corps, n. m.

Us.: Le sens premier est biologique : ensemble matériel organisé qui assure l'identité d'un être du règne animal au cours de sa vie (et même, par extension, après sa mort, aussi longtemps que son aspect extérieur reste reconnaissable). Il s'étend à la sociologie pour désigner un ensemble de personnes, toujours avec une idée d'organisation, soit générale (corps social), soit spéciale (corps des sapeurs-pompiers, corps des inspecteurs généraux, corps diplomatique, etc.); il peut même prendre en philosophie ou en science un sens abstrait : ensemble d'idées, de thèses, en général clos, aussi exhaustif et cohérent que possible (corps de doctrine).

Math.: L'idée d'ensemble matériel prévaut en physique; la mécanique y ajoute en général celle de rigidité, au moins approchée; celle de rigidité parfaite dominait en géométrie (jadis on disait les « corps platoniciens » pour les cinq polyèdres réguliers, les « corps ronds » pour la sphère, le cylindre, etc, aujourd'hui on dit plutôt *solides*). Mais c'est l'idée d'organisation qui prévaut dans l'emploi algébrique étudié ci-après; dans ce dernier sens on a dit *champ* qui est resté dans « champ de Galois » et dans l'anglais *field*, mais c'est la terminologie allemande *Körper* (Dirichlet, Dedekind) à laquelle l'usage français s'est rallié.

1. Corps.

1.1. *Structure de corps.* Soit un ensemble K muni de deux lois internes :

$(x, y) \mapsto x+y$ (addition dans K)

$(x, y) \mapsto x \,.\, y$ (multiplication dans K; dans de nombreux cas, $x.y$ se note aussi $x \times y$, ou même, plus couramment, xy lorsqu'il n'y a aucun risque de confusion).

Le triplet (K, +, .) est un corps si et seulement si :

a) (K, +) est un groupe commutatif (l'élément neutre en est usuellement noté 0);

b) la multiplication est associative, elle possède un élément neutre, différent de 0, noté généralement 1 ou *e*, et de plus tout élément non nul a un inverse;

c) la multiplication est distributive par rapport à l'addition à droite et à gauche.

Cette définition équivaut à la suivante : (K, +, .) est un anneau, et de plus la loi induite dans K—{0} par la multiplication confère à K—{0} une structure de groupe. Tout corps est donc aussi un anneau intègre et unitaire.

Remarque : Un abus de langage constant parce que commode consiste à désigner le corps (K, +, .) par la même lettre, K, que l'ensemble sous-jacent. Cependant, un ensemble pouvant être constitué en corps de plusieurs façons, l'abréviation précédente ne doit être admise que si aucune confusion ne peut en résulter.

Exemples :

1. Quand le naturel p est premier, l'anneau des classes d'entiers modulo p est un corps.

2. Corps des rationnels $\mathbb{Q}$, corps des réels $\mathbb{R}$, corps des complexes $\mathbb{C}$.

3. Corps des quaternions sur $\mathbb{R}$[QUATERNION].

4. Corps des quotients d'un anneau d'intégrité [QUOTIENT].

1.2. *Corps commutatifs :* corps dont la deuxième loi est commutative; on appelle parfois « corps gauche » (anglais *skew field*) un corps non commutatif (noter que certains réservent l'appellation *corps* aux corps commutatifs).

Les corps des exemples 1 et 2 ci-dessus sont commutatifs; le corps des quaternions ne l'est pas.

1.3. *Corps finis*, appelés aussi « corps de Galois » ou « champs de Galois » : corps dont l'ensemble sous-jacent est fini; le cardinal de cet ensemble, qui est nécessairement une puissance d'un nombre

premier, s'appelle l'*ordre* du corps. Réciproquement toute puissance d'un nombre premier est l'ordre d'un corps fini, qui est unique à un isomorphisme près. On montre que tous les corps finis sont commutatifs.

Les corps de l'exemple 1 ci-dessus sont finis.

1.4. La structure de corps peut intervenir dans des structures plus complexes, définies soit sur un autre ensemble (par exemple structure d'*espace vectoriel* [VECTORIEL]), soit même sur l'ensemble sous-jacent au corps : tel est le cas des *corps valués* [VALUÉ] et des *corps ordonnés*.

Un corps ordonné est un quadruplet $(K, +, ., \prec)$ tel que d'une part $(K, +, \prec)$ soit un groupe ordonné [GROUPE, **6**] et d'autre part, si l'on désigne par K^+ le sous-ensemble de K constitué par les éléments postérieurs à l'élément nul, K^+ soit stable pour la multiplication, c'est-à-dire :

$$\forall a \in K^+, \quad \forall b \in K^+, \quad a.b \in K^+.$$

(Voir aussi ARCHIMÉDIEN.)

2. Sous-corps et surcorps. Corps premiers.

2.1. Soient deux corps K et L tels que $K \subset L$ et que les lois de K soient les lois induites par celles de L : K est dit un *sous-corps* de L, L est dit un *surcorps* de K. On dit aussi que L est une *extension* de K, mais on réserve plutôt ce mot pour attirer l'attention sur le fait que L est canoniquement un espace vectoriel sur K.

