

# Relations binaires sur un ensemble

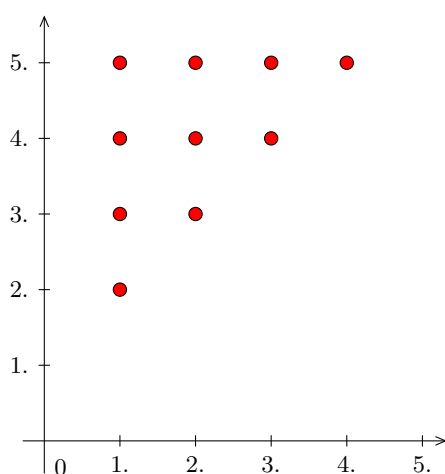
On se donne dans tout ce chapitre un ensemble non vide  $E$ .

## I Relations binaires sur un ensemble

### Définition.

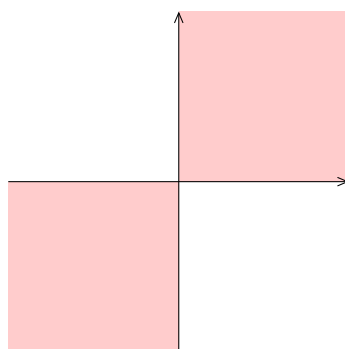
- On appelle relation binaire sur  $E$  une partie  $G$  de  $E \times E$ .
- On dit que  $x$  est en relation avec  $y$  si  $(x, y) \in G$ . On note alors  $xRy$  et on parle de la relation  $R$ .

**Remarque :** En d'autres termes, une relation binaire est définie comme l'ensemble des couples qui la vérifient. Par exemple, la relation « inférieur strict » sur  $\llbracket 1 ; 5 \rrbracket$  est l'ensemble  $\{(1, 2); (1, 3); (1, 4); (1, 5); (2, 3); \dots; (4, 5)\}$  représenté par les points ci-dessous :



De façon analogue, on aurait pu définir une fonction  $f : E \rightarrow F$  comme une partie  $G$  de  $E \times F$  (son graphe) vérifiant la propriété suivante :  $\forall x \in E, \exists! y \in F, (x, y) \in G$ . Lorsque  $(x, y) \in G$ , on noterait alors  $y = f(x)$  et on dirait que  $y$  est l'image de  $x$  par la fonction  $f$ . Nous ne l'avons pas fait car nous nous sommes contentés d'une définition intuitive de fonction.

De même, l'égalité est la relation associée à la première bissectrice dans le plan, et la relation « être de même signe » (sur  $\mathbb{R}^*$ ) est la partie du plan associée aux deux carrés (sans les axes, on se place sur  $\mathbb{R}^*$ ) ci-dessous :



**Remarque :** Bien sûr, on peut noter certaines relations différemment, tout dépend du type de relation (voir plus bas : on notera en général différemment les relations d'ordre et les relations d'équivalence). Cela dépend aussi de si on connaît déjà la relation ou non : noter  $xRy$  lorsque  $R$  est la relation « inférieur strict » ou lorsque  $R$  est la relation d'égalité relève un peu du vice, et on continuera à l'écrire  $x < y$  et  $x = y$ ...

**Remarque :** Attention, on peut avoir  $xRy$  sans avoir  $yRx$  ! L'ordre compte ! Nous verrons de nombreux exemples dans la suite, mais la relation « inférieur strict » nous donne déjà

un contre-exemple. Sinon, dans le cas général, il suffit de voir que les couples  $(x, y)$  et  $(y, x)$  sont distincts, et donc ils n'ont aucune raison d'appartenir tous les deux à  $G$ .

**Définition.** Une relation binaire  $R$  sur  $E$  est dite :

- réflexive si :  $\forall x \in E, xRx$ .
- symétrique si :  $\forall (x, y) \in E^2, xRy \Rightarrow yRx$ .
- antisymétrique si :  $\forall (x, y) \in E^2, (xRy \text{ et } yRx) \Rightarrow x = y$ .
- transitive si :  $\forall (x, y, z) \in E^3, (xRy \text{ et } yRz) \Rightarrow xRz$ .

Voir la suite du cours pour de nombreux exemples.

## II Relations d'ordre

### II.1 Définition

**Définition.** Une relation d'ordre est une relation binaire réflexive, antisymétrique et transitive. Si  $E$  est un ensemble muni d'une relation d'ordre, on dit que c'est un ensemble ordonné.

**Remarque :** Intuitivement, une relation d'ordre sert à définir rigoureusement le fait qu'un élément est « plus petit » (au sens large) qu'un autre. Les trois conditions de la définition sont alors naturelles :

- la réflexivité dit juste qu'un élément est « plus petit » que lui-même.
- l'antisymétrie dit juste que si un élément est « plus petit » qu'un autre, et si le deuxième est aussi « plus petit » que le premier, alors ils sont égaux.
- la transitivité dit juste que si un élément est « plus petit » qu'un deuxième, et si celui-ci est « plus petit » qu'un troisième, alors le premier est « plus petit » que le troisième.

Certaines relations d'ordre sont notées  $\preccurlyeq$  ou plus simplement  $\leq$ , à ne pas confondre avec le  $\leq$  réel (mais, quand ça arrivera, il n'y aura aucune ambiguïté).

### II.2 Exemples

La relation  $\leq$  est évidemment une relation d'ordre sur  $\mathbb{R}$ . En effet :

- Soit  $x \in \mathbb{R}$ . Alors  $x \leq x$  :  $\leq$  est réflexive.
- Soit  $(x, y) \in \mathbb{R}^2$  tel que  $x \leq y$  et  $y \leq x$ . Alors  $x = y$  :  $\leq$  est antisymétrique.
- Soit  $(x, y, z) \in \mathbb{R}^3$  tel que  $x \leq y$  et  $y \leq z$ . Alors  $x \leq z$  :  $\leq$  est transitive.

L'inclusion  $\subset$  est une relation d'ordre sur  $\mathcal{P}(E)$ . En effet :

- Soit  $X \in \mathcal{P}(E)$ . Alors  $X \subset X$  :  $\subset$  est réflexive.
- Soit  $(X, Y) \in \mathcal{P}(E)^2$  tel que  $X \subset Y$  et  $Y \subset X$ . Alors  $X = Y$  :  $\subset$  est antisymétrique.
- Soit  $(X, Y, Z) \in \mathcal{P}(E)^3$  tel que  $X \subset Y$  et  $Y \subset Z$ . Alors  $X \subset Z$  :  $\subset$  est transitive.

**Remarque :** Attention à l'idée intuitive de relation d'ordre comme moyen de dire qu'un élément est « plus petit » qu'un autre. Par exemple, si on prend  $E = \mathcal{P}([1; n])$  et si on définit la relation  $R$  par :  $XRY \iff \text{card}(X) \leq \text{card}(Y)$ , alors  $R$  n'est pas une relation d'ordre (car elle n'est pas antisymétrique : deux ensembles peuvent avoir le même cardinal sans être égaux) alors qu'intuitivement, un ensemble avec moins d'éléments peut être considéré comme plus petit qu'un ensemble avec plus d'éléments.

Voir un autre exemple dans le paragraphe III.2.


La divisibilité  $|$  est une relation d'ordre sur  $\mathbb{N}$ ,  $\mathbb{N}^*$ ,  $\mathbb{N} \setminus \{0; 1\}$  etc. En effet :

- Soit  $n \in \mathbb{N}$ . Alors  $n = 1 \times n$  donc  $n|n$  :  $|$  est réflexive.
- Soit  $(n_1, n_2) \in \mathbb{N}^2$  tel que  $n_1|n_2$  et  $n_2|n_1$ . Alors il existe  $(k_1, k_2) \in \mathbb{N}^2$  tel que  $n_1 \times k_1 = n_2$  et  $n_2 \times k_2 = n_1$ . Par conséquent,  $n_1 = n_1 \times k_1 k_2$ . Si  $n_1 = 0$ , alors  $n_2 = n_1 \times k_1 = 0$  donc  $n_1 = n_2$ . Si  $n_1 \neq 0$ , alors  $1 = k_1 k_2$  donc  $k_1 = k_2 = 1$  (ce sont des nombres positifs) si bien que  $n_1 = n_2$ . Dans tous les cas,  $n_1 = n_2$  :  $|$  est antisymétrique.

Ci-contre, on se place sur  $\mathbb{N}$ , mais c'est évidemment encore valable sur  $\mathbb{N}^*$ ,  $\mathbb{N} \setminus \{0; 1\}$  etc.

- Soit  $(n_1, n_2, n_3) \in \mathbb{N}^3$  tel que  $n_1|n_2$  et  $n_2|n_3$ . Alors il existe  $(k_1, k_2) \in \mathbb{N}^2$  tel que  $n_1 \times k_1 = n_2$  et  $n_2 \times k_2 = n_3$  si bien que  $n_1 \times (k_1 k_2) = n_3$ . Or,  $k_1 k_2 \in \mathbb{N}$  donc  $n_1|n_3$  :  $|$  est transitive.

### Remarques :

- Nous avons pris la définition de la divisibilité suivante :  $a|b \iff \exists k \in \mathbb{N}, a \times k = b$ . Cela nous permet de dire sans problème que  $0|0$ . De plus, sur  $\mathbb{N}^*$ , alors on a l'équivalence suivante :  $a|b \iff b/a \in \mathbb{N}$ .
-  La divisibilité n'est pas une relation d'ordre sur  $\mathbb{Z}$  ni même sur  $\mathbb{Z}^*$  car n'est pas antisymétrique ! En effet,  $2|-2$  et  $-2|2$  mais  $2 \neq -2$  !

cf. chapitre 6.

On définit la relation  $\leq$  sur  $\mathbb{R}^{\mathbb{R}}$  par :

$$f \leq g \iff \forall x \in \mathbb{R}, f(x) \leq g(x)$$

Alors c'est une relation d'ordre. En effet :

- Soit  $f \in \mathbb{R}^{\mathbb{R}}$ . Alors, pour tout  $x \in \mathbb{R}, f(x) \leq f(x)$  donc  $f \leq f$  :  $\leq$  est réflexive.
- Soit  $(f, g) \in (\mathbb{R}^{\mathbb{R}})^2$  tel que  $f \leq g$  et  $g \leq f$ . Alors, pour tout  $x \in \mathbb{R}, f(x) \leq g(x)$  et  $g(x) \leq f(x)$  donc  $f(x) = g(x)$ , c'est-à-dire que  $f = g$  :  $\leq$  est antisymétrique.
- Soit  $(f, g, h) \in (\mathbb{R}^{\mathbb{R}})^3$  tel que  $f \leq g$  et  $g \leq h$ . Alors, pour tout  $x \in \mathbb{R}, f(x) \leq g(x)$  et  $g(x) \leq h(x)$  donc  $f(x) \leq h(x)$ , c'est-à-dire que  $f \leq h$  :  $\leq$  est transitive.

Ci-contre, ne pas confondre le  $\leq$  sur  $\mathbb{R}^{\mathbb{R}}$  et le  $\leq$  réel.

Dans le même ordre d'idée, on peut montrer que la relation  $\preceq$  définie dans l'exercice 52 du chapitre 12 est aussi une relation d'ordre.

Terminons par deux exemples classiques d'ordre sur un ensemble produit.

Soient  $(E, \leq_E)$  et  $(F, \leq_F)$  deux ensembles ordonnés. On définit sur  $E \times F$  l'ordre produit  $\preceq$  par :

$$(x_1, y_1) \preceq (x_2, y_2) \iff x_1 \leq_E x_2 \quad \text{et} \quad y_1 \leq_F y_2$$

Montrons que  $\preceq$  est une relation d'ordre sur  $E \times F$ .

- Soit  $(x, y) \in E \times F$ . Les relations d'ordre  $\leq_E$  et  $\leq_F$  sont réflexives donc  $x \leq_E x$  et  $y \leq_F y$  donc  $(x, y) \preceq (x, y)$  :  $\preceq$  est réflexive.
- Soient  $(x_1, y_1)$  et  $(x_2, y_2) \in E \times F$  tels que  $(x_1, y_1) \preceq (x_2, y_2)$  et  $(x_2, y_2) \preceq (x_1, y_1)$ . Alors  $x_1 \leq_E x_2, y_1 \leq_F y_2, x_2 \leq_E x_1$  et  $y_2 \leq_F y_1$ . En particulier,  $x_1 \leq_E x_2$  et  $x_2 \leq_E x_1$  donc  $x_1 = x_2$  car  $\leq_E$  est antisymétrique. De même,  $y_1 = y_2$  donc  $(x_1, y_1) = (x_2, y_2)$  :  $\preceq$  est antisymétrique.
- Soient  $(x_1, y_1), (x_2, y_2)$  et  $(x_3, y_3) \in E \times F$  tels que  $(x_1, y_1) \preceq (x_2, y_2)$  et  $(x_2, y_2) \preceq (x_3, y_3)$ . Alors  $x_1 \leq_E x_2, y_1 \leq_F y_2, x_2 \leq_E x_3$  et  $y_2 \leq_F y_3$ . En particulier,  $x_1 \leq_E x_2$  et  $x_2 \leq_E x_3$  donc  $x_1 \leq_E x_3$  car  $\leq_E$  est transitive. De même,  $y_1 \leq_F y_3$  donc  $(x_1, y_1) \preceq (x_3, y_3)$  :  $\preceq$  est transitive.

