l'espace E des fonctions continues sur $[0\,;1]$ et à valeurs réelles, muni du produit scalaire $\langle f|g\rangle = \int_0^1 fg$, le sous-espace vectoriel U des fonctions s'annulant en 0 est un hyperplan de E et admet donc des supplémentaires ; cependant, il n'admet pas de supplémentaire orthogonal, car on peut montrer que $\mathrm{U}^\perp = \{0\}$.

Symétrie orthogonale ☞ SYMÉTRIE.

Théorème de projection orthogonale ☞ PROJECTION.

Vecteurs orthogonaux Dans un espace vectoriel préhilbertien, vecteurs dont le produit scalaire est nul.

ORTHONORMÉE

Base orthonormée d'un espace vectoriel euclidien E Base $(e_1, \dots, e_n)$ de E telle que $\langle e_i|e_j\rangle = \delta_{ij}$ pour tous i, j de $[\![1\,;n]\!]$.

REMARQUE : Dans une telle base, les calculs sont particulièrement simples. En effet, si $x = \sum_{k=1}^{n} x_k\, e_k$ et $y = \sum_{k=1}^{n} y_k\, e_k$, et si l'on note

$$\mathrm{X} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \qquad \text{et} \qquad \mathrm{Y} = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix},$$

alors $\langle x|y\rangle = {}^{\mathrm{t}}\mathrm{X} \cdot \mathrm{Y}$ si E est euclidien, et $\langle x|y\rangle = {}^{\mathrm{t}}\overline{\mathrm{X}} \cdot \mathrm{Y}$ si E est hermitien. De plus, $x_k = \langle e_k|x\rangle$ pour tout $k \in \mathbb{N}$. On a donc, au total :

$$x = \sum_{k=1}^{n} \langle e_k|x\rangle\ e_k \qquad \langle x|y\rangle = \sum_{k=1}^{n} \overline{x_k}\, y_k = \sum_{k=1}^{n} \langle x|e_k\rangle\ \langle e_k|x\rangle$$

Ces formules sont à rapprocher respectivement de la formule de Dirichlet, de la forme polaire de la formule de Parseval et de la définition d'un coefficient de Fourier.

Famille orthonormée d'un espace vectoriel préhilbertien E Famille $(x_i)_{i\in \mathrm{I}}$ de vecteurs de E telle que $\langle x_i|x_j\rangle = \delta_{ij}$ pour tous $i, j \in \mathrm{I}$. ✦ Une telle famille est nécessairement libre.

☞ BASE *HILBERTIENNE.

OSCULATEUR

Cercle osculateur Soit $\gamma : \mathrm{I} \to \mathbb{R}^2$ un arc paramétré plan de classe $\mathscr{C}^2$ au moins, paramétré par une abscisse curviligne, et soit $\mathrm{M}(s)$ un point birégulier de cet arc. Le cercle $\mathcal{C}$ de centre $\Omega = \mathrm{M}(s) + \mathrm{R}(s)\,\mathbf{N}(s)$, où $\mathrm{R}(s)$ est le rayon de courbure et $\mathbf{N}(s)$ le vecteur normal en $\mathrm{M}(s)$, est appelé cercle osculateur de γ en $\mathrm{M}(s)$. ✦ Le cercle $\mathcal{C}$ est, parmi tous les cercles passant par $\mathrm{M}(s)$, celui qui « épouse » au mieux l'arc au voisinage de $\mathrm{M}(s)$ (il s'en éloigne en $o(s^2)$).

☞ COURBURE, FRENET.

OUVERT

Soit E un espace vectoriel normé. Une partie $\mathrm{A} \subset \mathrm{E}$ est dite ouverte dans E (on dit aussi que A est un ouvert) si A est un voisinage de chacun de ses points, ou encore, si chacun des points de A est intérieur à A. En d'autres termes :

$$\forall a \in \mathrm{A} \quad \exists r > 0 \qquad \mathcal{B}(a\,;r) \subset \mathrm{A}.$$

☞ BOULES, ÉTOILÉ, FERMÉ, POINT *INTÉRIEUR, TOPOLOGIE RELATIVE, VOISINAGE.

P

PAIR

Fonction paire Fonction définie sur un intervalle I de $\mathbb{R}$, symétrique par rapport à 0, et telle que, pour tout $x \in \mathrm{I}$, on ait $f(-x) = f(x)$.

REMARQUES : Si f est paire et dérivable, sa dérivée est impaire. ✦ Si f est impaire et dérivable, alors sa dérivée est paire. ✦ Si f est développable en série entière $\sum a_n\, x^n$, alors f est paire si et seulement si $a_{2n+1} = 0$ pour tout $n \in \mathbb{N}$.

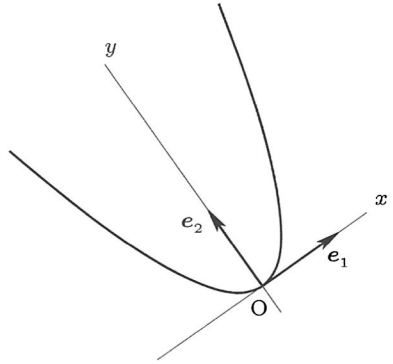
Partie paire d'une fonction Toute fonction $f :]-\mathrm{A}\,;+\mathrm{A}[\to \mathbb{K}$ peut s'écrire, de manière unique, comme la somme d'une fonction paire et d'une fonction impaire ; en notant $\hat{f} : x \mapsto f(-x)$, cette décomposition s'écrit $f = \frac{1}{2}(f + \hat{f}) + \frac{1}{2}(f - \hat{f})$, ou encore

$$\forall x \in \mathrm{I} \qquad f(x) = \frac{f(x) + f(-x)}{2} + \frac{f(x) - f(-x)}{2}.$$

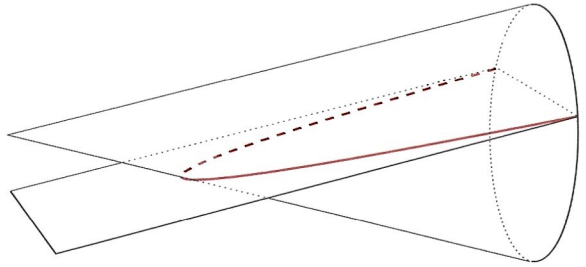
La partie paire de f est $\frac{1}{2}(f + \hat{f})$.

PARABOLE

Conique à un seul axe de symétrie, d'équation $x^2 = 2p\,y$ dans un repère orthonormé d'axe Oy confondu avec cet axe de symétrie, et d'origine le sommet de la parabole. ✦ C'est une conique connexe et non bornée.

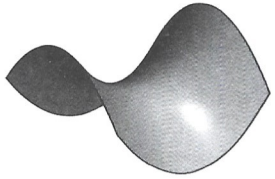
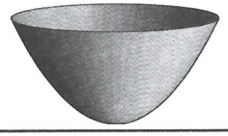


REMARQUE : Une parabole est obtenue par section d'un cône de révolution par un plan parallèle à une génératrice du cône.

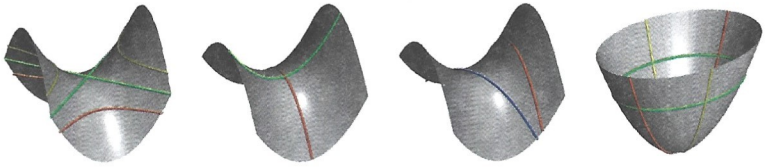


PARABOLOÏDE

Quadrique de rang 2. ✦ Est appelée *paraboloïde elliptique* si la forme quadratique associée a (en plus de zéro) deux valeurs propres de même signe (strict), et *paraboloïde hyperbolique* si elle a une valeur propre strictement positive et une autre strictement négative. ✦ Un *paraboloïde de révolution* est un paraboloïde elliptique dont la section droite est un cercle. Un tel paraboloïde est engendré par une parabole tournant autour de son axe de symétrie.

Nom	Équation réduite	allure
Paraboloïde elliptique	$z = \frac{x^2}{a^2} + \frac{y^2}{b^2}$	
Paraboloïde hyperbolique	$z = \frac{x^2}{a^2} - \frac{y^2}{b^2}$	
Paraboloïde de révolution	$z = \frac{x^2}{a^2} + \frac{y^2}{a^2}$	

Remarque : L'intersection d'un paraboloïde hyperbolique avec un plan $z = C^{te}$ donne une hyperbole, ou la réunion de deux droites (1re figure ci-dessous). L'intersection avec les plans d'équations respectives $x = 0$ et $y = 0$ est une parabole (2e figure), ainsi que l'intersection avec tout plan vertical (3e figure). De même, les intersections d'un paraboloïde elliptique avec des plans sont des paraboles ou des ellipses (4e figure).



☞ Quadrique, Surface *réglée.

