module, n.m.

[modulo]

Lat. *modulus,* diminutif de *modus* (mesure) ; le sens général est celui de mesure, mais il ne se rencontre que dans la langue technique (architecture, physique, etc.).

1. Module d'un nombre complexe.

Soit $z = x + iy$ un nombre complexe, x et y étant réels ; le nombre réel positif ou nul $r = \sqrt{x^2 + y^2}$ s'appelle *module*, (ou parfois *valeur absolue*) de z et se note $|z|$. (Le mot a été introduit par Argand en 1806, la notation $|z|$ par Weierstrass).

2. Module d'une congruence.

Soit $\mathbb{Z}$ l'ensemble des entiers et p un naturel supérieur ou égal à 1.

Considérons la relation « $\exists k \in \mathbb{Z},\ x - y = kp$ » entre deux éléments x et y de $\mathbb{Z}$. C'est une relation d'équivalence sur $\mathbb{Z}$, appelée *congruence de module p.*, et notée :

$$x \equiv y \pmod{p}$$

qui se lit habituellement « x est congru à y modulo p ». (Il vaudrait peut-être mieux dire « x est congru modulo p à y »). [MODULO].

De même, sur $\mathbb{R}$, la relation d'équivalence « $\exists k \in \mathbb{Z},\ x - y = k \cdot 2\pi$ » entre deux éléments x et y de $\mathbb{R}$ définit une congruence de module 2π.

3. Module sur un anneau.

Soit $(E, +)$ un groupe commutatif et $(A, \dot{+}, .)$ un anneau ; on dit que E est un *module* sur l'anneau A ou un *A-module* (à gauche), s'il existe une loi de composition externe $A \times E \to E$, notée $(\lambda, x) \mapsto \lambda x$, telle que :

$$\begin{aligned}
&(a)\ \lambda(\mu x) = (\lambda . \mu)x,\\
&(b)\ (\lambda \dotplus \mu)x = \lambda x + \mu x,\\
&(c)\ \lambda(x + y) = \lambda x + \lambda y,
\end{aligned}$$

(*d*) au cas où l'anneau est unitaire : $1x = x$.

Un A-module à droite est défini de façon analogue, la loi externe $A \times E \to E$ étant notée $(\lambda, x) \to x\lambda$, avec les conditions :

$$\begin{aligned}
&(a)\ (x\mu)\lambda = x(\mu . \lambda),\\
&(b)\ x(\lambda \dotplus \mu) = x\lambda + x\mu,\\
&(c)\ (x + y)\lambda = x\lambda + y\lambda,
\end{aligned}$$

(*d*) au cas où l'anneau est unitaire : $x1 = x$.

Si l'anneau est commutatif, il n'y a pas lieu de faire la distinction entre module à droite et module à gauche.

Dans la pratique, si la confusion n'est pas à redouter, on ne distingue pas les deux signes $+$ et $\dotplus$.

Les éléments de A sont généralement appelés les *scalaires* du A-module, et ceux de E ses *vecteurs*.

Ex.: Tout groupe commutatif $(G, +)$ est un $\mathbb{Z}$-module; on a ainsi $2x = x + x$.

Lorsque l'anneau A est un *corps*, le A-module est appelé *espace vectoriel*; l'algèbre linéaire est l'étude des modules et des espaces vectoriels.

4. Module de continuité.

Soit E un intervalle de $\mathbb{R}$ et f une application de E dans $\mathbb{R}$. Posons :

$$\varphi(\delta) = \sup \{|f(x_1) - f(x_2)|;\ (x_1, x_2) \in E^2;\ |x_1 - x_2| \leqslant \delta\}$$

la fonction φ s'appelle le *module de continuité de f* sur E.

Plus généralement, étant donné deux espaces métriques (E, d) et (E', d') où d et d' désignent les distances dans les espaces corres-

/...

pondants, désignons par φ une application croissante de $\mathbb{R}^+$ dans $\mathbb{R}^+$ et par f une application de E dans E′; on dit que φ est un *module de continuité* de f sur E si pour tout couple (x_1, x_2) de E^2 :

$$d'(f(x_1), f(x_2)) \leqslant \varphi(d(x_1, x_2)).$$

Cette notion est en relation directe avec la notion de continuité uniforme.

5. Autres sens.

Module d'un système de logarithmes [LOGARITHME].
Module d'une intégrale elliptique [ELLIPTIQUE].
Module d'un vecteur : expression encore usitée, mais peu recommandée à présent pour désigner la *longueur* ou la *norme euclidienne* [NORME].

modulo

Cette forme du mot latin *modulus* a donné naissance à un véritable ablatif absolu dans la langue mathématique. Au départ « modulo p » signifie littéralement « p étant le module » au sens des congruences; ainsi l'on écrit : $x \equiv y \pmod p$ [MODULE, 2].

D'un point de vue voisin, étant donné un ensemble E et une relation d'équivalence R sur E, pour dire que x et y sont dans la même classe d'équivalence, il est courant de substituer à l'écriture $R\{x, y\}$ la notation : $x \equiv y \pmod R$, qui se lit « x est congru à y modulo la relation R ».

Exemple : Classes modulo un sous-groupe. Soit un groupe G et H un sous-groupe de G. Considérons la relation d'équivalence R telle que

$$\forall(x,y) \in G^2, \ [x \equiv y \ (\text{mod } R)] \Leftrightarrow [x^{-1}y \in H]$$

L'ensemble C_x des éléments de G qui sont de la forme xz avec $z \in H$, c'est-à-dire :

$$C_x = \{y \mid \exists z \in H, y = xz\}$$

est une classe d'équivalence; on l'appelle *classe à droite modulo le sous-groupe* H. On définit de même les classes à gauche modulo H.

Cette expression « modulo... » est devenue passe-partout, il est devenu courant d'entendre « modulo la propriété P, nous avons la propriété Q », « les transformations affines se ramènent aux transformations linéaires, modulo les translations », etc.