En d'autres termes, pour l'ordre produit, un couple est inférieur à un autre lorsque la première coordonnée du premier couple est inférieure à la coordonnée du deuxième couple, et idem pour la deuxième coordonnée.

Soient  $(E, \leq_E)$  et  $(F, \leq_F)$  deux ensembles ordonnés. On définit sur  $E \times F$  l'ordre lexicographique  $<$  par :

$$(x_1, y_1) < (x_2, y_2) \iff x_1 <_E x_2 \quad \text{ou} \quad (x_1 = x_2 \text{ et } y_1 \leq_F y_2)$$

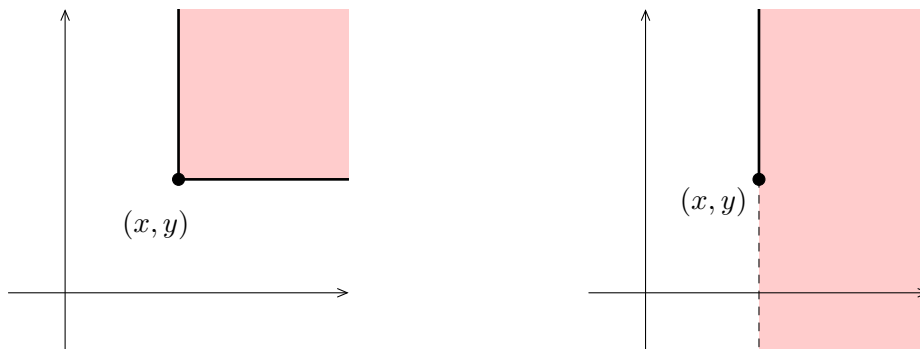
Remarquons que si  $(x_1, y_1) < (x_2, y_2)$ , alors  $x_1 \leq_E x_2$  : en effet, soit  $x_1 <_E x_2$ , et alors  $x_1 \leq_E x_2$ , soit  $x_1 = x_2$ , et alors  $x_1 \leq_E x_2$  car  $\leq_E$  est réflexive. Montrons que  $<$  est une relation d'ordre sur  $E \times F$ .

- Soit  $(x, y) \in E \times F$ . Alors  $x = x$  et  $y \leq_F y$  car  $\leq_F$  est réflexive donc  $(x, y) < (x, y)$  :  $<$  est réflexive.

De façon analogue au cas réel, on définit  $<_E$  par :  $x_1 <_E x_2 \iff x_1 \leq_E x_2$  et  $x_1 \neq x_2$ , et on dit alors que  $x_1$  est strictement inférieur à  $x_2$ . On dit que  $<_E$  est une relation d'ordre strict, et on peut évidemment généraliser à un ensemble ordonné quelconque.

- Soient  $(x_1, y_1)$  et  $(x_2, y_2) \in E \times F$  tels que  $(x_1, y_1) \preceq (x_2, y_2)$  et  $(x_2, y_2) \preceq (x_1, y_1)$ . Alors  $x_1 <_E x_2$  ou  $x_1 = x_2$  donc, dans tous les cas,  $x_1 \leq_E x_2$  et, par symétrie des rôles (qu'on ne confondra pas avec la symétrie d'une relation d'équivalence, voir plus bas),  $x_2 \leq_E x_1$ . La relation  $\leq_E$  étant antisymétrique,  $x_1 = x_2$ . Puisque  $(x_1, y_1) \preceq (x_2, y_2)$  et que  $x_1 = x_2$ , cela signifie que  $y_1 \leq_F y_2$ . Par symétrie des rôles,  $y_2 \leq_F y_1$  donc  $y_1 = y_2$  car  $\leq_F$  est antisymétrique donc  $(x_1, y_1) = (x_2, y_2)$  :  $\preceq$  est antisymétrique.
- Soient  $(x_1, y_1), (x_2, y_2)$  et  $(x_3, y_3) \in E \times F$  tels que  $(x_1, y_1) \preceq (x_2, y_2)$  et  $(x_2, y_2) \preceq (x_3, y_3)$ . Supposons (raisonnement analogue dans les autres cas) que  $x_1 = x_2$  et  $y_1 \leq_F y_2$  et que  $x_2 <_E x_3$ . Alors, en particulier,  $x_2 \leq_E x_3$  donc, par transitivité de  $\leq_E$ ,  $x_1 \leq_E x_3$ . Si  $x_1 = x_3$ , alors  $x_2 = x_1 = x_3$  ce qui est exclu. En d'autres termes,  $x_1 <_E x_3$  donc  $(x_1, y_1) \preceq (x_3, y_3)$  :  $\preceq$  est transitive.

L'ordre produit et l'ordre lexicographique permettent de munir l'ensemble produit  $E \times F$  d'un ordre lorsque  $E$  et  $F$  sont eux-mêmes ordonnés (on peut évidemment généraliser à un produit de plus de deux ensembles). Par exemple, cela permet de munir  $\mathbb{R}^2$  (ou, ce qui revient au même,  $\mathbb{C}$ ) d'un ordre. Ci-dessous, on a représenté les éléments de  $\mathbb{R}^2$  supérieurs ou égaux à  $(x, y)$  dans les deux cas : à gauche, l'ordre produit, à droite, l'ordre lexicographique.



Il y a trois autres cas :

- ★  $x_1 <_E x_2$  et  $x_2 <_E x_3$ .
- ★  $x_1 <_E x_2, x_2 = x_3$  et  $y_2 \leq_F y_3$ .
- ★  $x_1 = x_2, y_1 \leq_F y_2$  et  $x_2 = x_3, y_2 \leq_F y_3$ .

L'ordre lexicographique peut paraître artificiel, mais on l'a déjà vu ! En effet, il porte ce nom car c'est l'ordre dans lequel sont rangés les mots dans le dictionnaire !

Il n'y a pas d'ordre plus naturel qu'un autre (même si l'ordre lexicographique peut vérifier des conditions supplémentaires, voir paragraphe suivant), c'est pour cela qu'on a dit dans le chapitre 7 que  $\mathbb{C}$  n'est pas muni d'un ordre naturel.

### II.3 Activité : suites monotones dans un ensemble ordonné

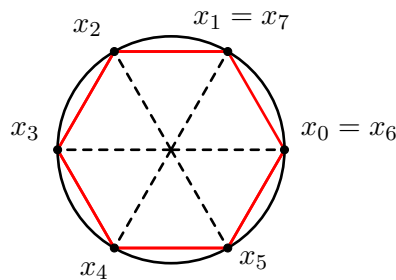
On se donne dans ce paragraphe un ensemble ordonné  $(E, \preceq)$ . On définit sur  $E$  une suite (strictement) monotone de la même façon que sur  $\mathbb{R}$  :

**Définition.**  $(u_n)_{n \in \mathbb{N}}$  est :

- croissante si, pour tout  $n \in \mathbb{N}$ ,  $u_n \preceq u_{n+1}$ ,
- décroissante si, pour tout  $n \in \mathbb{N}$ ,  $u_{n+1} \preceq u_n$ ,
- strictement croissante si, pour tout  $n \in \mathbb{N}$ ,  $u_n \preceq u_{n+1}$  et  $u_n \neq u_{n+1}$ ,
- strictement décroissante si, pour tout  $n \in \mathbb{N}$ ,  $u_{n+1} \preceq u_n$  et  $u_n \neq u_{n+1}$ ,
- monotone si elle est croissante ou décroissante, strictement monotone si elle est strictement croissante ou strictement décroissante.

L'idée générale d'une suite croissante est : les images sont dans le même ordre que les indices, et c'est le contraire pour une suite décroissante. Mais sur un ensemble ordonné, il faut travailler un peu : il n'est pas évident que, par exemple, pour une suite croissante, on ait  $x_{50} \preceq x_{100}$ . On pourrait avoir une situation « en cercle », où chaque élément est inférieur au suivant, mais où on tourne en rond :

Sans compter qu'on peut montrer qu'il n'existe pas de relation d'ordre sur  $\mathbb{C}$  compatible avec la structure de corps, cf. exercice 11.



Heureusement, les propriétés d'une relation d'ordre permettent d'éviter ce genre de problème. Montrons en effet (raisonnement analogue dans les autres cas) que  $(x_n)$  est strictement décroissante si et seulement si :  $\forall (n, p) \in \mathbb{N}^2, n < p \Rightarrow (u_n \preccurlyeq u_p \text{ et } u_n \neq u_p)$ .


Supposons que  $(u_n)$  soit strictement décroissante. Soit  $n \in \mathbb{N}$ . Montrons par récurrence (sur  $p$ ) que, pour tout  $p > n$ ,  $u_n \preccurlyeq u_p$  et  $u_n \neq u_p$ .

- Si  $p > n$ , notons  $H_p$  : «  $u_n \preccurlyeq u_p$  et  $u_n \neq u_p$  ».
- Par hypothèse,  $u_n \preccurlyeq u_{n+1}$  et  $u_n \neq u_{n+1}$  :  $H_{n+1}$  est vraie.
- Soit  $p > n$ . Supposons  $H_p$  vraie et prouvons que  $H_{p+1}$  est vraie. Par hypothèse de récurrence,  $u_n \preccurlyeq u_p$  et  $u_n \neq u_p$ . Par hypothèse (sur la suite),  $u_p \preccurlyeq u_{p+1}$  et  $u_p \neq u_{p+1}$ . Par transitivité,  $u_n \preccurlyeq u_{p+1}$ . Si  $u_n = u_{p+1}$  alors  $u_p \preccurlyeq u_n$  et puisque  $u_n \preccurlyeq u_p$ , par antisymétrie,  $u_n = u_p$  ce qui contredit l'hypothèse de récurrence : on en déduit que  $u_n \neq u_{p+1}$ , ce qui clôt la récurrence.

$n$  étant quelconque, on a donc montré :  $\forall (n, p) \in \mathbb{N}^2, n < p \Rightarrow (u_n \preccurlyeq u_p \text{ et } u_n \neq u_p)$ . La réciproque est immédiate : supposons ce résultat. Soit  $n \in \mathbb{N}$ . En prenant  $p = n + 1$ , alors  $n < p$  donc on a bien  $u_n \preccurlyeq u_{n+1}$  et  $u_n \neq u_{n+1}$ , la suite est strictement décroissante.

**Remarque :** Ce résultat n'étant pas explicitement au programme, il faut le redémontrer à chaque fois (cf. par exemple exercice 12).

## II.4 Ordre total, ordre partiel

 Attention, assimiler n'importe quelle relation d'ordre à la relation d'ordre réelle  $\leq$  peut être dangereux ! On voit avec l'exemple de l'inclusion que, si  $R$  est une relation d'ordre sur  $E$  et si  $x$  et  $y$  sont deux éléments de  $E$ , on n'a pas forcément  $xRy$  ou  $yRx$  ! Certains éléments ne peuvent pas être comparés ! Par exemple, si  $E = \mathbb{R}$ , alors  $\mathbb{R}_+$  n'est pas inclus dans  $\mathbb{R}_-$  et  $\mathbb{R}_-$  n'est pas inclus dans  $\mathbb{R}_+$ . Ainsi, pour une relation d'ordre quelconque, il est faux de dire : « si on prend deux éléments, il y en a forcément un qui est plus petit que l'autre ». Ce sera le cas uniquement pour les relations d'ordre total. Plus précisément :

**Définition.** Soit  $\preccurlyeq$  une relation d'ordre sur  $E$ .

- On dit que  $\preccurlyeq$  est une relation d'ordre total ou un ordre total si deux éléments quelconques de  $E$  sont toujours comparables, c'est-à-dire :  $\forall (x, y) \in E^2, x \preccurlyeq y$  ou  $y \preccurlyeq x$ . On dit alors que  $(E, \preccurlyeq)$  est un ensemble totalement ordonné.
- Dans le cas contraire, on dit que  $\preccurlyeq$  est une relation d'ordre partiel ou un ordre partiel et que  $(E, \preccurlyeq)$  est un ensemble partiellement ordonné.

**Exemples :** Parmi les relations d'ordre du paragraphe précédent :

- l'ordre  $\leq$  sur  $\mathbb{R}$  est un ordre total.
- l'inclusion est un ordre partiel dès que  $E$  a au moins deux éléments. En effet, si  $a$  et  $b$  sont deux éléments distincts de  $E$ , alors on ne peut pas comparer  $\{a\}$  et  $\{b\}$  car aucun des deux n'est inclus dans l'autre.
- la divisibilité est un ordre partiel dans  $\mathbb{N}$  (ou  $\mathbb{N}^*$  ou...) : par exemple, 2 ne divise pas 3 et 3 ne divise pas 2.

En d'autres termes, comme sur  $\mathbb{R}$ , une suite (strictement) croissante préserve l'ordre des indices, et c'est l'inverse pour une suite décroissante. Attention, le reste du cours sur les suites n'est plus valide : par exemple, une suite décroissante minorée ne converge pas forcément ! D'ailleurs, qu'est-ce qu'une suite convergente dans un ensemble ordonné quelconque ? La définition avec des  $\varepsilon$  n'est plus valable !

Évidemment,  $\preccurlyeq$  est une relation d'ordre quelconque et n'a rien à voir avec les relations d'ordre notées de la même façon dans les paragraphes précédents.

De façon générale, si on prend deux parties de  $E$ , il n'y a aucune raison que l'une des deux soit incluse dans l'autre.