PARADOXE

On prendra soin de bien distinguer deux sortes bien distinctes de paradoxes. ✦ Les premiers sont les « vrais » paradoxes : des raisonnements qui ont l'apparence du vrai, mais qui conduisent à un résultat manifestement faux. La plupart du temps, ils sont basés sur des ambiguïtés de langage (un mot peut avoir deux sens légèrement différents, l'un et l'autre étant employés consécutivement lors de la démonstration) ou des abus mathématiques (application de certains raisonnements justes à des situations où ils ne s'appliquent pas).

Exemple : Un exemple célèbre est donné par le paradoxe de Russel, du nom du philosophe et mathématicien Bertrand Russell (1872–1970). Considérons tous les ensembles, et notons $\mathscr{E}$ l'ensemble de tous les ensembles. Parmi ceux-ci, distinguons les ensembles qui sont éléments d'eux-mêmes et ceux qui ne le sont pas. Notons $\mathscr{R}$ l'ensemble de tous les ensembles qui ne sont pas éléments d'eux-mêmes. La question se pose alors : $\mathscr{R}$ est-il un élément de $\mathscr{R}$? Le lecteur découvrira que la réponse « oui » comme la réponse « non » conduisent à une contradiction. ✦ Ici, le paradoxe est ainsi levé : ce que l'on a noté $\mathscr{E}$ et $\mathscr{R}$ ne sont pas des ensembles (on les appelle plutôt des classes), et le raisonnement conduisant au paradoxe ne tient plus. (Ce n'est pas juste un jeu de langage : la formalisation des définitions et propriétés du langage ensembliste a permis de dégager les règles de raisonnement valides concernant les ensembles, et ces règles ne laissent pas de place au « paradoxe » de Russel. En revanche, les travaux d'autres logiciens, comme Fregge, ont été anéantis pas les réflexions de Russel.)

✦ La deuxième classe de paradoxe est celle des résultats mathématiquement valides, mais qui sont simplement « étonnants » ou « contre-intuitifs ».

Exemples : C'est le cas des paradoxes de Banach-Tarski et de Walter Penney.
Le premier affirme l'existence d'un découpage particulier de la sphère de rayon 1 de $\mathbb{R}^3$ en cinq parties disjointes ($\mathscr{S} = A_1 \cup A_2 \cup A_3 \cup A_4 \cup A_5$) tel que l'on puisse faire subir une rotation et une translation à chacune de ces parties, afin de les réassembler (à la façon des pièces d'un puzzle) pour créer *deux* sphères de rayon 1, strictement identiques à la première (il ne leur manque aucun point) :

$$\mathscr{S}'_1 = A'_1 \cup A'_2 \qquad \mathscr{S}'_2 = A'_3 \cup A'_4 \cup A'_5.$$

Ce résultat semble paradoxal, car il semble violer la « conservation du volume » (le volume d'une partie de $\mathbb{R}^3$ est conservé lors d'une translation ou d'une rotation). En réalité, le découpage est choisi de manière à ce que certaines pièces du puzzle ne soient pas « mesurables », au sens où il est impossible de leur attribuer une mesure de volume. L'argument de conservation tombe alors. Il est à noter que ce résultat emploie, de manière fondamentale, l'axiome du choix. Aussi, aucun découpage de la sphère vérifiant cette propriété ne pourra jamais être exhibé explicitement.

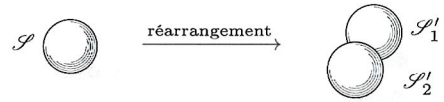


Fig. 69 — Le découpage de la sphère $\mathscr{S}$ permet de reconstruire deux sphères $\mathscr{S}'_1$ et $\mathscr{S}'_2$ strictement identiques à la sphère originelle.

✦ Le paradoxe de Walter Penney est un des nombreux paradoxes apparaissant dans le domaine des probabilités. On considère une succession infinie de tirages à pile ou face, qui a lieu devant plusieurs joueurs. Chacun des joueurs peut choisir une succession de trois résultats, par exemple *pile-pile-face*, ou *face-pile-face*. Le premier joueur qui voit sortir sa succession est déclaré vainqueur. W. Penney montra que, quelle que soit la succession choisie (parmi les huit possibles), il existe une succession qui soit meilleure, au sens où elle a une probabilité strictement plus grande que 1/2 d'apparaître avant la première. (Par exemple, la stratégie FPP est battue par FFP, qui est battue par PFF, qui est battue par PPF, qui est battue par FPP !)
L'aspect paradoxal de ce résultat (authentiquement étonnant) vient de ce que l'on a tendance à associer, au vocable « meilleur que », une propriété de transitivité : si A est meilleur que B et que B est meilleur que C, alors A est meilleur que C.

PARALLÈLES

Sous-espaces affines parallèles Un sous-espace affine $\mathscr{A}$ de direction A est dit parallèle à un sous-espace affine $\mathscr{B}$ de direction B si $A \subset B$ ou $B \subset A$. ✦ Parfois, on réserve la dénomination *parallèle* au cas où $A = B$, et on dit que $\mathscr{A}$ est *faiblement parallèle* à $\mathscr{B}$ si $A \subset B$. La relation « être faiblement parallèle » n'est pas symétrique, au contraire de la relation « être parallèle ».

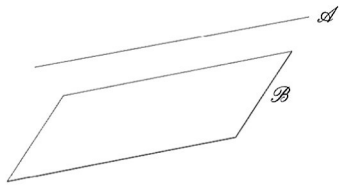
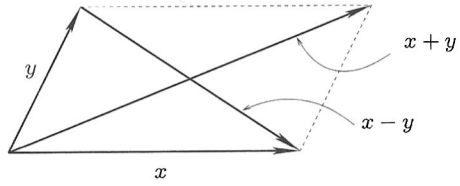


Fig. 70 — Une droite (faiblement) parallèle à un plan.

PARALLÉLOGRAMME

Égalité du parallélogramme Dans un espace vectoriel préhilbertien,

$$\|x+y\|^2 + \|x-y\|^2 = 2\|x\|^2 + 2\|y\|^2 .$$



PARAMÉTRAGE

Paramétrage admissible Soit $\gamma : [a\,;b] \to \mathrm{F}$ un arc paramétré de classe $\mathscr{C}^k$. Tout paramétrage $\mathscr{C}^k$-équivalent à γ, c'est-à-dire de la forme $\gamma \circ \varphi$, où φ est un $\mathscr{C}^k$-difféomorphisme, est dit admissible.

Paramétrage normal Un paramétrage γ d'un arc est dit normal si sa dérivée est de norme constante égale à 1. ✦ Si $\boldsymbol{f}$ est un paramétrage régulier de classe $\mathscr{C}^1$, et si S est une abscisse curviligne, alors $\gamma = \boldsymbol{f} \circ \mathrm{S}^{-1}$ est un paramétrage normal.

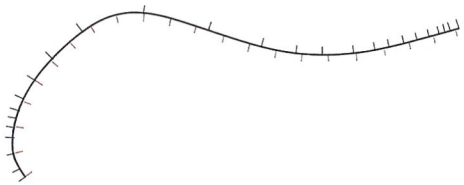


Fig. 71 — Deux paramétrages pour un même arc. En bleu, les positions des points $\boldsymbol{f}(t)$ pour des valeurs entières de t. En rouge, les positions des points $\gamma(s)$ pour des valeurs entières de l'abscisse curviligne s. L'arc γ est donc parcouru à vitesse constante (par rapport au temps « s »).

☞ Abscisse *curviligne.

Changement de paramétrage Si γ et μ sont deux paramétrages $\mathscr{C}^k$-équivalents d'un arc paramétré, le $\mathscr{C}^k$-difféomorphisme φ tel que $\gamma = \mu \circ \varphi$ est appelé changement de paramétrage. ✦ Par abus de langage, on l'appelle parfois paramétrage.

Remarque : On évitera d'employer « paramétrisation », qui est barbarisme.

PARAMÉTRIQUE

Représentation paramétrique d'un arc Représentation d'un arc au moyen d'un paramètre : si I est un intervalle et $\boldsymbol{f} : \mathrm{I} \to \mathbb{R}^n$ une application continue, à tout réel $t \in \mathrm{I}$ on associe le point $\mathrm{M}(t) = \boldsymbol{f}(t)$. En pratique, la donnée de la fonction vectorielle $\boldsymbol{f}$ se résume à la donnée de ses coordonnées : $t \mapsto x(t)$, $t \mapsto y(t)$, etc.

