

La structure algébrique de corps

DÉFINITION

Structure algébrique de corps

Si $\mathbb{K}$ est un ensemble muni de deux lois de compositions internes $+$ et $\cdot$ telles que

- (1) $(\mathbb{K}, +)$ est un groupe commutatif d'élément neutre $0_{\mathbb{K}}$
- (2) $(\mathbb{K}^*, \cdot)$ est un groupe commutatif d'élément neutre $1_{\mathbb{K}}$ où $\mathbb{K}^* = \mathbb{K} - \{0_{\mathbb{K}}\}$
- (3) la loi $\cdot$ est distributive par rapport à $+$: $\forall (x, y, z) \in \mathbb{K}^3, x \cdot (y + z) = x \cdot y + x \cdot z$

alors on dit que $(\mathbb{K}, +, \cdot)$ est un corps commutatif.

Exemples :

- Considérons l'ensemble $\mathbb{Q}$ munis des deux lois de compositions internes $+$ et $\cdot$ usuelles.

- $(\mathbb{Q}, +)$ est bien un groupe commutatif d'élément neutre $\frac{0}{1}$ où l'opposé de $\frac{p}{q}$ est $\frac{-p}{q}$.
- $(\mathbb{Q}^*, \cdot)$ est un groupe commutatif d'élément neutre $\frac{1}{1}$ où l'inverse de $\frac{p}{q}$ est $\frac{q}{p}$
- La loi $\cdot$ est distributive par rapport à $+$ car :

$$\forall (p, q) \in \mathbb{Z} \times \mathbb{N}^*, \forall (p', q') \in \mathbb{Z} \times \mathbb{N}^*, \forall (p'', q'') \in \mathbb{Z} \times \mathbb{N}^*,$$

$$\frac{p}{q} \cdot \left(\frac{p'}{q'} + \frac{p''}{q''} \right) = \frac{p}{q} \cdot \left(\frac{p'q'' + p''q'}{q'q''} \right) = \frac{p(p'q'' + p''q')}{qq'q''} = \frac{pp'q''}{qq'q''} + \frac{pp''q'}{qq'q''} = \frac{pp'}{qq'} + \frac{pp''}{qq''} = \frac{p}{q} \cdot \frac{p'}{q'} + \frac{p}{q} \cdot \frac{p''}{q''}$$

On a donc justifié que $(\mathbb{Q}, +, \cdot)$ est un corps commutatif

- De même, les lois $+$ et $\cdot$ usuelles sur $\mathbb{R}$ font clairement de $(\mathbb{R}, +, \cdot)$ un corps commutatifs

- $(\mathbb{R}, +)$ est bien un groupe commutatif d'élément neutre 0 où l'opposé de a est $-a$
- $(\mathbb{R}^*, \cdot)$ est bien un groupe commutatif d'élément neutre 1 où l'inverse de a est $\frac{1}{a}$
- La loi $\cdot$ est bien distributive par rapport à $+$

- Considérons les lois usuelles $+$ et $\cdot$ sur $\mathbb{Z}$ alors :

- $(\mathbb{Z}, +)$ est bien un groupe commutatif d'élément neutre 0 où l'opposé de n est $-n$
- $(\mathbb{Z}^*, \cdot)$ n'est pas un groupe.

Il possède un élément neutre 1 mais les seuls éléments de $\mathbb{Z}^*$ possédant un inverse sont $+1$ et -1

En effet, par exemple, $2 \in \mathbb{Z}^*$ n'a pas d'inverse dans $\mathbb{Z}^*$ car l'équation $2 \cdot n = 1$ n'a pas de solution dans $\mathbb{Z}^*$...

$(\mathbb{Z}, +, \cdot)$ n'est pas un corps

- Considérons l'ensemble $\mathbb{R}^2$ munis des deux lois $+$ et $\cdot$ définies par :

$$\forall (a, b) \in \mathbb{R}^2, \forall (a', b') \in \mathbb{R}^2, (a, b) + (a', b') = (a + a', b + b') \quad \text{et} \quad (a, b) \cdot (a', b') = (aa' - bb', ab' + a'b)$$