- l'ordre  $\leq$  sur  $\mathbb{R}$  est un ordre partiel car (par exemple), les fonctions cos et sin ne sont pas comparables.
- pour l'ordre produit et l'ordre lexicographique, cela dépend des ordres  $\leq_E$  et  $\leq_F$ . Contentons-nous de nous placer sur  $\mathbb{R}^2$  : alors l'ordre produit est partiel (les couples  $(1, 2)$  et  $(2, 1)$  sont incomparables) tandis que l'ordre lexicographique est total. En effet, soient  $(x_1, y_1)$  et  $(x_2, y_2)$  deux éléments de  $\mathbb{R}^2$ .

- ★ Si  $x_1 < x_2$  alors  $(x_1, y_1) \prec (x_2, y_2)$ .
- ★ Si  $x_2 < x_1$  alors  $(x_2, y_2) \prec (x_1, y_1)$ .
- ★ Si  $x_1 = x_2$  et  $y_1 \leq y_2$ , alors  $(x_1, y_1) \prec (x_2, y_2)$ , tandis que si  $x_1 = x_2$  et  $y_2 \leq y_1$ , c'est le contraire.

Ici,  $\prec$  est évidemment l'ordre lexicographique sur  $\mathbb{R}^2$ .

## II.5 Majorants, minorants et Cie

Dans ce paragraphe, on suppose que  $E$  est muni d'une relation d'ordre  $\prec$ , et on se donne  $A$  une partie non vide de  $E$ . Les définitions sont alors les mêmes que sur  $\mathbb{R}$ .

### Définition (Majorant, minorant).

- Soit  $M \in E$ . On dit que  $M$  est **un** majorant de  $A$  si :  $\forall a \in A, a \prec M$ .
- Soit  $m \in E$ . On dit que  $m$  est **un** minorant de  $A$  si :  $\forall a \in A, m \prec a$ .
- Si  $A$  admet un majorant  $M$ , on dit que  $A$  est majorée (par  $M$ ).
- Si  $A$  admet un minorant  $m$ , on dit que  $A$  est minorée (par  $m$ ).
- Si  $A$  est majorée et minorée, on dit que  $A$  est bornée.

### Définition (Plus petit, plus grand élément).

- Soit  $M$  un majorant de  $A$ . On dit que  $M$  est un plus grand élément ou un maximum de  $A$  si  $M \in A$ . En d'autres termes, un maximum est un majorant qui appartient à l'ensemble.
- Soit  $m$  un minorant de  $A$ . On dit que  $m$  est un plus petit élément ou un minimum de  $A$  si  $m \in A$ . En d'autres termes, un minimum est un minorant qui appartient à l'ensemble.

Sur un ensemble quelconque, il n'y a évidemment pas de valeur absolue, et donc le critère «  $A$  est bornée si et seulement si  $A$  est majorée en valeur absolue » n'a pas de sens !

**Proposition.** Si  $A$  admet un maximum (respectivement minimum), celui-ci est unique. On le note alors  $\max(A)$  (respectivement  $\min(A)$ ).

DÉMONSTRATION. Soient  $M_1$  et  $M_2$  deux maxima de  $A$ . Puisque  $M_1$  est un majorant de  $A$  et  $M_2$  un élément de  $A$ , alors  $M_2 \prec M_1$ . Par symétrie des rôles,  $M_1 \prec M_2$  donc  $M_1 = M_2$  par antisymétrie de  $\prec$ . De même pour le minimum.

### Définition (Borne supérieure, borne inférieure).

- Sous réserve d'existence, on appelle borne supérieure ou supremum de  $A$  le plus petit de ses majorants.
- Sous réserve d'existence, on appelle borne inférieure ou infimum de  $A$  le plus grand de ses minorants.

**Remarque :** Lorsqu'elle existe, la borne supérieure est donc le plus petit élément de  $B$ , l'ensemble des majorants de  $A$ , et est donc unique : on la note  $\sup(A)$ . De même, lorsqu'elle existe, la borne inférieure est donc le plus grand élément de  $C$ , l'ensemble des minorants de  $A$ , et est donc unique : on la note  $\inf(A)$ .

Contrairement à ce qui se passe sur  $\mathbb{R}$ , une partie non vide majorée n'admet pas forcément de borne supérieure, même si l'ordre est total ! On a déjà vu un contre-exemple dans le chapitre 12 :  $\mathbb{Q}$  n'a pas la propriété de la borne supérieure...



### Proposition.

- Si  $A$  admet un maximum, alors  $A$  admet une borne supérieure et  $\sup(A) = \max(A)$ .
- Si  $A$  admet un minimum, alors  $A$  admet une borne inférieure et  $\inf(A) = \min(A)$ .

**Remarque :** En d'autres termes, comme sur  $\mathbb{R}$  : « maximum  $\Rightarrow$  borne supérieure » mais la réciproque est fautive car une borne supérieure n'appartient pas forcément à l'ensemble. De même pour une borne inférieure.

**DÉMONSTRATION.** Supposons que  $A$  admette un maximum  $M$ . Soit  $B$  l'ensemble des majorants de  $A$ . Alors  $M \in B$  car le maximum est un majorant. De plus, soit  $\tilde{M} \in B$ . Puisque  $M \in A$ , alors  $M \leq \tilde{M}$  :  $M$  est un minorant de  $B$ . Puisque  $M \in B$ , c'est le plus petit élément de  $B$  donc la borne supérieure de  $A$ . De même pour la borne inférieure.

### Exemples :

Pour  $E$  muni de l'inclusion : si  $A$  est un ensemble de parties de  $E$ , alors  $A$  admet une borne supérieure et une borne inférieure. Montrons en effet que  $U_A = \bigcup_{X \in A} X$  et  $I_A = \bigcap_{X \in A} X$  sont respectivement la borne supérieure et la borne inférieure de  $A$ .

- Tout d'abord, si  $X \in A$ , alors  $I_A \subset X$  et  $X \subset U_A$  :  $I_A$  est un minorant de  $A$  et  $U_A$  un majorant.
- Soit  $M$  un majorant de  $A$ . Alors,  $X \subset M$  pour tout  $X \in A$  donc  $U_A \subset M$  :  $U_A$  est le plus petit des majorants donc  $U_A = \sup(A)$ .
- Soit  $m$  un minorant de  $A$ . Alors  $m \subset X$  pour tout  $X \in A$  donc  $m \subset I_A$  :  $I_A$  est le plus grand des minorants de  $A$  donc  $I_A = \inf(A)$ .
- Cependant,  $U_A$  et  $I_A$  n'appartiennent pas forcément à  $A$  donc  $A$  n'a pas forcément de plus grand ou plus petit élément. Par exemple, si  $A = \{\mathbb{R}_+; \mathbb{R}_-\}$ , alors  $A$  n'a pas de plus petit élément ni de plus grand élément car aucun élément n'est plus grand que l'autre, alors que  $A$  admet une borne supérieure et une borne inférieure (égales à  $\mathbb{R}$  et  $\{0\}$  respectivement).  $A$  admet un maximum lorsque l'un des éléments de  $A$  contient tous les autres, et  $A$  admet un minimum lorsque l'un des éléments est contenu dans tous les autres, ce qui n'est pas toujours le cas.

Pour la divisibilité :

- Plaçons-nous sur  $\mathbb{N}^*$ . Soient  $a$  et  $b$  dans  $\mathbb{N}^*$ .  $a$  et  $b$  divisent  $a \vee b$  donc  $a \vee b$  est un majorant de  $\{a; b\}$ . Si  $M \in \mathbb{N}^*$  est un majorant de  $\{a; b\}$  alors  $a$  et  $b$  divisent  $M$  donc  $a \vee b \mid M$  (cf. chapitre 6 : un multiple de  $a$  et  $b$  est un multiple de leur ppcm). En d'autres termes,  $a \vee b$  est la borne supérieure de  $\{a; b\}$ .
- De même,  $a \wedge b$  divise  $a$  et  $b$ , et si  $m$  est un minorant de  $\{a; b\}$ , alors  $m$  divise  $a$  et  $b$  donc  $m$  divise  $a \wedge b$  (idem, un diviseur de  $a$  et  $b$  divise leur pgcd). En d'autres termes,  $a \wedge b$  est la borne inférieure de  $\{a; b\}$ . Cependant  $\{a; b\}$  n'admet un maximum ou un minimum que si l'un des deux divise l'autre, ce qui n'a aucune raison d'être le cas en général : encore un ensemble fini qui n'admet pas forcément de maximum ou de minimum.
- $\mathbb{N}^*$  admet un plus petit élément égal à 1. En effet,  $1 \mid n$  pour tout  $n \in \mathbb{N}^*$ . Cependant,  $\mathbb{N}^*$  n'admet pas de plus grand élément ni même de majorant. Supposons en effet qu'il existe  $M \in \mathbb{N}^*$  un majorant de  $\mathbb{N}^*$ . Alors, en particulier,  $2M \mid M$  ce qui est absurde (car  $M$  est non nul).
- Cependant, si on étudie la divisibilité sur  $\mathbb{N}$  et non plus sur  $\mathbb{N}^*$ , alors 0 est le plus grand élément de  $\mathbb{N}$  (même si c'est contre-intuitif) car  $n \mid 0$  pour tout  $n \in \mathbb{N}$ .
- Enfin, si on étudie la divisibilité sur  $E = \mathbb{N} \setminus \{0; 1\}$ , alors  $E$  n'admet ni minorant ni majorant, et donc ni plus grand élément ni plus petit élément. On montre de même que ci-dessus qu'il n'admet pas de majorant, montrons qu'il n'admet pas de minorant. Si  $E$  admet un minorant, alors il existe  $m \in E$  tel que  $m \mid 2$  et  $m \mid 3$ , ce qui est absurde car 2 et 3 n'ont aucun diviseur commun strictement supérieur à 1.



... De plus, dans le cas général, il n'y a plus la caractérisation séquentielle ni l'écriture avec des  $\varepsilon$  vue dans le chapitre 12 : il n'y a que la définition et, lorsqu'on a de la chance, le fait que le plus grand élément, quand il existe, est aussi la borne supérieure.



Méthode classique pour montrer qu'un élément  $M$  est égal à la borne supérieure : montrer que c'est un majorant puis qu'il est inférieur à tout majorant.



On voit donc qu'un ensemble fini peut ne pas admettre de minimum ni de maximum, contrairement à ce qui se passe sur  $\mathbb{R}$  ! Tout ce qu'on peut affirmer est qu'il n'existe pas de suite strictement monotone.



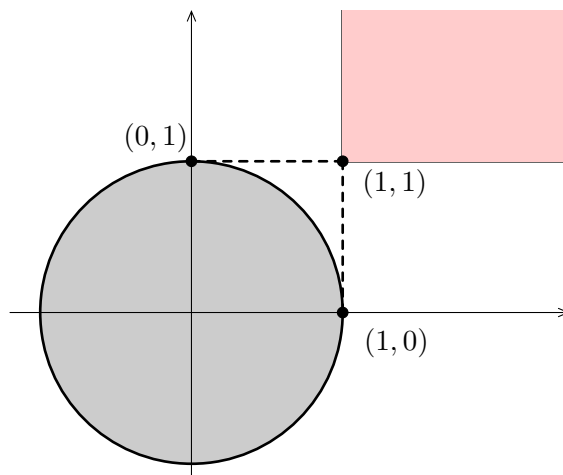
Cependant, il y a des éléments minimaux sur  $E$  : voir plus bas.

Pour l'ordre  $\preccurlyeq$  de l'exercice 52 du chapitre 12, on a montré que, si  $u$  est une suite bornée, alors la suite  $\bar{u}$  est le plus petit élément de l'ensemble  $A$  des suites décroissantes supérieures à  $u$ , et la suite  $\underline{u}$  est le plus grand élément de l'ensemble  $B$  des suites croissantes inférieures à  $u$ .

Pour l'ordre produit et l'ordre lexicographique, contentons-nous de chercher les majorant, borne supérieure et plus grand élément éventuels du disque unité fermé  $D = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 \leq 1\}$  sur  $\mathbb{R}^2$ .

Commençons par l'ordre produit.

- Soit  $M = (a, b) \in \mathbb{R}^2$ . Soit  $(x, y) \in D$ . Alors :  $(x, y) \preccurlyeq M \iff x \leq a$  et  $y \leq b$ . En particulier, si  $M$  est un majorant de  $D$ , alors  $(1, 0) \in D$  donc  $1 \leq a$  et  $(0, 1) \in D$  donc  $1 \leq b$ . Réciproquement, supposons que  $a \geq 1$  et  $b \geq 1$ , et soit  $(x, y) \in D$ . Puisque  $x^2 + y^2 = 1$ , alors  $x \leq 1$  et  $y \leq 1$  si bien que  $(x, y) \preccurlyeq (a, b)$ . En conclusion,  $M = (a, b)$  est un majorant de  $D$  si et seulement si  $1 \leq a$  et  $1 \leq b$ .
- Il en découle que  $D$  n'a pas de plus grand élément car aucun majorant n'appartient à  $D$ . En effet, si  $M(a, b)$  est un majorant, alors  $a^2 + b^2 \geq 2$ .
- Cependant,  $(1, 1)$  est la borne supérieure de  $D$  car tout majorant est supérieur ou égal à  $(1, 1)$ . Ci-dessous l'ensemble des majorants de  $D$  :

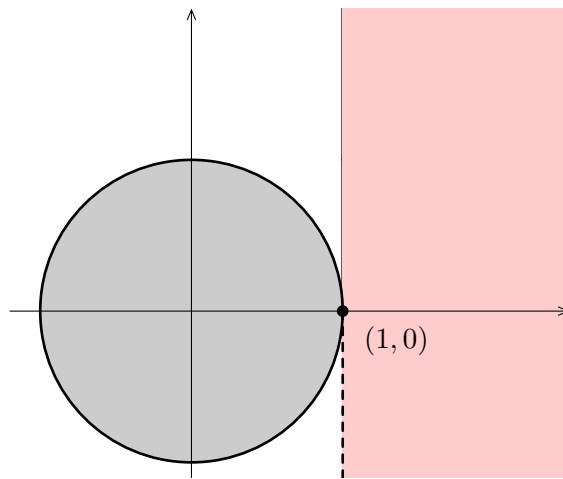


Lorsqu'on n'arrive pas à deviner le résultat comme ci-dessus, on voit donc que raisonner par analyse-synthèse est un bon moyen de trouver l'ensemble des majorants ou des mineurs.