Exemple : L'ellipse d'équation cartésienne $\dfrac{x^2}{a^2} + \dfrac{y^2}{b^2} = 1$ peut être représentée paramétriquement par

$$\begin{cases} x(t) = a\cos t, \\ y(t) = b\sin t, \end{cases} \qquad t \in [\,0\,;\,2\pi\,].$$

Représentation paramétrique d'une droite Une droite $\mathscr{D}$ passant par deux points A et B peut se représenter paramétriquement de la façon suivante : on note $\boldsymbol{u} = \mathbf{AB}$; alors

$$\mathscr{D} = \mathrm{A} + \mathbb{R}\,\boldsymbol{u} = \{\mathrm{A} + t\boldsymbol{u}\ ;\ t \in \mathbb{R}\}.$$

PARSEVAL *Marc Antoine Parseval des Chênes* (1755–1836)

(Mathématicien français)

Égalité de Parseval Si $(e_n)_{n\in\mathbb{N}}$ est une famille orthonormée d'un espace préhilbertien $\big(\mathrm{E}, \|\cdot\|\big)$, il y a équivalence entre les énoncés :

(*a*) l'espace Vect $\{e_n\ ;\ n \in \mathbb{N}\}$ est dense dans E ;

(*b*) pour tout $x \in \mathrm{E}$, on a $\|x\|^2 = \sum_{n=0}^{\infty} \big|\,\langle e_n|x\rangle\,\big|^2$;

(*c*) pour tous $x, y \in \mathrm{E}$, on a $\langle x|y\rangle = \sum_{n=0}^{\infty} = \langle x|e_n\rangle\ \langle e_n|y\rangle$.

Exemple : L'espace des polynômes trigonométriques étant dense (pour la norme $\|\cdot\|_2$) dans l'espace des fonctions continues et 2π-périodiques, cette égalité devient la formule de Parseval, que l'on peut généraliser aux fonctions continues par morceaux.

Formule de Parseval Soit $f : \mathbb{R} \to \mathbb{C}$ une fonction 2π-périodique et continue par morceaux. Alors, en notant a_n, b_n et c_n ses coefficients de *Fourier,

$$|c_0|^2 + \sum_{n=1}^{\infty} \big(\,|c_n|^2 + |c_{-n}|^2\,\big) = \frac{1}{2\pi}\int_{[2\pi]} |f(t)|^2\ \mathrm{d}t,$$

où l'intégrale est prise sur un intervalle quelconque de longueur 2π. ✦ Si f est réelle, alors la série $\sum(a_n^2 + b_n^2)$ converge et

$$\frac{a_0^2}{4} + \frac{1}{2}\sum_{n=1}^{\infty}(a_n^2 + b_n^2) = \frac{1}{2\pi}\int_{[2\pi]} f(t)^2\ \mathrm{d}t.$$

✦ Par polarisation, si g est également continue par morceaux et 2π-périodique, alors

$$\sum_{n=-\infty}^{\infty} \overline{c_n(f)}\ c_n(g) = \frac{1}{2\pi}\int_{[2\pi]} \overline{f(t)}\ g(t)\ \mathrm{d}t.$$

✦ Notamment, l'application $f \mapsto \hat{f}$ réalise une isométrie de l'espace des fonctions continues et 2π-périodiques vers l'espace $\ell^2(\mathbb{Z})$ des suites de carré intégrable ; elle est donc injective.

Théorème de Parseval Soit $f : \mathbb{R} \to \mathbb{C}$ une fonction 2π-périodique et continue par morceaux. Alors la suite des sommes partielles de Fourier de f converge en moyenne quadratique vers f : $\lim\limits_{n\to\infty} \int_{[2\pi]} |f - S_n|^2 = 0$.

PARTIE

Partie d'un ensemble E Ensemble A tel que tout élément de A est élément de E :

$$\forall x \in A \qquad x \in E.$$

On écrit alors $A \subset E$. ✦ L'ensemble des parties d'un ensemble E est noté $\mathfrak{P}(E)$. ✦ Si E est fini et de cardinal n, alors $\mathfrak{P}(E)$ est fini et de cardinal 2^n.

Partie entière d'un réel Si x est un réel, sa partie entière, notée $\lfloor x \rfloor$ ou $E(x)$, est l'unique entier n vérifiant $n \leqslant x < n+1$. ✦ La fonction partie entière est définie sur $\mathbb{R}$, croissante, continue à droite, mais pas à gauche, en chaque entier, et continue sur $\mathbb{R} \setminus \mathbb{Z}$.

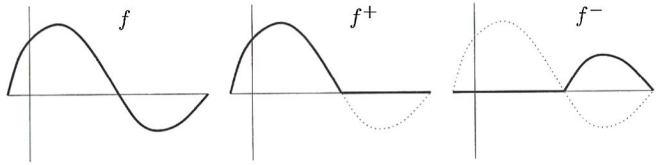
Partie entière d'une fraction rationnelle ☞ Décomposition en éléments *simples.

Partie polaire d'une fraction rationnelle ☞ Décomposition en éléments *simples.

Partie positive/négative Soit $f : I \to \mathbb{R}$. On définit les parties positive et négative de f par

$$f^+(x) = \max\big(f(x), 0\big) \qquad f^-(x) = \max\big(-f(x), 0\big)$$

pour tout $x \in I$. ✦ On a alors $f = f^+ - f^-$. ✦ De plus, si f est continue par morceaux, alors $f^+ = \frac{1}{2}(|f| + f)$ et $f^- = \frac{1}{2}(|f| - f)$ le sont également.



Intégration par parties ☞ Intégration.

PARTITION

Une partition d'un ensemble A est la donnée d'une famille $(C_i)_{i\in I}$ de parties non vides de A, deux à deux disjointes et dont la réunion vaut A :

$$C_i \cap C_j = \varnothing \text{ dès que } i \neq j \qquad \text{et} \qquad \bigcup_{i\in I} C_i = A.$$

✦ On peut alors définir une relation d'équivalence sur A en disant que $x \sim y$ si et seulement si x et y appartiennent au même C_i. La famille $(C_i)_{i\in I}$ est exactement la famille des classes d'équivalence de la relation « $\sim$ ».

☞ Classe d'équivalence, Système complet.

PAS

☞ Subdivision.

PASCAL *Blaise* (1623–1662)

(Philosophe, physicien et mathématicien français)

Triangle de Pascal Pour tous entiers n et k, $\binom{n+1}{k+1} = \binom{n}{k+1} + \binom{n}{k}$. Selon ce principe, on peut construire la succession des coefficients binomiaux en les disposant selon un triangle.

	$k=0$	$k=1$	$k=2$	$k=3$	$k=4$	
$n=0$	1					
$n=1$	1	1				
$n=2$	1	2	1			
$n=3$	1	3	3	1		
$n=4$	1	4	6	**4**	1	
...	1	...	...	...	...	1

Table 6 — Triangle de Pascal. Le premier coefficient de chaque ligne est égal à 1. Les autres coefficients sont égaux à la somme des coefficients directement au-dessus, et au-dessus et à gauche. Ici, le calcul menant à $\binom{4}{3} = 3+1 = 4$ est en couleur.

☞ Coefficients binomiaux.

PASSAGE

Matrice de passage ☞ Matrice.

Passage à la limite Derrière cette expression galvaudée et parfois employée un peu trop rapidement, on a essentiellement deux résultats. ✦ Le premier est une tautologie : si $(u_n)_{n\in\mathbb{N}}$ et $(v_n)_{n\in\mathbb{N}}$ sont deux suites à valeurs dans un espace vectoriel normé, si $u_n = v_n$ pour tout $n \in \mathbb{N}$ et si $(u_n)_{n\in\mathbb{N}}$ converge, alors $(v_n)_{n\in\mathbb{N}}$ converge et admet la même limite. On l'emploie en général quand on a deux expressions manifestement très différentes pour une même quantité. ✦ Le second n'est pas une tautologie, mais un vrai résultat d'analyse : si $(u_n)_{n\in\mathbb{N}}$ et $(v_n)_{n\in\mathbb{N}}$ sont des suites réelles vérifiant $u_n \leqslant v_n$ pour tout $n \in \mathbb{N}$, si $(u_n)_{n\in\mathbb{N}}$ converge vers ℓ et si $(v_n)_{n\in\mathbb{N}}$ converge vers ℓ', alors $\ell \leqslant \ell'$. ✦ Si ces suites vérifient $u_n < v_n$ pour tout $n \in \mathbb{N}$, la conclusion est inchangée : on obtient $\ell \leqslant \ell'$ (et non $\ell < \ell'$) !

Remarque : Par caractérisation séquentielle de la limite, un résultat semblable peut être énoncé pour des fonctions numériques : si $f(x) \leqslant g(x)$ pour tout $x \in I$ et si f et g admettent une limite en un point a adhérent à I, alors $\lim_a f \leqslant \lim_a g$.

Passage à la borne supérieure Soit A une partie de $\mathbb{R}$, et M un réel vérifiant $a \leqslant M$ pour tout $a \in A$. Alors $\sup A \leqslant M$ (rappelons que la borne supérieure est le plus petit des majorants...).