- $(\mathbb{R}^2, +)$ est bien un groupe commutatif d'élément neutre $(0, 0)$ où l'opposé de (a, b) est $(-a, -b)$.
 - $(\mathbb{R}^2 - \{(0, 0)\}, \cdot)$ est un groupe commutatif d'élément neutre $(1, 0)$ où l'inverse de (a, b) est $\left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2} \right)$
 - La loi $\cdot$ est distributive par rapport à $+$ car : $\forall (a, b) \in \mathbb{R}^2, \forall (a', b') \in \mathbb{R}^2, \forall (a'', b'') \in \mathbb{R}^2$
- $$\begin{aligned} (a, b) \cdot ((a', b') + (a'', b'')) &= (a, b) \cdot (a' + a'', b' + b'') = (a(a' + a'') - b(b' + b''), a(b' + b'') + b(a' + a'')) \\ &= ((aa' - bb') + (aa'' - bb''), (ab' + ba') + (ab'' + ba'')) \\ &= (aa' - bb', ab' + ba') + (aa'' - bb'', ab'' + ba'') \\ &= (a, b) \cdot (a', b') + (a, b) \cdot (a'', b'') \end{aligned}$$

On a donc justifié que $(\mathbb{R}^2, +, \cdot)$ est un corps commutatif.

Mais, si on assimile le couple (a, b) au complexe $a + ib$ pour tout couple $(a, b) \in \mathbb{R}^2$ alors :

$$\forall (a, b) \in \mathbb{R}^2, \forall (a', b') \in \mathbb{R}^2,$$

$$(a, b) + (a', b') = (a + a', b + b') \quad \text{correspond à} \quad (a + ib) + (a' + ib') = (a + a') + i(b + b')$$

$$(a, b) \cdot (a', b') = (aa' - bb', ab' + a'b) \quad \text{correspond à} \quad (a + ib) \cdot (a' + ib') = (aa' - bb') + i(ab' + a'b)$$

Finalement, on a justifié que $(\mathbb{C}, +, \cdot)$ est un corps commutatif

Une "brève" histoire des nombres...

La construction de l'algèbre moderne est une longue histoire qui n'est ni linéaire, ni attachée à une seule civilisation. Elle n'est pas aussi "carré" que le laisse penser la présentation achevée actuelle.

On peut néanmoins essayer de l'observer avec un peu de recul à l'aide des structures algébriques déjà introduites.

Les nombres entiers naturels non nuls $1, 2, 3, \dots$ se sont "naturellement" imposés aux hommes car ils permettent de compter. La représentation de ces nombres et la façon de les utiliser varient beaucoup d'une civilisation à l'autre.

Des os prétaillés de la préhistoire (-35000 à -20000 ans) aux cailloux "calculi" du Proche-Orient (-9000 à -2000 ans) (laissant le mot "calcul"), des premières notions abstraites de nombre sumériennes (vers -3300 ans) et babyloniennes (vers -1900 ans) qui sont en base 60 (et qu'on retrouve dans les heures-minutes-secondes et les degrés-minutes-secondes (angles)) en passant par la numération en base 5 des gréco-romains (-1400 à -1200 ans) et la numérotation en base 20 des mayas (V^{ème} siècle) et des celtes (qu'on retrouve lorsqu'on compte entre 60 et 100...) jusqu'aux chiffres enfin en base 10 des égyptiens (-3000 ans) et des chinois (vers -800), le chemin jusqu'à nos chiffres arabes (VI^{ème} siècle) a été long...

Ces chiffres (qui sont en fait des chiffres indiens!) ne sont arrivés en occident qu'au X^{ème} siècle et ne se développeront qu'aux XII^{ème} siècle... On peut donc dire que la construction du concept nombre a été plus que difficile!

L'ensemble $\mathbb{N}^*$ dispose naturellement d'une loi de composition interne $+$ qui est associative et commutative
mais elle n'a pas d'élément neutre.

La création du zéro a été difficile car conceptuellement très innovante (c'est un très grand pas dans l'abstraction mathématiques) Les premières traces dates de -300 en Babylone et il a aussi été crée de façon autonome par les mayas (V^{ème} siècle) Mais c'est en Inde au V^{ème} siècle avec le savant Brahmagupta (598-660) qu'il est vraiment conceptualisé. Le symbole 0 y est crée. Le zéro n'arrive en occident qu'au XII^{ème} siècle où le mathématicien Fibonacci (1170-1250) lui donne le nom de "zefirum" devenu zéro.