Prenons à présent l'ordre lexicographique.

- Soit  $M = (a, b) \in \mathbb{R}^2$ . Soit  $(x, y) \in D$ . Alors :  $(x, y) \preccurlyeq M \iff x < a$  ou  $(x = a \text{ et } y \leq b)$ . En particulier, si  $M$  est un majorant de  $D$ , alors  $x \leq a$  pour tout  $(x, y) \in D$  donc  $1 \leq a$  car  $(1, 0) \in D$ . Supposons que  $a = 1$ . Alors  $0 \leq b$  car  $(1, 0) \in D$  donc  $(1, 0) \preccurlyeq M = (1, b)$ . Finalement, si  $M = (a, b)$  est un majorant de  $D$ , alors  $1 \leq a$  et, si  $a = 1$ , alors  $0 \leq b$ .
- Montrons la réciproque. Soit  $(x, y) \in D$ . Alors (voir ci-dessus)  $x \leq 1$ . Supposons que  $1 < a$ . Alors  $(x, y) \preccurlyeq M$ . Supposons à présent que  $a = 1$  et  $b \geq 0$ . Si  $x < 1$  alors  $(x, y) \preccurlyeq M$  et, si  $x = 1$ , alors  $y = 0$  car  $x^2 + y^2 = 1$  donc  $(x, y) \preccurlyeq M$ . En d'autres termes,  $M$  est bien un majorant de  $D$ , c'est-à-dire que les majorants de  $D$  sont exactement les couples  $(a, b)$  avec  $a > 1$  ou  $(a = 1 \text{ et } b \geq 0)$ .
- En particulier,  $(1, 0)$  est un majorant de  $D$ , et puisque  $(1, 0) \in D$ , c'est le maximum (donc la borne supérieure) de  $D$ . Ci-dessous l'ensemble des majorants de  $D$  :





Terminons par une nouvelle notion (HP) que nous n'avons pas définie sur  $\mathbb{R}$  : la notion d'élément maximal.

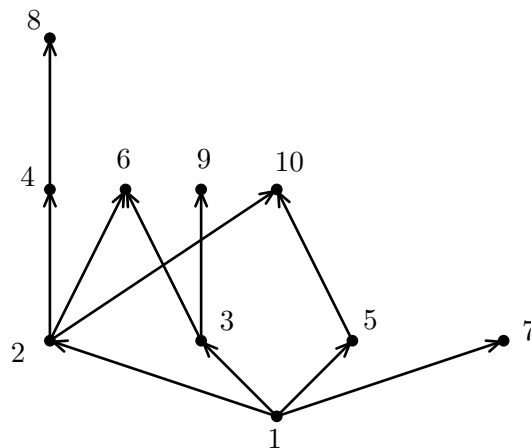
**Définition (Élément maximal, élément minimal).**

- Soit  $M \in A$ . On dit que  $M$  est un élément maximal de  $A$  s'il n'existe pas d'élément de  $A$  strictement supérieur à  $M$ . En d'autres termes,  $M$  est un élément maximal si :  $\forall x \in A, M \preccurlyeq x \Rightarrow x = M$ .
- Soit  $m \in A$ . On dit que  $m$  est un élément minimal de  $A$  s'il n'existe pas d'élément de  $A$  strictement inférieur à  $m$ . En d'autres termes,  $m$  est un élément minimal si :  $\forall x \in A, x \preccurlyeq m \Rightarrow x = m$ .

**Remarque :** Un plus grand élément est évidemment un élément maximal, mais il faut bien comprendre que, si l'ordre n'est pas total, un élément maximal n'a aucune raison d'être supérieur à tous les éléments de l'ensemble, et donc n'est pas forcément le plus grand élément de l'ensemble. C'est pour cela que nous n'avons pas défini la notion d'élément maximal dans  $\mathbb{R}$  : quand l'ordre est total, un élément maximal n'est rien d'autre qu'un maximum.

**Exemple :** Plaçons-nous sur  $\llbracket 1 ; 10 \rrbracket$  avec, comme relation d'ordre, la divisibilité. Alors 6, 7, 8, 9 et 10 sont des éléments maximaux (et 1 est l'unique élément minimal car c'est le plus petit élément). En effet (par exemple), si  $6|n$  dans  $\llbracket 1 ; 10 \rrbracket$  alors  $n = 6$ , et de même pour les autres.

**Remarque :** On peut parfois représenter une relation d'ordre  $\preccurlyeq$  par un diagramme : on représente les éléments de  $E$  sous forme de points et on relie deux points  $a$  et  $b$  par une flèche de  $a$  vers  $b$  si  $a \preccurlyeq b$ . Ci-dessous le diagramme associé à la divisibilité sur  $\llbracket 1 ; 10 \rrbracket$ .



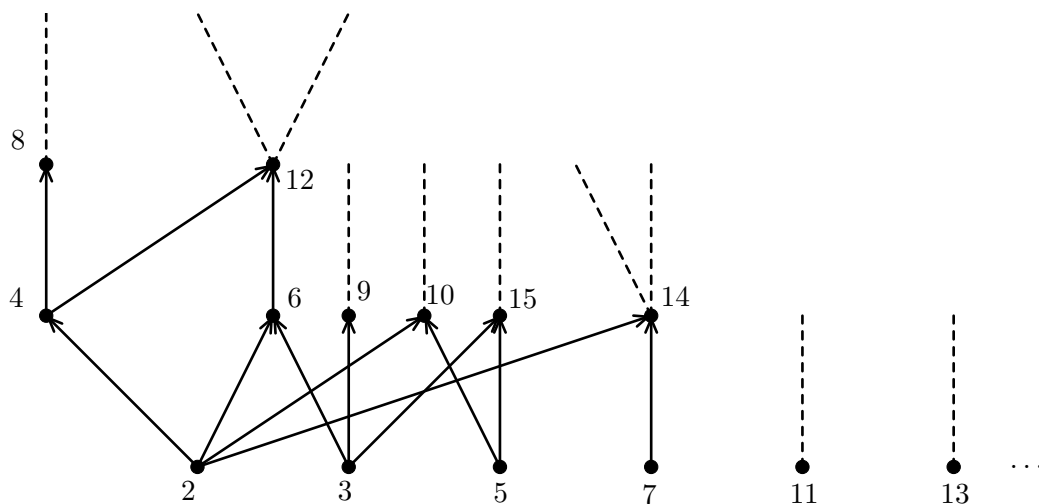
On ne le fait en général que lorsque  $E$  est fini et encore, cela peut parfois ne pas ressembler à grand-chose... Rien qu'avec 10 éléments il y a des croisements, et avec 15 c'est encore pire... On ne le fait pas non plus quand l'ordre est total car alors le diagramme est linéaire : voir  $\mathbb{N}$ ,  $\mathbb{Z}$  ou  $\mathbb{R}$ .

On peut visualiser les éléments maximaux comme les derniers éléments d'une chaîne, comme le terminus d'une ligne de train si on veut. On voit alors très bien qu'il peut y

avoir plus éléments maximaux car on ne peut pas toujours les comparer : tout dépend la ligne de train que l'on prend... On peut bien sûr faire la même chose pour les éléments minimaux et voir les éléments minimaux comme les diverses gares de départ d'une ligne de train : voir le diagramme ci-dessous.

**Exemple :** Montrons que, sur  $E = \mathbb{N} \setminus \{0; 1\}$ , il n'y a pas d'élément maximal et les éléments minimaux sont exactement les nombres premiers. Soit  $M \in E$ . Alors  $M|2M$  et  $M \neq 2M$  (car  $M \neq 0$ ) donc  $M$  n'est pas un élément maximal :  $M$  étant quelconque,  $E$  n'admet pas d'élément maximal.

Soit  $p$  un nombre premier et soit  $d \in E$  tel que  $d|p$ .  $d \neq 1$  donc  $d = p$  car  $p$  est premier, si bien que les nombres premiers sont des éléments minimaux. Réciproquement, si  $n$  n'est pas un nombre premier, alors il existe  $1 < p, q < n$  tels que  $n = p \times q$ . Par conséquent,  $p \in E$ ,  $p|n$  et  $p \neq n$  :  $n$  n'est pas un élément minimal. D'où le résultat.



### III Relations d'équivalence

#### III.1 Définition

**Définition.** Une relation d'équivalence est une relation binaire réflexive, symétrique et transitive.

**Remarque :** Intuitivement, une relation d'équivalence sert à définir rigoureusement le fait que des éléments ont un point commun, une caractéristique commune, c'est-à-dire qu'ils « sont les mêmes, qu'ils ne comptent que pour un » **quand on s'intéresse à cette caractéristique**. Les trois conditions de la définition sont alors naturelles :

- la réflexivité dit juste qu'un élément est « le même » que lui-même.
- la symétrie dit juste que si un élément est « le même » qu'un autre, alors le deuxième est « le même » que le premier. Pour cette raison, si  $xRy$ , au lieu de dire que  $x$  est en relation avec  $y$ , on dit que  $x$  et  $y$  sont en relation. Ainsi, contrairement à une relation d'ordre, pour une relation d'équivalence, les deux éléments de  $E$  jouent le même rôle.
- la transitivité dit juste que si un élément est « le même » qu'un deuxième, et si celui-ci est « le même » qu'un troisième, alors le premier est « le même » que le troisième.

#### III.2 Exemples

La relation « avoir les yeux de la même couleur » est une relation d'équivalence. En effet :

- Une personne a la même couleur d'yeux qu'elle-même : c'est une relation réflexive.

Certaines relations d'ordre sont notées  $\sim$ ,  $\approx$ ,  $\equiv$ , à ne pas confondre avec le  $\equiv$  réel (mais, quand ça arrivera, il n'y aura aucune ambiguïté).

Attention, comme dit ci-dessus, quand on dit qu'ils sont « les mêmes », c'est uniquement vis-à-vis d'une caractéristique, cela ne signifie pas qu'ils soient égaux ! Une relation d'équivalence sert justement à définir rigoureusement la notion d'appartenir à la « même communauté ».

- Si une personne a la même couleur d'yeux qu'une deuxième, alors la deuxième personne a la même couleur d'yeux que la première : c'est une relation symétrique.
- Si une personne a les yeux de la même couleur qu'une deuxième, et cette deuxième a la même couleur d'yeux qu'une troisième, alors la première personne et la troisième ont les yeux de la même couleur : c'est une relation transitive.

La relation « être né le même jour de la semaine » (i.e. un lundi, un mardi etc.) est une relation d'équivalence. En effet :

- Une personne est née le même jour de la semaine qu'elle-même : c'est une relation réflexive.
- Si une personne est née le même jour de la semaine qu'une deuxième, alors la deuxième personne est née le même jour de la semaine que la première : c'est une relation symétrique.
- Si une personne est née le même jour de la semaine qu'une deuxième, et cette deuxième est née le même jour de la semaine qu'une troisième, alors la première personne et la troisième sont nées le même jour de la semaine : c'est une relation transitive.

On peut en définir beaucoup d'autres : avoir le même nom de famille, habiter dans le même pays, être dans la même classe etc.

L'égalité est une relation d'équivalence sur  $E$  (c'est d'ailleurs aussi une relation d'ordre, et c'est la seule à être les deux à la fois).

Soit  $m \in \mathbb{R}^*$ . Montrons que la congruence modulo  $m$  est une relation d'équivalence sur  $\mathbb{R}$ .

- Soit  $x \in \mathbb{R}$ . Alors  $x \equiv x[m] : \equiv$  est réflexive.
- Soit  $(x, y) \in \mathbb{R}^2$  tel que  $x \equiv y[m]$ . Alors il existe  $k \in \mathbb{Z}$  tel que  $x = y + km$  si bien que  $y = x + (-k)m$ . Or,  $-k \in \mathbb{Z}$  donc  $y \equiv x[m] : \equiv$  est symétrique.
- Soit  $(x, y, z) \in \mathbb{R}^3$  tel que  $x \equiv y[m]$  et  $y \equiv z[m]$ . Alors il existe  $(k_1, k_2) \in \mathbb{Z}^2$  tel que  $y = x + k_1m$  et  $y = z + k_2m$  donc  $z = x + (k_1 + k_2)m$ . Or,  $k_1 + k_2 \in \mathbb{Z}$  donc  $z \equiv x[m] : \equiv$  est transitive.

On peut prendre  $m = 0$ , mais alors la congruence modulo  $m$  est tout simplement l'égalité.

Si  $E$  et  $F$  sont deux ensembles, on dit que  $E$  est équipotent à  $F$  s'il existe une bijection  $\varphi$  de  $E$  dans  $F$ . Montrer qu'on définit ainsi une relation d'équivalence.