Exemple : Pour toute fonction φ continue sur $[0\,;1]$, notons $\|\varphi\|_\infty = \sup_{x\in[0\,;1]} |\varphi(x)|$. Soient f et g deux fonctions continues sur $[0\,;1]$; montrons que $\|f+g\|_\infty \leqslant \|f\|_\infty + \|g\|_\infty$. Pour cela, fixons momentanément un réel $x \in [0\,;1]$. Alors

$$|f(x)+g(x)| \leqslant |f(x)| + |g(x)|.$$

Par définition de la borne supérieure, on a $|f(x)| \leqslant \|f\|_\infty$ et $|g(x)| \leqslant \|g\|_\infty$, ce qui donne donc :

$$|f(x)+g(x)| \leqslant \|f\|_\infty + \|g\|_\infty.$$

On passe enfin à la borne supérieure sur x, pour obtenir $\|f+g\|_\infty \leqslant \|f\|_\infty + \|g\|_\infty$.

PAVÉ

Un pavé de $\mathbb{R}^n$ est une partie de $\mathbb{R}^n$ de la forme $I_1 \times \cdots \times I_n$, où les I_k sont des intervalles. ✦ On dit que c'est un *pavé ouvert* si tous les intervalles I_k sont ouverts.

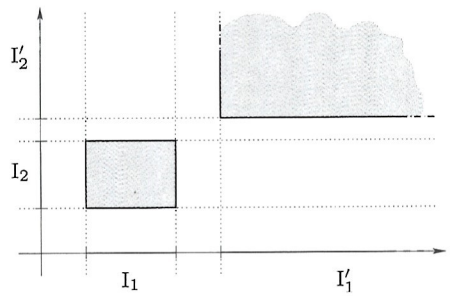


Fig. 72 — Un pavé borné $I_1 \times I_2$, et un pavé semi-infini $I'_1 \times I'_2$.

PEANO *Giuseppe* (1858–1932)
(Mathématicien italien)

Axiomatique de Peano Système axiomatique permettant de définir l'ensemble $\mathbb{N}$ des entiers naturels (et donc, notamment, l'arithmétique).

Remarque : Ce système axiomatique n'est plus utilisé — on utilise aujourd'hui le système ZFC (☞ Axiome) — mais il a une importance historique, car il a constitué la première formalisation rigoureuse de l'ensemble des entiers. ✦ Il comporte plusieurs axiomes (ou schémas d'axiomes), qui, transcrits en langage courant, postulent notamment : • 0 est un entier naturel ; • tout entier naturel a un successeur ; • 0 n'est le successeur d'aucun entier naturel ; • si deux entiers ont le même successeur, alors ils sont égaux ; • si une partie P de $\mathbb{N}$ contient 0, et si le successeur de tout élément de P est dans P, alors $P = \mathbb{N}$. ✦ Ce dernier axiome est appelé *axiome d'induction* et permet le raisonnement par récurrence.

☞ Axiome.

Courbe de Peano Suite à un résultat de Cantor, Peano exhiba une « courbe » remplissant entièrement un carré, c'est-à-dire une fonction $f : [0\,;1] \to [0\,;1]^2$, continue, et surjective. Les courbes vérifiant cette propriété portent le nom générique de courbes de Peano.

Remarque : La fonction f est obtenue comme somme d'une série de fonctions, ou comme limite d'une suite de fonctions $(f_n)_{n\in\mathbb{N}}$. On peut voir sur la figure 73 les premières courbes f_n. En réalité, les chemins se touchent (les fonctions ne sont pas injectives et leur limite f admet une infinité de points doubles), mais on a délibérément « émoussé » les angles afin de rendre visible le tracé continu, partant du coin inférieur gauche et menant au coin supérieur droit. ✦ De plus, la fonction f n'est nulle part dérivable (mais ce n'est pas une fatalité, il est possible de construire des courbes remplissant le carré et qui soient presque partout dérivable ☞ Lebesgue). ✦ À l'époque, la plupart des mathématiciens n'y virent qu'un « monstre », une curiosité de salon, et non un objet mathématique d'intérêt.

PÉRIODIQUE
Soit f une fonction définie sur $\mathbb{R}$ et à valeurs dans un ensemble E. Soit T un réel non nul. On dit que f est T-périodique si $f(x+\mathrm{T}) = f(x)$ pour tout $x \in \mathbb{R}$. ✦ T est alors appelé *une* période de f.

PERMUTATION
Permutation d'un ensemble Bijection de cet ensemble sur lui-même. ✦ Le *support* d'une permutation est l'ensemble des éléments qui ne sont pas invariants par cette permutation. ✦ Une permutation de $[\![1\,;n]\!]$ est fréquemment notée, symboliquement :

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n). \end{pmatrix}$$

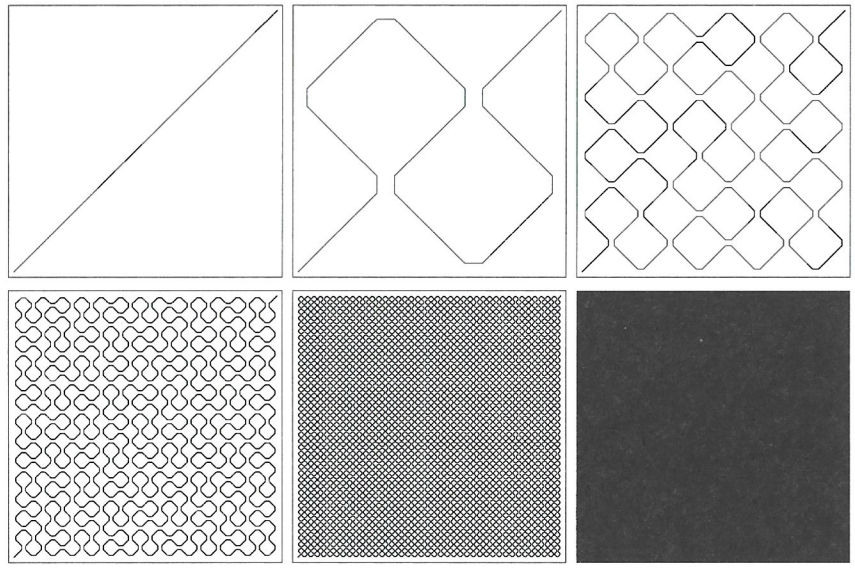


Fig. 73 — Courbe de Peano : les premières itérations. La courbe limite est la courbe de Peano, qui remplit entièrement le carré, et qui s'auto-intersecte une infinité de fois.

Exemples : La permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ est un cycle. ✦ La permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ est le produit $\sigma = \tau \circ \tau'$ de deux transpositions $\tau = (1\ 2)$ et $\tau' = (3\ 4)$.

Groupe des permutations d'un ensemble E Ensemble $\mathfrak{S}(\mathrm{E})$ des permutations d'un ensemble E qui, muni de la loi de composition, a une structure de groupe. ✦ Si E est fini et de cardinal n, le groupe $\mathfrak{S}(\mathrm{E})$ est isomorphe au groupe symétrique $\mathfrak{S}_n = \mathfrak{S}\big(\{1, 2, \ldots, n\}\big)$. Son ordre est $|\mathfrak{S}_n| = n!$.

☞ Groupe *alterné, Cycle, Dérangement, Groupe *symétrique, Signature, Transposition.

PETIT
Plus petit élément Soit $(\mathrm{A}, \leqslant)$ un ensemble ordonné. Un élément $m \in \mathrm{A}$ est appelé *plus petit élément* de A, s'il est inférieur à tous les éléments de A :

$$\forall a \in \mathrm{A} \qquad m \leqslant a.$$

✦ Un tel élément, s'il existe, est unique ; on le note $m = \min \mathrm{A}$. On l'appelle également *minimum* de A.

Remarques : Le plus petit élément de A, s'il existe, est nécessairement un élément de A. ✦ Toute partie non vide de $\mathbb{N}$ admet un plus petit élément.

☞ Atteindre, Borne inférieure, Maximum, Bon *ordre, Weierstrass (théorème sur les compacts).

Petit « o » ☞ Négligeable.

PGCD

PGCD de deux entiers a et b Générateur positif de l'idéal $a\mathbb{Z}+b\mathbb{Z}$. On le note $a\wedge b$ ou $\text{PGCD}(a,b)$. ✦ Ainsi, $a\mathbb{Z}+b\mathbb{Z}=(a\wedge b)\mathbb{Z}$. ✦ C'est également le plus grand (au sens de la divisibilité) diviseur positif commun à a et à b.

Exemple : $63\wedge 54=9$. ✦ $0\wedge 42=42$.

