

## Corps

|                   |                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Définition</b> | Soit $(A, +, *)$ un anneau. $A$ est appelé un <b>corps</b> lorsque tous les éléments de $A$ non nuls sont inversibles pour la multiplication.                                                                                                                                                                                                                                                            |
| <b>Exemples</b>   | <ul style="list-style-type: none"> <li><math>(\mathbb{Q}, +, *)</math>, <math>(\mathbb{R}, +, *)</math>, <math>(\mathbb{C}, +, *)</math> sont des corps.</li> <li>Par contre <math>(\mathbb{Z}, +, *)</math> est un anneau mais pas un corps. En effet les éléments non nuls de <math>\mathbb{Z}</math> (à part 1 et <math>-1</math>) ne sont pas inversibles dans <math>\mathbb{Z}^*</math>.</li> </ul> |
| <b>Propriétés</b> | <ol style="list-style-type: none"> <li>L'ensemble <math>(\mathbb{Z}/5\mathbb{Z}, +, *)</math> est un corps</li> <li>L'ensemble <math>F = \{a + b\sqrt{2}, (a, b) \in \mathbb{Q}\}</math> est un corps.</li> </ol>                                                                                                                                                                                        |
| <b>Remarque</b>   | Tous les corps que nous étudierons cette année seront des corps commutatifs pour la multiplication.                                                                                                                                                                                                                                                                                                      |

## Preuve

- Nous savons déjà que  $(\mathbb{Z}/5\mathbb{Z}, +, *)$  est un anneau. (voire le chapitre sur les anneaux). Soit  $\dot{x}$  un élément non nul de  $\mathbb{Z}/5\mathbb{Z}$ .  $\dot{x} \in \{\dot{0}, \dot{1}, \dot{2}, \dot{3}, \dot{4}\}$  et soit  $x$  le représentant de  $\dot{x}$  dans  $\{0, 1, 2, 3, 4\}$   
 $5$  est un nombre premier et  $x < 5$  donc  $x \wedge 5 = 1$   
Le théorème de bezout dans sa forme générale nous donne l'existence de deux entiers relatifs  $u$  et  $v$  tels que  $x * u + 5 * v = 1 \Rightarrow x * u = 1 - 5 * v \Rightarrow x * u \equiv 1[5]$   
Soit  $\dot{u}$  la classe d'équivalence de  $u$  dans  $\mathbb{Z}/5\mathbb{Z}$ .  
Nous avons donc  $\dot{x} * \dot{u} = \dot{1}$ .  $\dot{x}$  est donc inversible dans  $\mathbb{Z}/5\mathbb{Z}$ . Son inverse est  $\dot{u}$
- L'ensemble  $F = \{a + b\sqrt{2}, (a, b) \in \mathbb{Q}^2\}$  est un corps.
  - $(F, +)$  est un groupe commutatif.  
 $+$  est une loi de composition interne commutative.  
 $+$  est associative.  
 $0 \in F$   
 $\forall x \in F, -x \in F$
  - $(F, +, *)$  est un anneau unitaire.  
 $(F, +)$  est un groupe commutatif.  
 $*$  est associative et distributive par rapport à l'addition.  
 $1 \in F$  et est l'élément neutre de la multiplication dans  $F$
  - $(F, +, *)$  est un corps.  
Soit  $x = a + b\sqrt{2}$ , un élément non nul de  $F$   
 $(a - b\sqrt{2})(a + b\sqrt{2}) = a^2 - 2b^2$   
Donc  $x^{-1} = \frac{a - b\sqrt{2}}{a^2 - 2b^2}$  est l'inverse de  $x$  dans  $F$ . (Remarquons que  $\frac{a}{a^2 - 2b^2}$  et  $\frac{-b}{a^2 - 2b^2}$  sont des éléments de  $\mathbb{Q}$  lorsque  $(a, b) \in \mathbb{Q}^2$ )