- Soit  $E$  un ensemble. Alors  $\text{Id}_E$  est une bijection de  $E$  dans  $E$  donc  $E$  est équipotent à  $E$  : c'est une relation réflexive.
- Soient  $E$  et  $F$  deux ensembles tel que  $E$  soit équipotent à  $F$ . Alors il existe une bijection  $\varphi$  de  $E$  dans  $F$ . Par conséquent,  $\varphi^{-1}$  est une bijection de  $F$  dans  $E$ , c'est-à-dire que  $F$  est équipotent à  $E$  : c'est une relation symétrique (et donc on dira que deux ensembles sont équipotents lorsqu'il existe une bijection de l'un dans l'autre).
- Soient  $(E, F, G)$  trois ensembles tels que  $E$  et  $F$  soient équipotents, ainsi que  $F$  et  $G$ . Il existe donc une bijection  $\varphi_1$  de  $E$  dans  $F$  et une bijection  $\varphi_2$  de  $F$  dans  $G$ . Dès lors,  $\varphi_2 \circ \varphi_1$  est une bijection de  $E$  dans  $G$  (une composée de bijections est une bijection, cf. chapitre 4), c'est-à-dire que  $E$  et  $G$  sont équipotents : c'est une relation transitive.

Nous avons étudié la congruence sur  $\mathbb{R}$  modulo un réel  $m$  quelconque, mais on montrerait de la même façon que, pour tout  $n \in \mathbb{Z}$ , la congruence modulo  $n$  est une relation d'équivalence sur  $\mathbb{Z}$ . Cela nous permettra de définir les ensembles  $\mathbb{Z}/n\mathbb{Z}$ , cf. paragraphe IV.2.

### Remarques :

- Cette relation d'équivalence nous permettra de définir rigoureusement la notion de cardinal au chapitre 17.
- Cette relation d'équivalence formalise l'intuition qu'on a de deux ensembles « de même taille » (cf. chapitre 4). Dans la même veine, s'il existe une injection de  $E$  dans  $F$ , on peut se dire que «  $E$  est plus petit que  $F$  » et définir une relation d'ordre par :  $E \preceq F$  si et seulement s'il existe une injection de  $E$  dans  $F$ . Sauf que cette relation n'est pas une relation d'ordre car elle n'est pas antisymétrique : s'il existe une injection de  $E$  dans  $F$  et une injection de  $F$  dans  $E$ , tout ce qu'on peut dire est qu'il existe une bijection entre  $E$  et  $F$  (théorème de Cantor-Bernstein, cf. chapitre 4). Bon ben tant pis... On voit comme au paragraphe II.2 qu'il faut parfois être prudent avec l'interprétation d'une relation d'ordre comme moyen de dire qu'un élément est « plus petit » qu'un autre.

Soit  $E = \mathbb{Z} \times \mathbb{Z}^*$ . On définit sur  $E$  la relation  $\equiv_{\mathbb{Q}}$  par :

$$(p_1, q_1) \equiv_{\mathbb{Q}} (p_2, q_2) \iff p_1 q_2 = p_2 q_1$$

Montrons que c'est une relation d'équivalence.

- Soit  $(p, q) \in E$ . Alors  $p \times q = p \times q$  donc  $(p, q) \equiv_{\mathbb{Q}} (p, q) : \equiv_{\mathbb{Q}}$  est réflexive.
- Soient  $(p_1, q_1)$  et  $(p_2, q_2)$  deux éléments de  $E$  tels que  $(p_1, q_1) \equiv_{\mathbb{Q}} (p_2, q_2)$ . Alors  $p_1 q_2 = p_2 q_1$  donc  $p_2 q_1 = p_1 q_2$  donc  $(p_2, q_2) \equiv_{\mathbb{Q}} (p_1, q_1) : \equiv_{\mathbb{Q}}$  est symétrique.
- Soient  $(p_1, q_1), (p_2, q_2)$  et  $(p_3, q_3)$  trois éléments de  $E$  tels que  $(p_1, q_1) \equiv_{\mathbb{Q}} (p_2, q_2)$  et  $(p_2, q_2) \equiv_{\mathbb{Q}} (p_3, q_3)$ . Alors  $p_1 q_2 = p_2 q_1$  donc, en multipliant par  $q_3$ ,  $p_1 q_2 q_3 = p_2 q_1 q_3$ . Or,  $p_2 q_3 = p_3 q_2$  donc cette égalité devient  $p_1 q_2 q_3 = p_3 q_2 q_1$  donc  $q_2(p_1 q_3 - p_3 q_1) = 0$ . Or,  $q_2 \neq 0$  donc  $p_1 q_3 - p_3 q_1 = 0$  c'est-à-dire que  $p_1 q_3 = p_3 q_1$ . En d'autres termes,  $(p_1, q_1) \equiv_{\mathbb{Q}} (p_3, q_3) : \equiv_{\mathbb{Q}}$  est transitive.

**Remarque :** Pourquoi ce nom  $\equiv_{\mathbb{Q}}$  pour cette relation? Et pourquoi, à la fin, n'a-t-on pas tout simplement simplifié par  $q_2 \neq 0$ ? Car cette relation d'équivalence permet de définir  $\mathbb{Q}$  proprement et donc on a fait « comme si  $\mathbb{Q}$  n'existait pas encore ». Cette relation d'équivalence dit en fait que deux couples sont équivalents lorsqu'ils définissent le même quotient  $p/q$  (en effet, quand  $\mathbb{Q}$  est défini, alors  $p_1/q_1 = p_2/q_2$  si et seulement si  $p_1 q_2 = p_2 q_1$ ). Cette relation permettra de définir  $\mathbb{Q}$  comme ensemble quotient (cf. paragraphe IV), et c'est la raison pour laquelle on n'a pas divisé dans cette démonstration, car on voulait faire « comme si  $\mathbb{Q}$  n'existait pas encore » pour pouvoir le construire à partir de cette relation d'équivalence. Bref, on en reparle.

On se donne  $E = (\mathbb{R}^2)^2$  l'ensemble des couples  $(A, B)$  de points du plan (un couple de points  $(A, B)$  est aussi appelé un bipoint). On définit la relation  $\sim$  par :

$$(A, B) \sim (C, D) \iff (x_B - x_A = x_D - x_C \text{ et } y_B - y_A = y_D - y_C)$$

On a pris les notations transparentes  $A(x_A, y_A)$ ,  $B(x_B, y_B)$  etc.

Montrons que c'est une relation d'équivalence.

- Soit  $(A, B) \in E$ . Alors  $x_B - x_A = x_B - x_A$  et  $y_B - y_A = y_B - y_A$  donc  $(A, B) \sim (A, B) : \sim$  est réflexive.
- Soient  $(A, B)$  et  $(C, D)$  deux éléments de  $E$  tels que  $(A, B) \sim (C, D)$ . Alors  $(x_B - x_A = x_D - x_C \text{ et } y_B - y_A = y_D - y_C)$  donc  $(x_D - x_C = x_B - x_A \text{ et } y_D - y_C = y_B - y_A)$  donc  $(C, D) \sim (A, B) : \sim$  est symétrique.
- Soient  $(A, B), (C, D)$  et  $(E, F)$  trois éléments de  $E$  tels que  $(A, B) \sim (C, D)$  et  $(C, D) \sim (E, F)$ . Alors  $(x_B - x_A = x_D - x_C \text{ et } y_B - y_A = y_D - y_C)$  et  $(x_D - x_C = x_F - x_E \text{ et } y_D - y_C = y_F - y_E)$  donc  $(x_B - x_A = x_F - x_E \text{ et } y_B - y_A = y_F - y_E)$  i.e.  $(A, B) \sim (E, F) : \sim$  est transitive.

On peut encore définir nombre d'exemples :

- la relation « avoir le même signe » est une relation d'équivalence sur  $\mathbb{R}^*$  (attention, pas sur  $\mathbb{R}$ !).
- la relation « avoir le même module » est une relation d'équivalence sur  $\mathbb{C}$ .
- la relation « avoir les mêmes arguments » est une relation d'équivalence sur  $\mathbb{C}^*$  (attention, pas sur  $\mathbb{C}$ !).
- la relation «  $\cos(x) = \cos(y)$  » est une relation d'équivalence sur  $\mathbb{R}$ . Plus généralement, si  $f$  est une fonction de  $\mathbb{R}$  dans  $\mathbb{R}$ , alors la relation «  $f(x) = f(y)$  » est une relation d'équivalence sur  $\mathbb{R}$ .
- la relation « avoir la même limite » est une relation d'équivalence sur l'ensemble des suites **convergentes**.
- et bien plus encore!

Encore plus généralement, si  $f$  est une fonction de  $E$  dans  $F$ , alors la relation «  $f(x) = f(y)$  » est une relation d'équivalence sur  $E$ .

### III.3 Classes d'équivalence

**Définition.** Soit  $\sim$  une relation d'équivalence sur  $E$ . Soit  $x \in E$ . On appelle classe d'équivalence de  $x$  l'ensemble

$$\text{cl}(x) = \{y \in E \mid x \sim y\}$$

En d'autres termes, c'est l'ensemble des éléments de  $E$  équivalents à  $x$ .

On rencontre également les notations  $\bar{x}$ ,  $\dot{x}$  ou, plus rarement,  $C_x$ .

**Remarque :** On a vu qu'une relation d'équivalence était un moyen de définir rigoureusement que des éléments avaient un point commun, avaient une caractéristique commune, étaient « les mêmes », quand on s'intéressait à cette caractéristique. Il est donc naturel de les regrouper en « communauté » selon cette caractéristique, et cela donne les diverses classes d'équivalence. Une fois ce point compris, le résultat suivant est totalement intuitif.

**Proposition.** Soit  $\sim$  une relation d'équivalence sur  $E$ . Alors les classes d'équivalence de  $\sim$  forment une partition de  $E$ .

**DÉMONSTRATION.** Tout d'abord, une classe d'équivalence n'est jamais vide car une relation d'équivalence est réflexive et donc, pour tout  $x \in E$ ,  $x \in \text{cl}(x)$ .

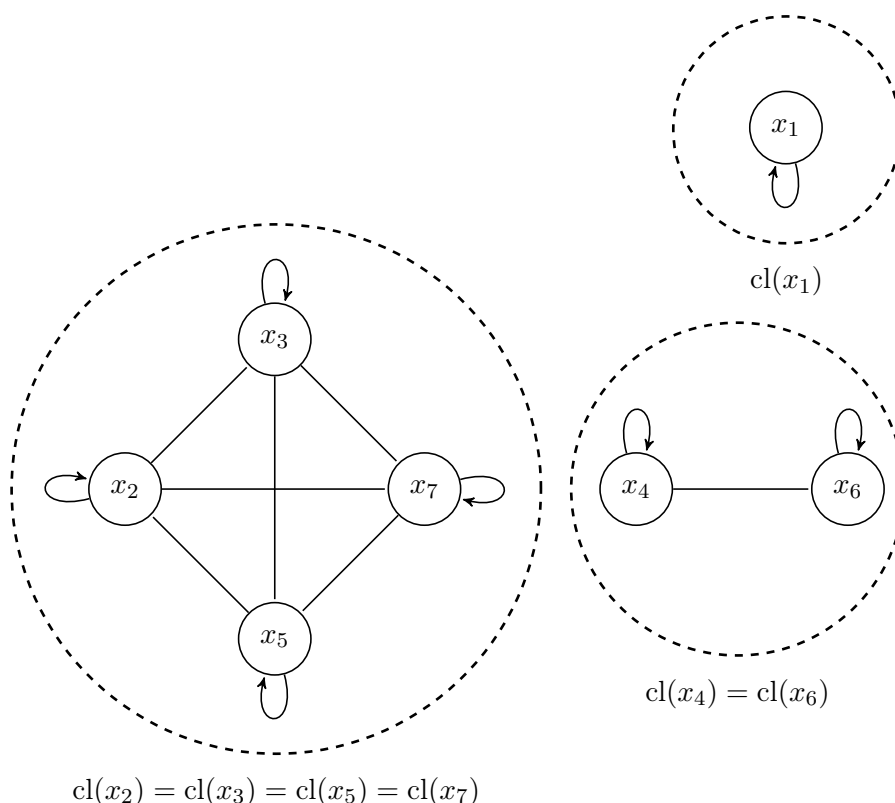
Soit  $x \in E$ . Alors  $x \in \text{cl}(x)$  donc  $E \subset \bigcup_{x \in E} \text{cl}(x)$ . L'inclusion réciproque étant évidente, on a l'égalité.

Montrons à présent que deux classes d'équivalence sont soit disjointes, soit confondues. Soit  $(x, y) \in E^2$  tel que  $\text{cl}(x) \cap \text{cl}(y) \neq \emptyset$  : il existe donc  $z \in \text{cl}(x) \cap \text{cl}(y)$ . Soit  $t \in \text{cl}(x)$ . Alors  $t \sim x$  et  $x \sim z$  donc, par transitivité,  $t \sim z$ . Or,  $z \sim y$  donc  $t \sim y$ . En d'autres termes,  $t \in \text{cl}(y)$  donc  $\text{cl}(x) \subset \text{cl}(y)$ . Par symétrie des rôles, on a l'inclusion réciproque, d'où l'égalité.

Rappelons qu'une partition est une famille de parties **non vides** et deux à deux disjointes dont l'union vaut tout l'ensemble.