Remarques : Si a ou b est non nul, l'ensemble des diviseurs communs à a et b est une partie de $\mathbb{Z}$, non vide (1 en est élément) et majorée par $\max(|a|,|b|)$. Cet ensemble possède donc un plus grand élément (au sens de l'ordre usuel dans $\mathbb{Z}$), qui est également le plus grand au sens de la divisibilité, c'est donc $a\wedge b$. ✦ Lorsque $a=b=0$, tout élément de $\mathbb{Z}$ est diviseur commun à a et b ; l'ensemble des diviseurs communs à a et b n'est donc pas majoré au sens de l'ordre usuel ; en revanche, au sens de la divisibilité, il admet un plus grand élément, qui est 0 ; le PGCD de a et b est donc égal à 0.

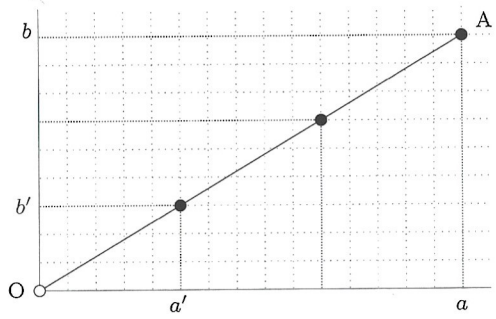


Fig. 74 — On peut interpréter le PGCD de deux nombres entiers a et b comme le nombre de points à coordonnées entières du segment [O ; A] privé de O, où A est le point de coordonnées (a,b). Sur la figure, $a=15$ et $b=9$, donc $d=3$. On a représenté également $a'=a/d$ et $b'=b/d$.

PGCD de deux polynômes A et B de $\mathbb{K}[X]$ Générateur normalisé de l'idéal $A\mathbb{K}[X]+B\mathbb{K}[X]$. On le note $A\wedge B$ ou $\text{PGCD}(A,B)$. ✦ Notamment, $A\mathbb{K}[X]+B\mathbb{K}[X]=(A\wedge B)\mathbb{K}[X]$. ✦ C'est également le plus grand (au sens de la divisibilité) diviseur normalisé commun à A et à B.

☞ Bézout, Euclide, Générateur, Idéal, PPCM.

PHASE

Portrait de phases Lors de l'étude d'un système différentiel autonome

$$\begin{cases} x'=f(x,y) \\ y'=g(x,y) \end{cases}$$

on construit généralement le portrait de phases du système, c'est-à-dire que l'on fait apparaître en certains points du plan un vecteur (souvent unitaire) de direction $\big(f(x,y),g(x,y)\big)$. ✦ Ces vecteurs sont tangents en tout point aux trajectoires du système.

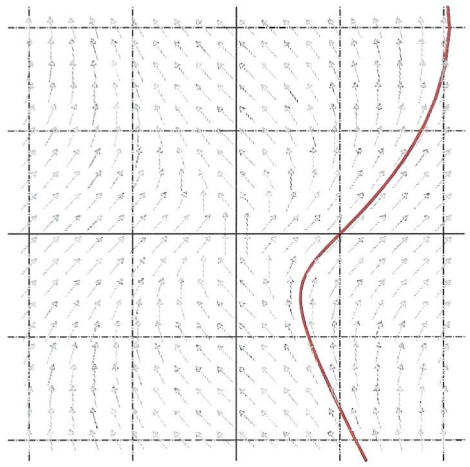


Fig. 75 — Portrait de phases associé au système différentiel autonome $x'=x^2-y^2$, $y'=x^2+y^2$. Une trajectoire est également affichée.

Remarques : Une telle figure est obtenue avec Maple à l'aide des instructions :

```
with(DEtools):
DEplot({
  diff(x(t),t) = x(t)^2-y(t)^2,
  diff(y(t),t)=x(t)**2+y(t)**2},
  [x(t),y(t)], t = -2..2, x = -2..2, y=-2..2,
  [[x(0) = 1,y(0)=0]],
  linecolor = red, thickness = 2, arrows=MEDIUM,
  stepsize = 0.05,  color=gray);
```

✦ Une équation du second degré de la forme $x''=f(x,x')$ se vectorialise sous la forme

$$\begin{cases} x'=y \\ y'=f(x,y) \end{cases}$$

ce qui permet de dresser un portrait de phase pour cette équation, avec en abscisse x et en ordonnée x'. Cette représentation est particulièrement pratique lors de l'étude de systèmes mécaniques. ✦ Une équation $x'=f(x)$ peut se vectorialiser dans le plan (t,x) sous la forme

$$\begin{cases} t'=1 \\ x'=f(x) \end{cases}$$

et son portrait de phase est alors invariant par translation selon t.

☞ Trajectoire.

PHÉNOMÈNE

Phénomène de Gibbs ☞ Gibbs.

Phénomène de Runge ☞ Runge.

PIVOT

Algorithme du pivot de Gauss Considérons un système linéaire de m équations à n inconnues $x_1,\dots,x_n$:

$$\begin{cases} a_{11}x_1+\cdots+a_{1n}x_n=b_1 & (L_1) \\ \vdots \qquad\qquad \vdots \quad \vdots & \\ a_{m1}x_1+\cdots+a_{mn}x_n=b_m & (L_m) \end{cases}$$

(On suppose qu'aucune colonne n'est identiquement nulle.) On cherche un coefficient $p_1 = a_{j1}$ non nul de l'inconnue x_1, appelé *pivot* de x_1 ; on effectue alors un échange entre les lignes L_1 et L_j, puis les transformations $L_k \leftarrow p_1 L_k - a_{k1} L_1$ pour $k = 2, \dots, n$. On aboutit alors à un système équivalent

$$\begin{cases} \boxed{p_1}\, x_1 + a'_{12} x_2 + \cdots + a'_{1n} x_n = b'_1 & (L'_1) \\ \qquad a'_{22} x_2 + \cdots + a'_{2n} x_n = b'_2 & (L'_2) \\ \qquad\qquad \vdots \qquad\qquad\quad \vdots \quad \vdots & \\ \qquad a'_{m2} x_2 + \cdots + a'_{mn} x_n = b'_m & (L'_m) \end{cases}$$

On réitère ce procédé sur les lignes (L'_2) à (L'_m) ; si l'on ne trouve pas de pivot à l'inconnue x_2, on peut échanger le rôle de x_2 et d'une inconnue suivante. ✦ Lorsqu'il n'est plus possible de poursuivre, le système a la forme suivante :

$$\begin{cases} \boxed{p_1}\, x_1 + \star\, x_2 + \cdots + \star\, x_r + \star x_{r+1} + \cdots + \star x_n = c_1 \\ \qquad \boxed{p_2}\, x_2 + \cdots + \star\, x_r + \star x_{r+1} + \cdots + \star x_n = c_2 \\ \qquad\qquad \ddots \qquad\qquad\qquad\qquad\qquad \vdots \quad \vdots \quad \vdots \\ \qquad\qquad\qquad \boxed{p_r}\, x_r + \star x_{r+1} + \cdots + \star x_n = c_r \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad 0 = c_{r+1} \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \vdots \quad \vdots \quad \vdots \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad 0 = c_m \end{cases}$$

✦ Le nombre r de pivots est le *rang* du système. ✦ Les r premières équations sont les *équations principales* et les $m - r$ dernières les *conditions de compatibilité*. Le système est *compatible* si et seulement si $c_{r+1} = \cdots = c_m = 0$. S'il est compatible, il admet des solutions. Dans le cas contraire, il n'en admet aucune. ✦ Les r premières inconnues $x_1, \dots, x_r$ sont les *inconnues principales* et les $n - r$ dernières sont les *inconnues auxiliaires*. ✦ Une base de l'ensemble des solutions du système homogène peut être obtenue ainsi. On choisit $n - r$ manières (linéairement indépendantes) de fixer les inconnues auxiliaires, par exemple sous la forme

$$(x_{r+1}, \dots, x_n) = (0, \dots, 0, \underset{\substack{\uparrow \\ k}}{1}, 0, \dots, 0)$$

pour k variant de $r + 1$ à n ; on résout, pour chacun de ces choix de l'ensemble des inconnues auxiliaires, les r premières équations à r inconnues (qui est un système de Cramer) ; on obtient alors une base de l'ensemble des solutions du système homogène.

Remarques : Cet algorithme est fondamental, tant du point de vue calculatoire (les formules de Cramer devenant inutilisables, même à l'ordinateur, dès que le nombre d'équations dépasse quelques dizaines) que du point de vue théorique. ✦ En pratique, si le système a des coefficients entiers, on choisira, pour chaque inconnue, le pivot le « plus proche de 1 » possible, afin d'éviter d'avoir des coefficients trop grands dans les systèmes successifs. ✦ Cependant, choisir le pivot « maximal » (au sens de la valeur absolue) et diviser la ligne considérée par ce pivot permet une plus grande stabilité numérique (méthode du *pivot maximal*).