L'ensemble $\mathbb{N}$ dispose d'une loi $+$ associative, commutative avec un élément neutre qui est 0
mais $(\mathbb{N}, +)$ n'est pas un groupe car il manque les opposés (càd les symétriques pour $+$)

L'arrivée des entiers négatifs est assez concrète. On raconte que les bergers utilisaient des cailloux pour dénombrer les moutons. Déposant dans un sac un caillou pour chaque mouton emmené dans les alpages, ils retiraient, au retour, un caillou par mouton rentré. S'il restait des cailloux, ils avaient "perdu" des moutons... Les premières représentations viennent de Chine (vers 220-280) pour des besoins de comptabilité marchande. Mais c'est Brahmagupta en Inde (encore lui!) qui conceptualise ces nombres. L'occident aura beaucoup de difficulté à les accepter. Bien qu'ils apparaissent dans les équations dès 1484 et que le calcul symbolique se développent durant tous le XVI^{ème} siècles (Création des symboles $+$ et $-$ en 1489 par l'allemand Eger, du $=$ en 1557 par l'anglais Record, des notations littérales pour les inconnues par le français Viète en 1591) Les nombres négatifs sont rejetés par de nombreux savants. Descartes (1596-1635) qualifie même de "moindres que rien" les solutions négatives de ses équations et il n'utilise que le quart de plan positif... C'est l'écossais Maclaurin (1698-1746) et le suisse Euler (1707-1783) qui utiliseront les premiers les repères actuels.

Voici construit le groupe abélien $(\mathbb{Z}, +)$

$\mathbb{Z}$ possède aussi une autre loi de composition interne $\times$ qui est associative, commutative et distributive par rapport à $+$ et qui possède un élément neutre 1. Mais $(\mathbb{Z}^*, \times)$ n'est pas un groupe car certains éléments de $\mathbb{Z}^*$ n'ont pas d'inverse!

$(\mathbb{Z}, +, \cdot)$ n'est donc pas un corps mais on dit que $(\mathbb{Z}, +, \times)$ est un anneau commutatif

Les premières fractions apparaissent en Egypte entre -3000 et -2000. Mais, elles seront surtout développées par les grecs car ils pensent que tous les nombres sont des rapports de longueurs (concept de nombre rationnel positif) (Pour Archimède (-287, -212), π vaut $\frac{223}{71}$ par exemple...) La barre de fractions est un héritage des arabes au X^{ème} siècle et les nombres rompus appelés "fractiones" n'arriveront en occident là encore qu'au XII^{ème} siècle.

Les prolongements de $+$ et $\times$ de $\mathbb{Z} \times \mathbb{Z}$ à $\mathbb{Q} \times \mathbb{Q}$ sont construits pour que $(\mathbb{Q}, +)$ et $(\mathbb{Q}^*, \times)$ soient des groupes et aussi pour que $\times$ soit distributive par rapport à $+$ (d'où la fameuse loi d'addition des fractions qui fait tant souffrir les collégiens...) :

$(\mathbb{Q}, +, \times)$ est alors un corps commutatif

La civilisation babylonienne (-4000) découvrent la première les irrationnels (notamment $\sqrt{2}$) mais c'est les grecs qui créeront le concept de nombre "irrationnel" car ils ne les comprennent pas "en rapport de longueur". Il faudra attendre la fin du XIX^{ème} siècle pour qu'irrationnels et rationnels soient réunis dans le corps des réels par le mathématicien allemand Richard Dedekind (1831-1916). Ces nombres sont "réels" car ils représentent des quantités réels (la longueur de la diagonale d'un carré de côté 1 pour $\sqrt{2}$, le périmètre d'un cercle de diamètre 1 pour π , etc) par opposition aux nombres complexes qui sont créés par les italiens Cardan et Tartaglia au XVI^{ème} siècle à partir des équations du troisième degré.

Les prolongements de $+$ et $\times$ de $\mathbb{Q} \times \mathbb{Q}$ à $\mathbb{R} \times \mathbb{R}$ sont naturels et font de $(\mathbb{R}, +, \times)$ un corps commutatif

Les lois $+$ et $\times$ que l'on a construite sur l'ensemble $\mathbb{C}$ des complexes respectent la structure algébrique de corps.

$(\mathbb{R}, +, \times)$ et $(\mathbb{C}, +, \times)$ sont des corps commutatifs