**Morale de l'histoire :** deux classes d'équivalence sont soit disjointes, soit confondues.

**Remarque :** Comme pour une relation d'ordre, on peut parfois représenter une relation d'équivalence par un diagramme



- Le diagramme se décompose en un certain nombre de blocs (les diverses « communautés » formées par les différentes caractéristiques, c'est-à-dire les diverses classes d'équivalence) non reliés les uns aux autres (car deux éléments de deux classes distinctes ne sont pas en relation), et les éléments d'un même bloc étant tous reliés entre eux.
- À l'intérieur de chaque bloc, toutes les flèches possibles sont présentes (y compris celles reliant un point à lui-même) car tous les éléments d'une même classe d'équivalence sont en relation les uns avec les autres.
- Chaque point appartient à un bloc et à un seul (il est éventuellement seul dans ce groupe) car deux classes d'équivalence distinctes sont disjointes.

Examinons à présent les classes d'équivalence de certaines des relations vues précédemment :

- Les classes d'équivalence de la relation « avoir les yeux de la même couleur » sont les différents ensembles de personnes ayant les yeux de la même couleur.
- Les classes d'équivalence de la relation « être né le même jour de la semaine » sont les ensembles de personnes nées le même jour de la semaine : le groupe de personnes nées le lundi (éventuellement vide), le groupe de personnes nées le mardi (idem) etc.
- Les classes d'équivalence de la relation d'égalité sur  $E$  sont les singletons de  $E$ .
- Les classes d'équivalence de la relation « congruence modulo  $m$  » sont les ensembles des éléments ayant la même congruence modulo  $m$ . Par exemple, sur  $\mathbb{Z}$ , les classes d'équivalence modulo 4 sont :

$$\star \bar{0} = \{\dots; -12; -8; -4; 0; 4; 8; 12; \dots\}$$

$$\star \bar{1} = \{\dots; -11; -7; -3; 1; 5; 9; 13; \dots\}$$

$$\star \bar{2} = \{\dots; -10; -6; -2; 2; 6; 10; \dots\}$$

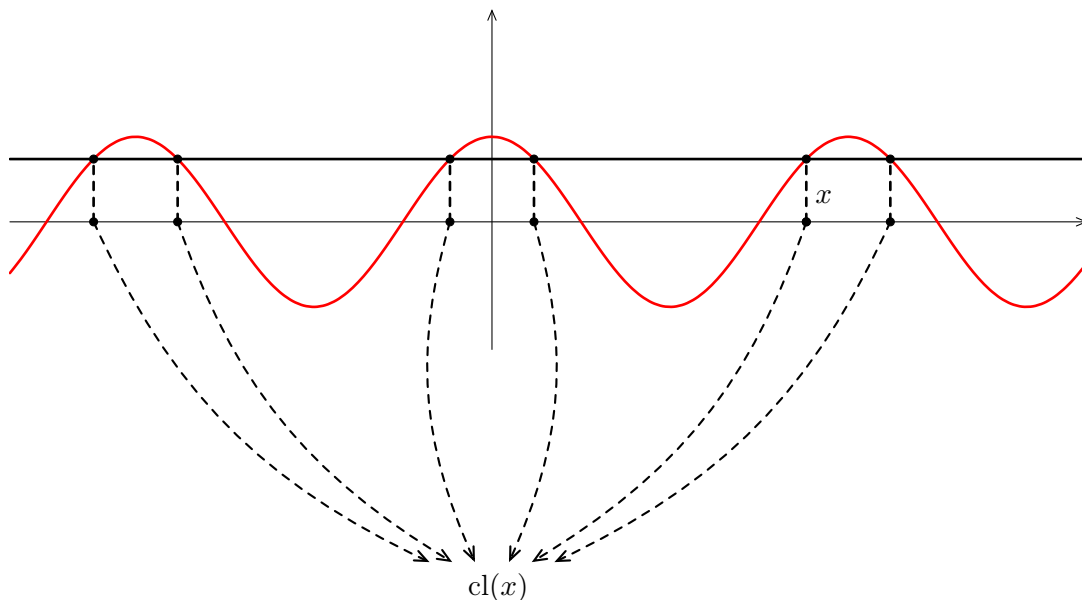
$$\star \bar{3} = \{\dots; -9; -5; -1; 3; 7; 11; \dots\}$$

Nous en reparlerons dans le paragraphe IV.2 quand nous parlerons de  $\mathbb{Z}/n\mathbb{Z}$ .

- Pour la relation « être équipotent », c'est un peu plus compliqué (surtout pour les ensembles infinis). Contentons-nous de dire que, pour les ensembles finis, les classes d'équivalence sont constituées des ensembles ayant le même nombre d'éléments.
- Pour la relation  $\equiv_{\mathbb{Q}}$ , les classes d'équivalence sont les couples donnant le même rationnel : c'est même comme cela qu'on définit un rationnel (voir le paragraphe suivant).
- Pour la relation d'équivalence sur les bipoints, les classes d'équivalences sont les ensembles de couples de points donnant les mêmes vecteurs : c'est même comme cela qu'on définit un vecteur (voir le paragraphe suivant).
- Pour la relation « avoir le même signe », les classes d'équivalence sont  $\mathbb{R}_+^*$  et  $\mathbb{R}_-^*$ .
- Pour la relation « avoir le même module », les classes d'équivalence sont tous les cercles de centre  $O$  (sans oublier le cercle de rayon nul!).
- Pour la relation « avoir les mêmes arguments », les classes d'équivalence sont les demi-droites issues de  $O$  (privées de  $O$  : on est sur  $\mathbb{C}^*$ !).
- Pour la relation «  $\cos(x) = \cos(y)$  », les classes d'équivalence sont les ensembles des éléments ayant la même image par la fonction  $\cos$ . Puisque la fonction  $\cos$  est à valeurs dans  $[-1; 1]$ , les différentes classes d'équivalence sont les ensembles de la forme  $\cos^{-1}(\{y\})$ , pour  $y \in [-1; 1]$ .

Pour une fonction  $f : E \rightarrow F$  quelconque, les classes d'équivalence sont les  $f^{-1}(\{y\})$ , pour  $y \in f(E)$ . Attention, si on prend  $y \in F$ , alors  $f^{-1}(\{y\})$  peut être vide, et dans ce cas ce n'est plus une classe d'équivalence.





On peut aisément généraliser à n'importe quelle fonction : voir ci-dessus et exercice 28.

- Pour la relation « avoir la même limite », les classes d'équivalence sont les ensembles de suites ayant la même limite. Par exemple, la classe d'équivalence des suites de limite nulle est :

$$\bar{0} = \left\{ (e^{-n})_{n \in \mathbb{N}} ; \left( \frac{1}{(n+1)} \right)_{n \in \mathbb{N}} ; (0)_{n \in \mathbb{N}} ; \dots \right\}$$



L'ensemble  $\bar{0}$  est très très gros !

On voit bien qu'à chaque fois, on a une partition de l'ensemble sous-jacent.

## IV Introduction aux ensembles quotients (HP)

On se donne dans toute cette partie un ensemble  $E$  muni d'une relation d'équivalence  $\sim$ . Il est temps d'aller au bout de l'idée sous-jacente à la notion de classe d'équivalence, à savoir : des éléments équivalents ne comptent que pour un. L'idée est donc de s'intéresser uniquement aux classes d'équivalence : une classe d'équivalence étant un seul ensemble, il suffit de s'intéresser à l'ensemble des classes d'équivalence, une classe d'équivalence ne comptera alors que pour un seul élément.

### IV.1 Définition et premiers exemples

**Définition.** On appelle ensemble quotient de  $E$  par  $\sim$  l'ensemble des classes d'équivalence pour la relation  $\sim$ . On le note  $E/\sim$ .

**Remarques :**

- $E/\sim$  est un sous-ensemble de  $\mathcal{P}(E)$  : il est formé uniquement des parties de  $E$  qui sont des classes d'équivalences pour  $\sim$ .
- Les éléments de  $E/\sim$  sont les classes d'équivalences pour  $\sim$ , c'est-à-dire que, si on note  $\bar{x}$  la classe d'équivalence d'un élément  $x$  de  $E$ ,  $E/\sim$  est l'ensemble formé des éléments  $\bar{x}$ , où l'on impose que  $\bar{x} = \bar{y}$  lorsque  $x \sim y$ .



C'est la même idée que dans  $\mathcal{P}(E)$  : les parties de  $E$  sont les éléments de  $\mathcal{P}(E)$ , elles **appartiennent** à  $\mathcal{P}(E)$ , les parties de  $E$  sont des **points** dans  $\mathcal{P}(E)$ , cf. chapitre 4.

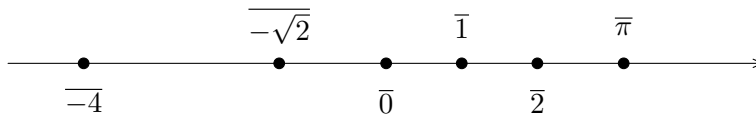


En d'autres termes,  $E/\sim = \{\bar{x} \mid x \in E\}$ .

**Exemples :**

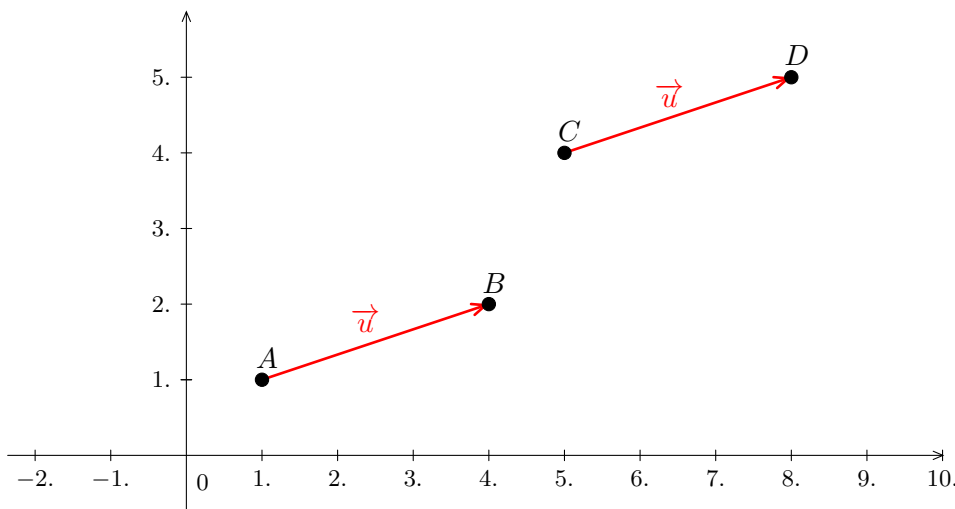
- Si on prend  $\sim$  la relation de congruence modulo 4 sur  $\mathbb{Z}$ , alors l'ensemble quotient associé est l'ensemble à quatre éléments  $\{\bar{0}; \bar{1}; \bar{2}; \bar{3}\}$ . Nous en parlerons plus longuement dans le paragraphe IV.2.

- On prend comme relation d'équivalence la relation « avoir la même limite » sur l'ensemble  $E$  des suites convergentes, alors  $E/\sim$  est l'ensemble formé des classes  $\bar{u}$ , où  $u$  est une suite convergente. Finalement, cela donne l'ensemble des suites qui convergent vers 0, l'ensemble des suites qui convergent vers 1, l'ensemble des suites qui convergent vers  $\pi$  etc. Si  $L \in \mathbb{R}$ , on peut aussi noter  $\bar{L}$  la classe d'équivalence des suites qui convergent vers  $L$ .  $E/\sim$  est donc l'ensemble contenant  $\bar{0}, \bar{1}, \bar{\sqrt{2}}, \bar{-1}$  etc. et plus généralement tous les  $\bar{L}$ . On peut donc représenter cet ensemble sous la forme d'une droite :



Terminons par deux exemples d'ensembles quotient que vous manipulez depuis des années :

- Si on prend  $\sim$  la relation d'équivalence sur les couples de points, on note  $\overrightarrow{AB}$  la classe d'équivalence d'un bipoint  $(A, B)$  et on l'appelle le vecteur  $\overrightarrow{AB}$  : si  $(A, B) \sim (C, D)$  alors  $\overrightarrow{AB} = \overrightarrow{CD}$ . Deux couples de points équivalents définissent une seule classe d'équivalence, c'est-à-dire **un seul vecteur** : c'est pour cela qu'on dit que, même lorsqu'il est à deux endroits différents, cela ne fait qu'un seul vecteur ! C'est parce que deux couples de points équivalents définissent une seule classe d'équivalence, un seul vecteur !



- Si on prend  $\equiv_{\mathbb{Q}}$  la relation d'équivalence sur  $\mathbb{Z} \times \mathbb{Z}^*$  vue plus haut, on note  $\frac{p}{q}$  la classe d'équivalence d'un couple  $(p, q)$  et on l'appelle le rationnel  $\frac{p}{q}$  : si  $(p_1, q_1) \equiv_{\mathbb{Q}} (p_2, q_2)$  alors  $\frac{p_1}{q_1} = \frac{p_2}{q_2}$ . Deux couples d'entiers équivalents définissent une seule classe d'équivalence, c'est-à-dire **un seul rationnel** : c'est comme cela qu'on définit  $\mathbb{Q}$  !

On voit que les ensembles quotient permettent de définir des ensembles intéressants, mais ils ne seront intéressants que si l'on définit des opérations sur ces ensembles : une somme de vecteurs, une somme de rationnels, un produit de rationnels etc. et si ces lois sont intéressantes i.e. vérifient certaines propriétés. On se pose donc la question suivante (qui est la base de l'algèbre) : peut-on munir un ensemble quotient de lois « intéressantes » ? Contentons-nous d'un exemple fondamental, au programme de deuxième année.