PLAN VECTORIEL

Espace ou sous-espace vectoriel de dimension 2.

POINCARÉ *Henri Jules* (1854–1912)

(Mathématicien français)

Théorème de Poincaré Soit ω une forme différentielle de classe $\mathscr{C}^1$ sur un ouvert étoilé Ω. Si ω est fermée, alors elle est exacte.

Remarque : L'hypothèse « Ω ouvert étoilé » est plus forte que nécessaire, mais choisie pour sa grande simplicité. Dans $\mathbb{R}^2$, un ouvert « sans trou » (simplement *connexe) convient. Dans $\mathbb{R}^n$, la situation est plus délicate et a donné naissance à la théorie de la cohomologie, qu'il n'est pas possible d'exposer ici.

☞ Forme différentielle, Étoilé.

Formule de Poincaré (ou du crible) Soient $n \in \mathbb{N}^*$ et $A_1, \dots, A_n$ des événements d'un espace probabiliste. Alors

$$\mathbf{P}\left(\bigcup_{i=1}^{n} A_i\right) = \sum_{k=1}^{n} (-1)^{k+1} \sum_{1 \leqslant i_1 < i_2 < \cdots < i_k \leqslant n} \mathbf{P}(A_{i_1} \cap \cdots \cap A_{i_k}).$$

Exemple : Les cas $n = 2$ et $n = 3$ donnent respectivement

$$\mathbf{P}(A \cup B) = \mathbf{P}(A) + \mathbf{P}(B) - \mathbf{P}(A \cap B)$$
$$\mathbf{P}(A \cup B \cup C) = \mathbf{P}(A) + \mathbf{P}(B) + \mathbf{P}(C) - \mathbf{P}(A \cap B) - \mathbf{P}(B \cap C) - \mathbf{P}(C \cap A) + \mathbf{P}(A \cap B \cap C).$$

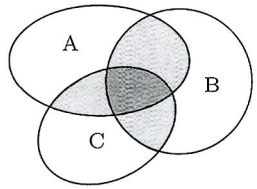


Fig. 76 — La formule de Poincaré pour $n = 3$. En gris foncé, $A \cap B \cap C$. En gris (clair + foncé), $A \cap B$, $A \cap C$ et $B \cap C$.

POINT

Dans un espace vectoriel, synonyme de vecteur.

Point d'accumulation ☞ Accumulation.

Point birégulier Soit $\gamma : I \to E$ un arc paramétré de classe $\mathscr{C}^2$. Soit $t \in I$. Le point $M = \gamma(t)$ est dit birégulier (ou *régulier à l'ordre* 2) si la famille $(\gamma'(t), \gamma''(t))$ est libre. ✦ Cette notion est invariante par changement de paramétrage. Si $\varphi : J \to I$ est un $\mathscr{C}^2$-difféomorphisme, alors l'arc $\Gamma : J \to E$ défini par $\Gamma = \gamma \circ \varphi$ est un arc de classe $\mathscr{C}^2$. Si $t = \varphi(u)$, alors $M(t)$ est un point birégulier de γ si et seulement si $\widetilde{M}(u) = \Gamma(u)$ est un point birégulier de Γ. (Les points géométriques M et $\widetilde{M}$ sont évidemment confondus.)

Remarque : Si γ est un arc de classe $\mathscr{C}^2$ et si $M = \gamma(t)$ est un point birégulier de γ, alors la courbure ne s'annule pas en M.

Point critique ☞ Critique.

Point fixe d'une fonction f ☞ Fixe.

Point d'inflexion Soit $M(t_0)$ un point d'un arc paramétré $\gamma : I \to \mathbb{R}^2$ de classe $\mathscr{C}^k$ du plan. Notons, s'ils existent, p et q le premier et le second entier *caractéristiques de γ en t_0. Si p et q sont impairs, on dit que la courbe admet un point d'inflexion en $M(t_0)$. ✦ Notamment, si $M(t_0)$ est un point régulier et si $\mathrm{Det}(\gamma', \gamma'')$ s'annule et change de signe en t_0, alors $M(t_0)$ est un point d'inflexion : la courbure a changé de signe.

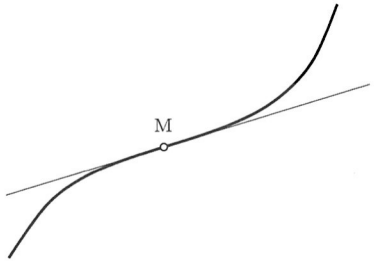


Fig. 77 — Point d'inflexion d'une courbe ; la tangente en M traverse la courbe en ce point.

☞ Courbure, Entiers *caractéristiques.

Point intérieur ☞ Intérieur.

Point pondéré ☞ Barycentre.

Point de rebroussement de 1re/2e espèce ☞ Rebroussement, Caractéristiques (entiers c.).

Point régulier Soit $\gamma : \mathrm{I} \to \mathrm{E}$ un arc paramétré de classe $\mathscr{C}^1$. Soit $t \in \mathrm{I}$. Le point $\mathrm{M} = \gamma(t)$ est dit régulier si $\gamma'(t) \neq 0$. ✦ En un tel point, l'arc admet une tangente, dirigée par $\gamma'(t)$.

Point stationnaire Point d'un arc paramétré γ de classe $\mathscr{C}^1$ en lequel la dérivée γ' s'annule. ✦ Synonyme : *point singulier.*

Remarque : Parfois, le terme est employé comme synonyme de point *critique. Cette dénomination fait référence à l'équation différentielle autonome associée à un champ de vecteurs : une solution prenant une valeur en un point critique est stationnaire (ou, du moins, peut l'être, car il n'y a pas forcément unicité...)

Point singulier Point d'un arc paramétré $\gamma : \mathrm{I} \to \mathrm{E}$ de classe $\mathscr{C}^1$ qui n'est pas régulier, c'est-à-dire en lequel la dérivée de γ s'annule. ✦ Synonyme : *point stationnaire.*

Point d'unicité locale/globale Condition initiale (t, x_0) pour laquelle une équation différentielle admet (localement ou globalement) une unique solution.

POISSON *Denis Siméon* (1781–1840)

(Mathématicien français)

Équation de Poisson Équation aux dérivées partielles de la forme $\triangle f = \rho$, où f est une fonction de classe $\mathscr{C}^2$ sur $\mathbb{R}^n$ (potentiel) et ρ une fonction représentant une densité (de charge, de masse...).

Formule sommatoire de Poisson Soit f une fonction de classe $\mathscr{C}^2$ par morceaux sur $\mathbb{R}$ telle que f, f' et f'' soient intégrables. Notons $\widetilde{f}$ sa transformée de *Fourier. Alors

$$\sum_{n=-\infty}^{+\infty} f(n) = \sum_{n=-\infty}^{+\infty} \widetilde{f}(n).$$

Noyau de Poisson Fonction définie sur $]\,0\,;\,1\,[\times \mathbb{R}$ par

$$\mathrm{K}(r,\theta) = \frac{1-r^2}{1-2r\cos\theta+r^2} = \frac{1-r^2}{\left|1-r\,\mathrm{e}^{\mathrm{i}\theta}\right|}.$$

Remarque : Cette fonction permet de calculer la valeur d'une fonction harmonique sur le disque unité, connaissant ses valeurs sur le cercle unité. ✦ Si f est continue sur le cercle unité complexe $\mathbb{U}$, alors

$$\lim_{r\to 1^-} \int_0^{2\pi} f(\mathrm{e}^{\mathrm{i}\theta})\,\mathrm{K}(r, t-\theta)\,\mathrm{d}\theta = f(\mathrm{e}^{\mathrm{i}t}).$$

La famille des fonctions $\left(t \mapsto \mathrm{K}(r,t)\right)_{r\in]\,0\,;\,1\,[}$ est une famille de fonctions de *Dirac sur le cercle $\mathbb{U}$.

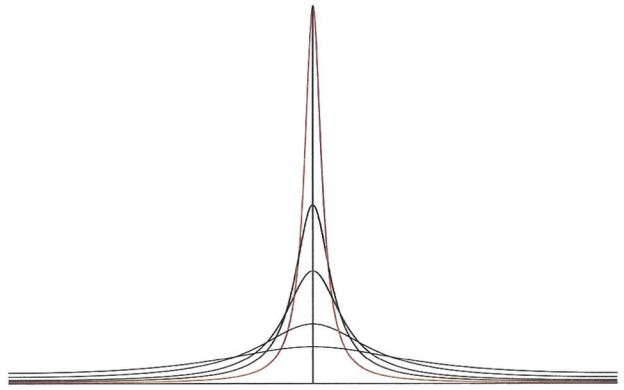


Fig. 78 — Les fonctions $t \mapsto \mathrm{K}(r,t)$ pour $r = 0,3$, $r = 0,5$, $r = 0,7$ et $r = 0,9$.