2.2. *Sous-corps premier. Corps premiers.* L'intersection de tous les sous-corps d'un corps L est un sous-corps de L, qu'on appelle le *sous-corps premier* de L.

Tout corps qui est son propre sous-corps premier est dit *corps*

premier. Tout corps premier fini est d'ordre premier p, et il est isomorphe au corps des classes d'entiers modulo p; tout corps premier infini est isomorphe à $\mathbb{Q}$.

2.3. *Caractéristique d'un corps*. Étant groupe additif, tout corps L est un $\mathbb{Z}$-module; il est donc légitime, si l'on désigne par e l'unité de L et par k un entier quelconque de $\mathbb{Z}$, de considérer dans L les éléments de la forme ke. Ces éléments constituent un anneau unitaire, isomorphe à un certain anneau $\mathbb{Z}/q\mathbb{Z}$, dont la caractéristique q est appelée *caractéristique* du corps L [CARACTÉRISTIQUE].

Tout corps a même caractéristique que son sous-corps premier, à savoir : p (premier) si ce sous-corps est fini d'ordre p, et 0 si ce sous-corps est infini (par exemple $\mathbb{C}$, $\mathbb{R}$, ainsi que leur sous-corps premier $\mathbb{Q}$ sont des corps de caractéristique nulle). Cette propriété donne une autre définition possible de la caractéristique d'un corps.

2.4. *Sous-corps engendré par une partie d'un corps; extensions d'un sous-corps*. Soit A une partie d'un corps L : l'intersection de tous les sous-corps de L contenant A est un sous-corps de L qu'on appelle le *sous-corps engendré par* A.

Si K est un sous-corps de L et A une partie de L, le sous-corps engendré par $K \cup A$, noté K(A), s'appelle l'*extension de* K *par* A (en particulier, si K est le sous-corps premier, K(A) n'est autre que le sous-corps engendré par A).

L'extension de K par un singleton $\{\theta\}$ est dite *extension simple* et notée plus brièvement $K(\theta)$.

3. Extensions d'un corps commutatif.

On suppose désormais que le corps K est *commutatif* et l'on désigne par $K[x]$ l'anneau des polynomes en x à coefficients dans K. Soit θ un élément d'un surcorps commutatif de K : si θ est racine d'un polynome de $K[x]$, on dit que θ est *algébrique* dans K; sinon on dit que θ est *transcendant* dans K.

3.1. *Extension transcendante simple.* Une extension simple de K par un élément transcendant est dite *extension transcendante simple* de K; toutes les extensions transcendantes simples de K sont isomorphes au corps des quotients de l'anneau K[x] et donc identiques à un isomorphisme près. *Ex.:* le corps des fractions rationnelles en π à coefficients dans $\mathbb{Q}$ est une extension transcendante simple de $\mathbb{Q}$.

3.2. *Extensions algébriques. Corps des racines d'un polynome.* Si un polynome P de K[x], de degré non nul, est irréductible dans K, on montre qu'on peut toujours construire une extension K(θ), unique à un isomorphisme près et isomorphe à l'anneau-quotient K[x]/P, dans laquelle P(θ) = 0; on l'appelle une *extension algébrique simple* du corps K.

Soit alors Q un polynome de K[x], de degré n non nul, sans racines dans K. Que Q soit irréductible dans K, ou qu'on construise une extension algébrique simple à partir d'un facteur irréductible de Q, de toute façon on dispose d'une extension K(θ) dans laquelle Q est décomposable en un produit de polynomes dont l'un au moins, x—θ, est du premier degré; c'est pourquoi on dit parfois que K(θ) est un *corps de rupture* ou *de décomposition* de Q. Cette décomposition est dite *totale* si elle comporte n facteurs du premier degré; sinon elle comporte seulement m facteurs du premier degré ($m \leqslant n-2$) et un polynome Q', de degré $n-m$, sans racines dans K(θ). On recommence alors avec Q', et, après un nombre nécessairement fini d'extensions successives, on arrive à une extension algébrique telle que le polynome Q s'y décompose en n facteurs du premier degré. On montre que le plus petit corps où cela est possible est déterminé par Q à un isomorphisme près et on l'appelle le *corps des racines* de Q. (Cette appellation semble préférable aux expressions « corps de rupture », « corps de décomposition », « corps de décomposition totale », dont la signification varie suivant les auteurs.)

3.3. Se rattachent aux notions précédentes les expressions :

Corps algébriquement clos. Un corps K est dit algébriquement clos lorsque tout polynome à coefficients dans K, de degré n non nul, se décompose dans K[x] en n facteurs du premier degré. C'est donc le corps des racines de tout polynome de K[x]. *Ex.:* $\mathbb{C}$ est algébriquement clos (théorème de d'Alembert).

Corps algébriquement fermé dans un surcorps. Dire que le corps K est algébriquement fermé dans le surcorps L signifie que toutes les racines dans L des polynomes à coefficients dans K sont des éléments de K. (Ne pas confondre cette notion, *relative à* L, avec la précédente, qui ne dépend que de K.)

Corps parfait : corps K tel que, pour tout polynome P de K[x] irréductible dans K, et pour tout surcorps L de K, les racines de P appartenant à L sont simples. *Ex.:* tout corps de caractéristique nulle, tout corps de Galois.