Cette représentation graphique laisse penser que l'ensemble des classes d'équivalence « ressemble à  $\mathbb{R}$  ». On peut aisément montrer que l'application  $\bar{L} \mapsto L$  est une bijection de  $E/\sim$  dans  $\mathbb{R}$ . D'où un des intérêts des ensembles quotient : l'application  $(u_n)_{n \in \mathbb{N}} \mapsto \lim u_n$  n'est pas injective de  $E$  dans  $\mathbb{R}$ , mais si on identifie les suites ayant les mêmes limites en les considérant comme une seule suite, c'est-à-dire en s'intéressant uniquement à leur classe d'équivalence, cela « devient » une bijection, mais là, ça devient furieusement hors programme...

C'est également comme cela qu'on construit  $\mathbb{K}(X)$  (cf. chapitre 20) et plus généralement le corps des fractions d'un anneau intègre (cf. chapitre 18).

## IV.2 $\mathbb{Z}/n\mathbb{Z}$ (deuxième année)

Dans tout ce paragraphe, on se donne un entier  $n$  supérieur ou égal à 2.

**Définition.** On note  $\mathbb{Z}/n\mathbb{Z}$  l'ensemble des classes d'équivalence de la congruence modulo  $n$  sur  $\mathbb{Z}$ .

**Remarque :** On pourrait prendre  $n = 1$ , mais alors tous les entiers sont congrus l'un à l'autre modulo  $n$ , et dans ce cas il n'y a qu'une classe d'équivalence, et donc  $\mathbb{Z}/n\mathbb{Z}$  n'a qu'un élément, ce qui en fait un ensemble avec peu d'intérêt...

**Exemples :**

$$\bullet \mathbb{Z}/2\mathbb{Z} = \{\bar{0}; \bar{1}\}. \quad \bullet \mathbb{Z}/3\mathbb{Z} = \{\bar{0}; \bar{1}; \bar{2}\}. \quad \bullet \mathbb{Z}/4\mathbb{Z} = \{\bar{0}; \bar{1}; \bar{2}; \bar{3}\}.$$

Plus généralement :

**Proposition.**  $\mathbb{Z}/n\mathbb{Z}$  est un ensemble à  $n$  éléments. Plus précisément :

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

DÉMONSTRATION. Soient  $p$  et  $q$  deux éléments distincts de  $\llbracket 0; n-1 \rrbracket$ . Alors  $p \not\equiv q [n]$ . Par conséquent, les classes d'équivalence  $\bar{p}$  et  $\bar{q}$  sont distinctes, c'est-à-dire que les classes d'équivalence  $\bar{0}, \dots, \overline{n-1}$  sont deux à deux distinctes. De plus, si  $p \in \mathbb{Z}$ , alors, d'après le théorème de la division euclidienne, il existe  $r \in \llbracket 0; n-1 \rrbracket$  tel que  $p \equiv r [n]$  et donc  $\bar{p} = \bar{r}$ . En conclusion : les classes d'équivalence ci-dessus sont les seules classes d'équivalences, et elles sont deux à deux distinctes, d'où le résultat.

**Remarque :** Détaillons un peu l'égalité  $\bar{p} = \bar{r}$  ci-dessus. L'égalité dans  $\mathbb{Z}/n\mathbb{Z}$  est l'analogue de la congruence modulo  $n$  dans  $\mathbb{Z}$ . Plus précisément, dans  $\mathbb{Z}/n\mathbb{Z}$ ,  $\bar{x} = \bar{y}$  si et seulement si, dans  $\mathbb{Z}$ ,  $x \equiv y [n]$  :  $\bar{x}$  et  $\bar{y}$  sont deux classes d'équivalence pour la relation de congruence modulo  $n$ , et donc les classes sont égales si et seulement si  $x$  et  $y$  sont équivalents i.e. congrus l'un à l'autre modulo  $n$ .

**Remarque :** On rappelle que  $\bar{0}$  est la classe d'équivalence de 0 c'est-à-dire l'ensemble des entiers congrus à 0 modulo  $n$ . Or,  $n \equiv 0 [n]$  donc  $\bar{n} = \bar{0}$ , c'est-à-dire que c'est la même classe d'équivalence, donc le même élément de  $\mathbb{Z}/n\mathbb{Z}$ . De même,  $\overline{n+1} = \bar{1}$  etc. Par conséquent,  $\bar{n}$  et  $\overline{n+1}$  appartiennent aussi à  $\mathbb{Z}/n\mathbb{Z}$ , ce n'est que par convention qu'on écrit

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

On pourrait très bien écrire :

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{n}; \bar{1}; \bar{2}; \dots; \overline{n-1}\}$$

ou (rappelons que dans l'écriture d'un ensemble avec des accolades, il n'y a pas d'ordre) :

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{1}; \bar{2}; \dots; \overline{n-1}; \bar{n}\}$$

Bref, la façon dont on les note importe peu : c'est l'ensemble des  $n$  classes d'équivalence modulo  $n$ . L'important est ce qu'on peut faire avec ça, et les lois qu'on peut définir sur cet ensemble.

**Définition.** On définit une addition, notée  $+$ , et un produit, noté  $\times$ , sur  $\mathbb{Z}/n\mathbb{Z}$ , par :

$$\forall (\bar{x}, \bar{y}) \in (\mathbb{Z}/n\mathbb{Z})^2, \quad \bar{x} + \bar{y} = \overline{x+y} \quad \text{et} \quad \bar{x} \times \bar{y} = \overline{x \times y}$$

En d'autres termes, si on note  $\equiv_n$  la relation congruence modulo  $n$  sur  $\mathbb{Z}$ , alors  $\mathbb{Z}/n\mathbb{Z}$  est l'ensemble quotient  $\mathbb{Z}/\equiv_n$ . Nous expliquerons la notation  $\mathbb{Z}/n\mathbb{Z}$  au chapitre 18.

Vous manipulez des ensembles du type  $\mathbb{Z}/n\mathbb{Z}$  depuis toujours : donner l'heure, ce n'est jamais que travailler dans  $\mathbb{Z}/24\mathbb{Z}$  (seule compte l'heure, pas la date), et donner le jour de la semaine, ce n'est jamais que travailler dans  $\mathbb{Z}/7\mathbb{Z}$  (seul compte le jour de la semaine, pas la date ou le mois).

Il ne viendrait à l'esprit de personne de confondre la notation  $\bar{0}$ , qui est la classe d'équivalence de 0, avec la notation  $\overline{0}$ , le conjugué complexe de 0...

Par exemple, si on travaille modulo 2, alors  $\bar{1} = \overline{-1}$  (car  $-1 \equiv 1 [2]$ ) et, si on travaille modulo 3, alors  $\bar{2} = \overline{-1}$  (car  $-1 \equiv 2 [3]$ ), donc pourrait écrire que  $\mathbb{Z}/2\mathbb{Z} = \{\bar{0}; \overline{-1}\}$  et  $\mathbb{Z}/3\mathbb{Z} = \{\overline{-1}; \bar{0}; \bar{1}\}$ .

**Remarque :** Il faut bien comprendre que les deux lois  $+$  ci-dessus (ainsi que les deux produits) ne sont pas la même loi (même si on les note de la même façon) et qu'on ne somme pas les mêmes objets. Plus précisément :

$$\overline{x} \quad \underbrace{+}_{\text{somme sur } \mathbb{Z}/n\mathbb{Z}} \quad \overline{y} = \overline{x + y} \quad \text{et} \quad \overline{x} \quad \underbrace{\times}_{\text{produit sur } \mathbb{Z}/n\mathbb{Z}} \quad \overline{y} = \overline{x \times y}$$

L'échec de type n'est pas loin...

Comme on l'a déjà vu, définir des opérations sur des ensembles est la base de l'algèbre. Cette année, nous avons appris à sommer et à multiplier des fonctions et des suites (alors qu'au début de l'année, nous ne savions sommer que des réels), et là nous définissons la somme et le produit de deux classes d'équivalence.

**Exemple :**  $\overline{2} + \overline{3} = \overline{5}$  et  $\overline{2} \times \overline{3} = \overline{6}$ .

**Proposition.** Les lois  $+$  et  $\times$  sont bien définies.

**Remarque :** En d'autres termes, le résultat ne dépend pas des entiers  $x$  et  $y$ . Expliquons un peu pourquoi il pourrait y avoir un problème (avant de démontrer qu'il n'y en a pas).

L'idée générale est que si  $a = c$  et  $b = d$ , alors on doit avoir  $a + b = c + d$ , sinon l'addition n'a pas de sens.

Cela a l'air évident, mais ici, il y a des choses à vérifier. Par exemple, dans  $\mathbb{Z}/4\mathbb{Z}$ ,  $\overline{1} = \overline{5}$  et  $\overline{2} = \overline{6}$  donc on doit avoir  $\overline{1} + \overline{2} = \overline{5} + \overline{6}$  : ce n'est a priori pas évident, mais il faut absolument avoir égalité sinon l'addition n'a pas de sens, car la définition d'une loi ne doit pas dépendre de la façon de noter le même objet (et ces deux sommes sont simplement deux façons d'écrire la somme des deux mêmes éléments). De la même façon (toujours dans  $\mathbb{Z}/4\mathbb{Z}$ ), a-t-on bien  $\overline{1} \times \overline{2} = \overline{5} \times \overline{6}$  ? Tout va bien car, quand on travaille modulo 4, alors on a bien  $\overline{3} = \overline{11}$  et  $\overline{2} = \overline{30}$ , mais on voit maintenant qu'il y a quelque-chose à montrer.

DÉMONSTRATION. Soit  $(x_1, x_2) \in \mathbb{Z}^2$  tels que  $\overline{x_1} = \overline{x_2}$ , et soit  $(y_1, y_2) \in \mathbb{Z}^2$  tels que  $\overline{y_1} = \overline{y_2}$ . Montrons que  $\overline{x_1 + y_1} = \overline{x_2 + y_2}$  et que  $\overline{x_1 \times y_1} = \overline{x_2 \times y_2}$ .

$\overline{x_1} = \overline{x_2}$  donc  $x_1 \equiv x_2 [n]$  et  $\overline{y_1} = \overline{y_2}$  donc  $y_1 \equiv y_2 [n]$ . Par conséquent,  $x_1 + y_1 \equiv x_2 + y_2 [n]$  et  $x_1 \times y_1 \equiv x_2 \times y_2 [n]$  (cf. chapitre 6), d'où les égalités demandées.

**Remarque :** L'idée (très simple !) qui se cache derrière cette définition et toutes ces barres horizontales est très simple : si on somme un nombre congru à  $x$  modulo  $n$  et un nombre congru à  $y$  modulo  $n$ , cela donne un nombre congru à  $x + y$  modulo  $n$ , et idem pour le produit. Cependant, pour que cela ait du sens, il faut vérifier que cela ne dépend pas de l'élément choisi, que tous les éléments donneront le même résultat, et c'est précisément ce que nous venons de montrer. Seulement, au lieu de définir l'addition (et le produit) sur  $\mathbb{Z}$ , c'est-à-dire la définir pour chaque élément de  $\mathbb{Z}$ , on la définit pour chaque classe d'équivalence ou, ce qui revient au même, pour tous les éléments de la classe d'équivalence en même temps comme s'ils n'étaient qu'un seul élément, et on peut le faire car on vient de prouver qu'ils donneront le même résultat.

C'est l'idée générale des lois sur les ensembles quotients : on définit des lois (ou des fonctions) sur les classes d'équivalence, mais pour que cela ait du sens, il faut que tous les éléments de la classe d'équivalence donnent le même résultat. Par exemple, si on reprend l'exemple des suites convergentes et de la relation d'équivalence « avoir la même limite », cela aurait du sens (voir ci-dessus) de définir la fonction

$$\begin{cases} E/\sim & \rightarrow & \mathbb{R} \\ \overline{u} & \mapsto & \lim u \end{cases}$$

car toutes les suites d'une même classe d'équivalence ont la même limite, mais cela n'aurait pas de sens de définir la fonction

Cela prouvera que la définition de la somme et du produit ne dépend pas des éléments choisis dans la classe d'équivalence, voir la remarque précédente. En d'autres termes : on montre que, peu importe la façon dont on note les deux mêmes objets, la valeur de leur somme ne varie pas (ce qui prouve donc que la somme est bien définie), et idem pour le produit.

$$\begin{cases} E/\sim & \rightarrow \mathbb{R} \\ \bar{u} & \mapsto u_0 \end{cases}$$

car deux suites équivalentes n'ont pas forcément le même premier terme. Par exemple, si on note  $u$  la suite nulle et  $v$  la suite de terme général  $e^{-n}$ , alors  $\bar{u} = \bar{v}$ , mais  $f(\bar{u}) = 0$  tandis que  $f(\bar{v}) = 1$  :  $f$  donne (au moins) deux images différentes pour le même élément, ce qui n'est pas possible pour une fonction, c'est-à-dire que  $f$  n'est pas bien définie.

Donnons un exemple plus prosaïque : si on prend  $E$  l'ensemble des élèves du lycée Faidherbe, et  $\sim$  la relation « être dans la même classe », alors c'est une relation d'équivalence, et les classes d'équivalence sont les différentes classes. On peut définir la fonction

$$\begin{cases} E/\sim & \rightarrow \{\text{professeurs}\} \\ \overline{\text{élève}} & \mapsto \text{professeur de maths de l'élève} \end{cases}$$

alors cela a du sens, alors que la fonction

$$\begin{cases} E/\sim & \rightarrow \{\text{couleurs}\} \\ \overline{\text{élève}} & \mapsto \text{couleur des yeux de l'élève} \end{cases}$$

ne l'est pas.