Loi de Poisson ☞ Loi.

POLAIRE

Coordonnées polaires À tout point $(x,y) \neq (0,0)$ de $\mathbb{R}^2$, on peut associer des coordonnées (ρ,θ) vérifiant $x = \rho\cos\theta$ et $y = \rho\sin\theta$. Il y a unicité de ces coordonnées si l'on impose $\rho > 0$ et $\theta \in\,]-\pi\,;\,+\pi\,]$ (ou n'importe quel intervalle semi-ouvert de longueur 2π).

Remarque : La formule de transformation inverse peut s'écrire, par exemple

$$\rho = \sqrt{x^2+y^2} \qquad \theta = \begin{cases} 2\,\mathrm{Arc\,tan}\left(\dfrac{y}{x+\sqrt{x^2+y^2}}\right) & \text{si } (x,y) \notin \mathbb{R}^{*-} \times \{0\}, \\ \pi & \text{sinon.} \end{cases}$$

☞ Difféomorphisme, Théorèmes d'*inversion.

Décomposition/factorisation polaire ☞ Décomposition.

Équation polaire d'une conique Équation donnée en représentation polaire d'une conique non dégénérée. ✦ Cette équation prend une forme particulièrement simple lorsque l'origine est choisie sur l'un des foyers de la conique et si l'axe Ox passe par le deuxième foyer (cas de l'ellipse et de l'hyperbole), ou est l'axe de symétrie (cas de la parabole). Dans ce cas, l'équation générale de la conique est

$$\rho(\theta) = \frac{p}{1+e\cos\theta}$$

où e est l'excentricité de la conique.

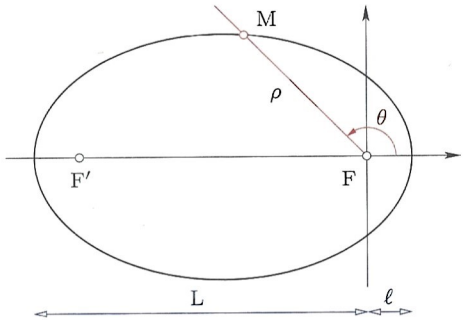


Fig. 79 — Représentation polaire d'une ellipse.

Exemple : L'orbite d'une planète, supposée de masse négligeable devant celle du soleil, et sans interaction avec le reste de l'univers, est une conique dont un des foyers est occupé par le soleil. Dans le cas d'une ellipse ($0 \leqslant e < 1$), le demi grand-axe vaut $p/(1-e^2)$, la distance minimale au soleil (la planète est au *périhélie*) vaut $L = p/(1+e)$ et la distance maximale est $\ell = p/(1-e)$ (la planète est alors à l'*aphélie* — prononcer [afeli]) .

Genre	Excentricité
Cercle	$e = 0$
Ellipse	$0 \leqslant e < 1$
Parabole	$e = 1$
Hyperbole	$e > 1$

TABLE 7 — Excentricité d'une conique en fonction de son genre.

Forme polaire d'une forme quadratique q Forme bilinéaire symétrique associée à la forme quadratique q par $q(x) = \varphi(x,x)$ pour tout $x \in E$. ✦ Elle est reliée à la forme q par les identités de *polarisation ; par exemple, dans le cas réel :

$$\varphi(x,y) = \frac{1}{4}\big[q(x+y) - q(x-y)\big] = \frac{1}{2}\big[q(x+y) - q(x) - q(y)\big].$$

☞ POLARISATION.

Partie polaire d'une fraction rationnelle ☞ DÉCOMPOSITION EN ÉLÉMENTS SIMPLES.

Repère polaire Dans le plan euclidien orienté, muni d'un repère orthonormé direct $(O, \boldsymbol{i}, \boldsymbol{j})$, on attache à tout point $M = (r\cos\theta, r\sin\theta)$ différent de l'origine, un repère orthonormé direct $(M, \boldsymbol{u}_r, \boldsymbol{u}_\theta)$, appelé repère polaire, défini par

$$\boldsymbol{u}_r = \cos\theta\,\boldsymbol{i} + \sin\theta\,\boldsymbol{j} \qquad \text{et} \qquad \boldsymbol{u}_\theta = -\sin\theta\,\boldsymbol{i} + \cos\theta\,\boldsymbol{j}.$$

✦ Ce repère est dit *mobile* car il varie avec le point M. ✦ Il est particulièrement adapté à l'étude d'une courbe du plan en coordonnées polaires, ainsi qu'à l'étude de la cinématique d'un point matériel dans un champ de force central.

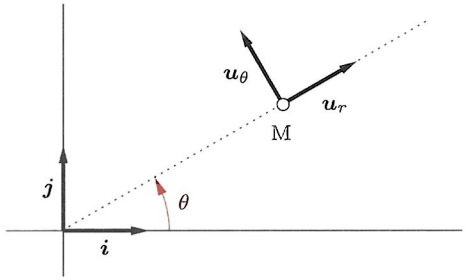


Fig. 80 — Repère polaire.

POLARISATION

Identités de polarisation Relations, toujours vraies, entre un produit scalaire φ et sa forme quadratique q associée. Ces relations permettent de retrouver le produit scalaire en ne connaissant que la forme q. ✦ Dans le cas d'un espace préhilbertien réel, on a

$$4\,\langle x|y\rangle = \|x+y\|^2 - \|x-y\|^2$$
$$2\,\langle x|y\rangle = \|x+y\|^2 - \|x\|^2 - \|y\|^2 .$$

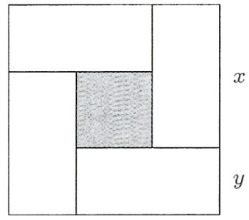
✦ Dans le cas d'un espace préhilbertien complexe, on a

$$4\mathscr{R}e\,\langle x|y\rangle = \|x+y\|^2 - \|x-y\|^2 \qquad 4\mathscr{I}m\,\langle x|y\rangle = \|x-\mathrm{i}y\|^2 - \|x+\mathrm{i}y\|^2$$

et donc

$$4\,\langle x|y\rangle = \|x+y\|^2 - \|x-y\|^2 + \mathrm{i}\,\|x-\mathrm{i}y\|^2 - \mathrm{i}\,\|x+\mathrm{i}y\|^2 .$$

REMARQUE : Dans le cas de la droite réelle, on peut trouver une jolie illustration graphique de l'identité de polarisation $4xy = (x+y)^2 - (x-y)^2$. Le grand carré est d'aire $(x+y)^2$ et le petit gris d'aire $(x-y)^2$.



PÔLE

Pôle d'une fraction rationnelle Soit $F \in \mathbb{K}(X)$ une fraction rationnelle, et choisissons un représentant irréductible (P, Q) de cette fraction. Un élément a du corps $\mathbb{K}$ est appelé pôle de F si c'est une racine de Q. ✦ Son ordre de *multiplicité en tant que pôle de F est son ordre de multiplicité en tant que racine de Q.

☞ FONCTION *RATIONNELLE.

POLYNÔME

Polynôme à une indéterminée Soit A un anneau commutatif. On définit, formellement, un polynôme à coefficients dans l'anneau A comme une suite $(a_n)_{n\in\mathbb{N}}$ à support fini (c'est-à-dire nulle à partir d'un certain rang). ✦ Si l'on munit l'ensemble des polynômes de l'addition et de la multiplication, définies pour deux polynômes $\mathrm{P} = (a_n)_{n\in\mathbb{N}}$ et $\mathrm{Q} = (b_n)_{n\in\mathbb{N}}$ par

$$\mathrm{P} + \mathrm{Q} = (a_n + b_n)_{n\in\mathbb{N}}$$

et

$$\mathrm{PQ} = (c_n)_{n\in\mathbb{N}} \qquad \text{où} \qquad c_n = \sum_{k=0}^{n} a_k\, b_{n-k},$$

on obtient un anneau commutatif, noté A[X]. ✦ Si on le munit de plus de la multiplication par un scalaire, on obtient l'algèbre des polynômes. ✦ Enfin, il est usuel de noter $\mathrm{X}^0 = 1 = (1, 0, 0, \dots)$, $\mathrm{X} = (0, 1, 0, \dots)$ et, de manière générale,

$$\mathrm{X}^k = (\delta_{k,n})_{n\in\mathbb{N}} = (0, 0, \dots, 0, \underset{\uparrow}{1}, 0, \dots)$$
$$k$$

Le polynôme $(a_0, a_1, \dots, a_n, 0, 0, \cdots)$ se note alors plus commodément

$$\mathrm{P} = \sum_{k=0}^{n} a_k\, \mathrm{X}^k.$$

✦ Si P est non nul, le plus grand entier n tel que a_n est non nul s'appelle le *degré* de P, et a_n est son *coefficient dominant.*

Remarque : Si A est un corps, alors l'anneau A[X] est principal.

