}$.

Si $n = 1$: Soit $(a, b) \in \mathbb{Z}^2$,

$a \equiv b\ [1] \iff 1$ divise $(a-b)$ ce qui est toujours vrai.

Donc tous les entiers sont équivalents deux à deux et il n'y a qu'une seule classe d'équivalence qui est $\mathbb{Z}$ entier :

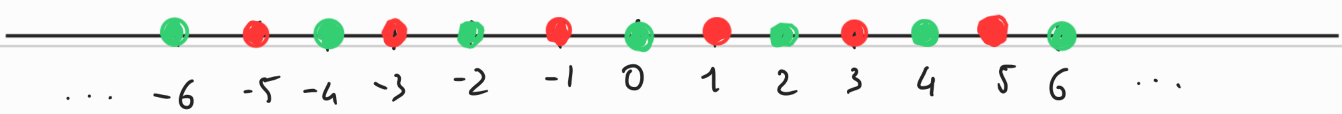
$$\mathbb{Z}/_{1\mathbb{Z}} = \{\bar{0}\} = \{\mathbb{Z}\}.$$

Si $n = 2$: $a \equiv b\ [2] \iff 2 \mid (a-b)$

$\iff$ a et b ont même parité.

Il y a donc deux classes d'équivalences :

- $\bar{0} = \{2k, k \in \mathbb{Z}\}$: "les entiers pairs"
- $\bar{1} = \{1 + 2k, k \in \mathbb{Z}\}$: "les entiers impairs".



Si $n = 3$: Les trois classes sont :

- $\bar{0} = \{3k, k \in \mathbb{Z}\}$: les multiples de 3.
- $\bar{1} = \{3k+1, k \in \mathbb{Z}\}$
- $\bar{2} = \{3k+2, k \in \mathbb{Z}\}$.