En conclusion, les éléments d'une même classe d'équivalence ne comptent que pour un seul « quand on s'intéresse à leur caractéristique commune », c'est-à-dire à la relation d'équivalence sous-jacente, mais il ne faut pas s'intéresser à autre chose.

Si l'on revient à  $\mathbb{Z}/n\mathbb{Z}$ , alors les éléments congrus l'un à l'autre modulo  $n$  représentent la même classe d'équivalence mais, si on veut définir des lois, des fonctions sur  $\mathbb{Z}/n\mathbb{Z}$ , il faut vérifier que ces lois, ces fonctions sont compatibles avec la congruence modulo  $n$ , c'est-à-dire que des nombres congrus l'un à l'autre modulo  $n$  renverront le même résultat.

Bref, tout va bien pour l'addition et la multiplication ci-dessus. Revenons à des choses plus simples.

**Proposition.** Sur  $\mathbb{Z}/n\mathbb{Z}$  :

- la somme et le produit sont commutatifs, c'est-à-dire :

$$\forall(\bar{x}, \bar{y}) \in (\mathbb{Z}/n\mathbb{Z})^2, \bar{x} + \bar{y} = \bar{y} + \bar{x} \text{ et } \bar{x} \times \bar{y} = \bar{y} \times \bar{x}$$

- la somme et le produit sont associatifs, c'est-à-dire :

$$\forall(\bar{x}, \bar{y}, \bar{z}) \in (\mathbb{Z}/n\mathbb{Z})^3, (\bar{x} + \bar{y}) + \bar{z} = \bar{x} + (\bar{y} + \bar{z})$$

et idem pour le produit.

- le produit est distributif par rapport à la somme, c'est-à-dire :

$$\forall(\bar{x}, \bar{y}, \bar{z}) \in (\mathbb{Z}/n\mathbb{Z})^3, (\bar{x} + \bar{y}) \times \bar{z} = \bar{x} \times \bar{z} + \bar{y} \times \bar{z}$$

- $\bar{0}$  est l'élément neutre pour l'addition et  $\bar{1}$  est le neutre pour le produit, c'est-à-dire :

$$\forall \bar{x} \in \mathbb{Z}/n\mathbb{Z}, \bar{0} + \bar{x} = \bar{x} \text{ et } \bar{1} \times \bar{x} = \bar{x}$$

On peut donc se passer de parenthèses quand on écrira (par exemple)  $\bar{1} + \bar{2} + \bar{3} = \bar{6}$ .

Pour les deux dernières, c'est aussi valable de l'autre côté par commutativité.

DÉMONSTRATION. Soit  $(\bar{x}, \bar{y}) \in (\mathbb{Z}/n\mathbb{Z})^2$ . Alors :

$$\begin{aligned}\bar{x} + \bar{y} &= \overline{x + y} \\ &= \overline{y + x} \\ &= \bar{y} + \bar{x}\end{aligned}$$

□

Car  $x + y = y + x$  puisque la somme sur  $\mathbb{Z}$  est commutative.

Le reste : exo.

**Définition.** Soit  $\bar{x} \in \mathbb{Z}/n\mathbb{Z}$ . On pose  $-\bar{x} = \overline{-x}$  et, si  $y \in \mathbb{Z}/n\mathbb{Z}$ , on pose  $\bar{y} - \bar{x} = \bar{y} + \overline{-x}$ .

**Remarque :** Là aussi, cette notation est bien définie, c'est-à-dire que si  $\bar{x} = \bar{y}$ , alors  $x \equiv y [n]$  donc  $-x \equiv -y [-n]$ , c'est-à-dire qu'il existe  $k \in \mathbb{Z}$  tel que  $-x = -y + k \times (-n) = -y + (-k) \times n$ . En d'autres termes,  $-x \equiv -y [n]$  i.e.  $\overline{-x} = \overline{-y}$  : la définition ne dépend pas de l'élément choisi, donc tout va bien.

**Remarque :** Si  $\bar{x} \neq \bar{0}$ , on aimerait définir  $\bar{x}^{-1}$ , l'inverse de  $\bar{x}$  comme l'élément  $\bar{y}$  tel que  $\bar{x} \times \bar{y} = \bar{1}$ , sauf que celui-ci n'existe pas forcément ! Par exemple, dans  $\mathbb{Z}/4\mathbb{Z}$ , il n'existe pas d'élément  $\bar{y}$  tel que  $\bar{2} \times \bar{y} = \bar{1}$  car il n'existe pas d'entier  $y$  tel que  $2y \equiv 1 [4]$  (rappelons que l'égalité dans  $\mathbb{Z}/n\mathbb{Z}$  est la même chose que la congruence modulo  $n$ ). En d'autres termes, tous les éléments non nuls de  $\mathbb{Z}/n\mathbb{Z}$  ne sont pas forcément inversibles. Nous dirons dans le chapitre 18 que  $\mathbb{Z}/n\mathbb{Z}$  est un anneau, mais pas forcément un corps. Nous verrons dans l'exercice 2 et dans le chapitre 18 que  $\bar{x}$  est inversible dans  $\mathbb{Z}/n\mathbb{Z}$  si et seulement si  $x$  est premier avec  $n$ .

Ne pas oublier qu'on travaille modulo  $n$  ! Par exemple, si on travaille dans  $\mathbb{Z}/5\mathbb{Z}$ , alors  $-\bar{2} = \bar{-2} = \bar{3}$ .

On ne peut évidemment pas définir  $\bar{x}^{-1}$  en posant  $\bar{x}^{-1} = \overline{x^{-1}}$  ou  $\overline{1/x}$  car  $1/x$  n'est pas un entier, et on travaille ici avec des classes d'équivalence sur  $\mathbb{Z}$ .

Ci-dessous les tables de l'addition de  $\mathbb{Z}/2\mathbb{Z}$ ,  $\mathbb{Z}/3\mathbb{Z}$  et  $\mathbb{Z}/4\mathbb{Z}$  :

+	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

$\mathbb{Z}/2\mathbb{Z}$

+	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

$\mathbb{Z}/3\mathbb{Z}$

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

$\mathbb{Z}/4\mathbb{Z}$

**Remarque :**  $\mathbb{Z}/2\mathbb{Z}$  et plus généralement  $(\mathbb{Z}/2\mathbb{Z})^n$  (i.e. l'ensemble de  $n$ -uplets d'éléments de  $\mathbb{Z}/2\mathbb{Z}$ ) sont des ensembles importants en informatique car on travaille beaucoup en binaire. Par exemple, on écrit souvent que  $\bar{1} + \bar{1} = \bar{0}$ , ce qui est exactement sommer dans  $\mathbb{Z}/2\mathbb{Z}$  !

Ci-dessous les tables du produit de  $\mathbb{Z}/2\mathbb{Z}$ ,  $\mathbb{Z}/3\mathbb{Z}$  et  $\mathbb{Z}/4\mathbb{Z}$  :

$\times$	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$

$\mathbb{Z}/2\mathbb{Z}$

$\times$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{1}$

$\mathbb{Z}/3\mathbb{Z}$

$\times$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$


$\mathbb{Z}/4\mathbb{Z}$

Tous les tableaux sont symétriques. C'est normal : les lois sont commutatives !



## Remarques :

- En clair, le produit et la somme vérifient les mêmes propriétés que sur  $\mathbb{R}$ , mais il ne faut pas oublier qu'on travaille modulo  $n$ . Par exemple, dans  $\mathbb{Z}/20\mathbb{Z}$ ,  $\bar{8} \times \bar{4} = \bar{12}$ ,  $\bar{3} \times \bar{7} = \bar{1}$  et  $\bar{5} \times \bar{4} = \bar{0}$ .

-  Dès qu'on s'approche de près ou de loin de la division, ce n'est plus du tout le cas !

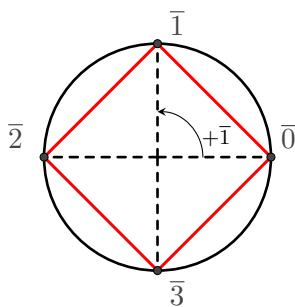
★ Tout élément (même non nul) n'admet pas forcément d'inverse, c'est-à-dire que si  $\bar{x} \in \mathbb{Z}/n\mathbb{Z}$ , alors il n'existe pas forcément d'élément  $\bar{y} \in \mathbb{Z}/n\mathbb{Z}$  tel que  $\bar{x} \times \bar{y} = \bar{1}$  (cf. exercice 2).

★ Par conséquent, on ne peut pas simplifier par un élément, même non nul ! Par exemple, dans  $\mathbb{Z}/10\mathbb{Z}$ ,  $\bar{4} \times \bar{5} = \bar{6} \times \bar{5} = \bar{0}$  mais on n'a pas  $\bar{4} = \bar{6}$  ! Ne jamais oublier que diviser ou simplifier, c'est multiplier par l'inverse : quand il n'y a pas d'inverse, on ne peut pas simplifier !

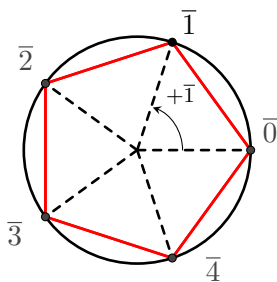
★  $\bar{0}$  est absorbant, c'est-à-dire que :  $\forall \bar{x} \in \mathbb{Z}/n\mathbb{Z}, \bar{0} \times \bar{x} = \bar{0}$ , mais on vient de voir que la réciproque est fausse, c'est-à-dire qu'on peut avoir  $\bar{x} \times \bar{y} = \bar{0}$  avec  $\bar{x}$  et  $\bar{y}$  différents de  $\bar{0}$ . Ainsi, il est faux de dire que : « un produit de facteurs est nul si et seulement si l'un au moins des facteurs est nul ». De toute façon, il suffit de se souvenir que cela vient du fait qu'on peut simplifier par un élément non nul : en effet, si  $xy = 0$  et si  $x \neq 0$ , alors on peut multiplier par  $1/x$  pour obtenir  $y = 0$ , et puisqu'on ne peut pas simplifier dans  $\mathbb{Z}/n\mathbb{Z}$ , alors ce n'est plus valable.

- On a  $\bar{n} = \underbrace{\bar{1} + \dots + \bar{1}}_{n \text{ fois}} = \bar{0}$ , et si on ajoute encore  $\bar{1}$ , alors on retombe sur  $\bar{1}$ , c'est-à-dire que  $\overline{n+1} = \bar{1}$ , puis  $\overline{n+2} = \bar{2}$ , et ainsi de suite jusqu'à avoir de nouveau  $\overline{2n} = \bar{0}$  et ainsi de suite.

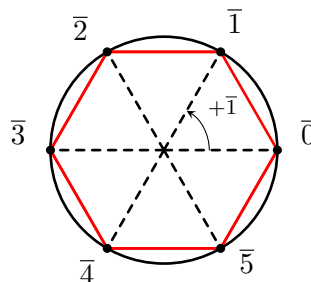
On dit que  $\mathbb{Z}/n\mathbb{Z}$  est cyclique. C'est normal : on travaille modulo  $n$  ! On peut résumer ça par : « quand on ajoute un multiple de  $n$ , on fait des tours donc on se retrouve au même endroit ». Par conséquent, on représente en général  $\mathbb{Z}/n\mathbb{Z}$  comme des éléments sur un cercle comme ci-dessous :



$\mathbb{Z}/4\mathbb{Z}$



$\mathbb{Z}/5\mathbb{Z}$



$\mathbb{Z}/6\mathbb{Z}$

Vu sous cette forme,  $\mathbb{Z}/n\mathbb{Z}$  ressemble à l'ensemble  $\mathbb{U}_n$  : nous montrerons au chapitre 18 qu'il y a un lien très fort entre ces deux ensembles. Attention, cela ne signifie pas que les éléments de  $\mathbb{Z}/n\mathbb{Z}$  soient des racines de l'unité ou même des complexes avec une partie réelle ou une partie imaginaire, ni que  $\mathbb{Z}/n\mathbb{Z}$  soit une partie du plan ou de  $\mathbb{C}$  : les éléments de  $\mathbb{Z}/n\mathbb{Z}$  sont des classes d'équivalence, c'est-à-dire des ensembles, ceci n'est qu'une façon pratique de les représenter pour mieux visualiser  $\mathbb{Z}/n\mathbb{Z}$  et mieux se familiariser avec les lois  $+$  et  $\times$ .

Alors qu'on peut simplifier sans scrupule pour la somme ! En effet, si  $\bar{x} + \bar{y} = \bar{x} + \bar{z}$ , alors, en ajoutant  $-\bar{x}$  des deux côtés, et par associativité, il vient :

$$-\bar{x} + \bar{x} + \bar{y} = -\bar{x} + \bar{x} + \bar{z}$$

donc  $\bar{0} + \bar{y} = \bar{0} + \bar{z}$  donc  $\bar{y} = \bar{z}$  : pour la somme et le produit, on travaille comme sur  $\mathbb{R}$ , c'est quand on veut diviser ou simplifier que les problèmes se posent.

Nous définirons la notion de groupe cyclique dans le chapitre 18.

Cette représentation en cercle n'aurait pas été adaptée, par exemple, aux classes d'équivalence de la relation « avoir la même limite » sur l'ensemble des suites convergentes : pour celle-ci, la représentation en droite est beaucoup plus adaptée (cf. paragraphe IV.1).