☞ Degré, Dérivé, Relations coefficients-racines.

Polynôme à plusieurs indéterminées Si A est un anneau commutatif, l'anneau A[X] des polynômes à coefficients dans A est également un anneau commutatif. On peut donc définir $(\mathrm{A}[\mathrm{X}])[\mathrm{Y}]$, que l'on note plus commodément A[X, Y], qui est l'anneau des polynômes à deux indéterminées. Un polynôme de cet anneau est de la forme

$$\mathrm{P} = \sum_i \sum_j a_{ij}\, \mathrm{X}^i\, \mathrm{Y}^j$$

où la famille $(a_{ij})_{ij}$ est à support fini. ✦ De la même façon, on définit des polynômes à trois indéterminées, quatre, etc.

☞ Degré, Homogène.

Polynôme annulateur Soit E un $\mathbb{K}$-espace vectoriel. Soient u un endomorphisme de E et P un polynôme de $\mathbb{K}[\mathrm{X}]$. On dit que P annule u ou que P est un polynôme annulateur de u si $\mathrm{P}(u) = 0$. ✦ De même, si A une matrice carrée d'ordre n sur le corps $\mathbb{K}$. Un polynôme P est dit annulateur de A si $\mathrm{P}(\mathrm{A}) = 0$.

☞ Polynôme d'endomorphisme.

Polynôme caractéristique Soit $\mathrm{A} \in \mathfrak{M}_n(\mathbb{K})$. L'application $t \mapsto \det(\mathrm{A} - t\,\mathrm{I}_n)$ est un polynôme de $\mathbb{K}[\mathrm{X}]$ et de degré n, que l'on note symboliquement $\chi_{\mathrm{A}}(\mathrm{X}) = \det(\mathrm{A} - \mathrm{XI}_n)$, et on l'appelle polynôme caractéristique de A. ✦ Ses racines sont les scalaires λ tel que $\mathrm{A} - \lambda\,\mathrm{I}_n$ n'est pas inversible, c'est-à-dire les valeurs propres de A. ✦ Si E est un espace vectoriel de dimension finie et si $u \in \mathscr{L}(\mathrm{E})$, on définit de même $\chi_u(\mathrm{X}) = \det(u - \mathrm{X}\,\mathrm{Id})$. ✦ Si $\mathcal{B}$ est une base quelconque de E et si $\mathrm{A} = \mathrm{mat}_{\mathcal{B}}(u)$, alors $\chi_u = \chi_{\mathrm{A}}$.

☞ Cayley-Hamilton, Spectre.

Polynôme d'endomorphisme Si u est un endomorphisme d'un $\mathbb{K}$-espace vectoriel E, on appelle polynôme en u tout endomorphisme s'écrivant sous la forme d'une combinaison linéaire de puissances de u (au sens de la composition : $u^k = u \circ u \circ \cdots \circ u$). ✦ Si $\mathrm{P} = a_0 + a_1\,\mathrm{X} + \cdots + a_d\,\mathrm{X}^d$ est un polynôme de $\mathbb{K}[\mathrm{X}]$, on note

$$\mathrm{P}(u) = a_0\,\mathrm{Id}_{\mathrm{E}} + a_1\,u + \cdots + a_d\,u^d.$$

✦ On note $\mathbb{K}[u]$ l'algèbre des polynômes en u. ✦ Si $u \in \mathscr{L}(\mathrm{E})$ est fixé, l'application $\Phi_u : \mathbb{K}[\mathrm{X}] \to \mathbb{K}[u]$ définie par $\Phi_u(\mathrm{P}) = \mathrm{P}(u)$ est un morphisme d'algèbre.

☞ Théorème de *Hilbert-Dirac, Polynôme minimal.

Polynômes de Lagrange ☞ Lagrange.

Polynôme minimal Soit E un espace vectoriel de dimension finie. On appelle polynôme minimal d'un endomorphisme u, et on note μ_u, le générateur unitaire de l'idéal des polynômes annulateurs de u. ✦ En d'autres termes, μ_u est unitaire et, pour tout $\mathrm{P} \in \mathbb{K}[\mathrm{X}]$, P est annulateur de u si et seulement si P est multiple de μ_u.

Remarques : Les valeurs propres d'un endomorphisme sont les racines de son polynôme minimal. ✦ Un endomorphisme est diagonalisable si et seulement si son polynôme minimal est scindé à racines simples, et trigonalisable si et seulement si son polynôme minimal est scindé. ✦ Le polynôme minimal divise le polynôme caractéristique (théorème de Cayley-Hamilton). ✦ Le polynôme minimal et le polynôme caractéristique ont mêmes diviseurs irréductibles.

Polynôme normalisé Polynôme unitaire ou nul.

Polynômes orthogonaux Famille $(\mathrm{P}_n)_{n\in\mathbb{N}}$ de polynômes obtenus en orthogonalisant la base canonique pour un produit scalaire donné. ✦ C'est donc notamment une famille étagée en degré. ✦ Selon le produit scalaire choisi, on obtient évidemment des familles distinctes de polynômes. Très souvent, le produit scalaire choisi est de la forme

$$\langle \mathrm{P} | \mathrm{Q} \rangle = \int_{\mathrm{I}} \mathrm{P}(t)\,\mathrm{Q}(t)\,w(t)\,\mathrm{d}t,$$

où I est un intervalle et w une fonction continue et strictement positive sur I, appelée fonction de poids (*weight*).

Nom	I	$w(t)$
Hermite	$]-\infty\,;+\infty[$	e^{-t^2}
Laguerre	$[0\,;+\infty[$	e^{-t}
Legendre	$[-1\,;+1]$	1
Tchebychev	$]-1\,;+1[$	$1/\sqrt{1-t^2}$

Table 8 — Familles de polynômes orthogonaux.

✦ Les polynômes orthogonaux de ce type vérifient une relation de récurrence d'ordre 2 et sont solutions d'une équation différentielle d'ordre 2. ✦ De plus, le polynôme P_n, de degré n, possède n racines distinctes, toutes à l'intérieur de l'intervalle I.

☞ Hermite, Laguerre, Legendre, Tchebychev.

Polynôme scindé Polynôme $\mathrm{P} \in \mathbb{K}[\mathrm{X}]$ se factorisant sous la forme de produit de polynômes de degré 1 :

$$\mathrm{P} = a \prod_{k=1}^{n} (\mathrm{X} - \lambda_k)^{m_k}.$$

Exemple : $P = X^3 - 3X + 2 = (X-1)^2(X+2)$ est scindé dans $\mathbb{R}[X]$. ✦ $Q = X^2 - 2$ est scindé dans $\mathbb{R}[X]$ mais pas dans $\mathbb{Q}[X]$. ✦ $R = X^2 + 1$ n'est pas scindé dans $\mathbb{R}[X]$, mais l'est dans $\mathbb{C}[X]$. ✦ Tout polynôme complexe est scindé dans $\mathbb{C}[X]$. ☞ Théorème de d'*Alembert-Gauss.

Polynôme simplement scindé Polynôme scindé dont toutes les racines sont simples ; il peut donc se décomposer sous la forme

$$P = a \prod_{k=1}^{d} (X - \lambda_k),$$

où d est le degré de P et où les λ_k sont deux à deux distincts.

☞ Multiplicité.

Polynôme trigonométrique Application $P : \mathbb{R} \to \mathbb{C}$ telle qu'il existe $\omega > 0$, $n \in \mathbb{N}$ et une famille $(c_{-n}, \dots, c_0, \dots, c_{n-1}, c_n) \in \mathbb{C}^{2n+1}$ vérifiant

$$\forall t \in \mathbb{R} \qquad P(t) = \sum_{k=-n}^{n} c_k \, e^{ik\omega t}.$$

✦ ω est appelé la *pulsation* du polynôme, et $T = 2\pi/\omega$ est sa *période*. Un polynôme trigonométrique de période T est T-périodique.

☞ Weierstrass (2e théorème d'approximation).

Polynôme unitaire Polynôme dont le coefficient dominant vaut 1.

Algèbre des fonctions polynomiales sur $\mathbb{K}^n$ Algèbre des fonctions de la forme

$$P(x_1, \dots, x_n) = \sum_{k_1, \dots, k_n \in \mathbb{N}^n} a_{k_1, \dots, k_n} \, x_1^{k_1} \cdots x_n^{k_n},$$

c'est-à-dire, en notant $x = (x_1, \dots, x_n)$ et $k = (k_1, \dots, k_n)$, des combinaisons linéaires de monômes de la forme

$$M_k(x) = x_1^{k_1} \cdots x_n^{k_n}.$$

PONDÉRÉ

☞ Barycentre.

POSITIF

Endomorphisme symétrique (défini) positif Soit E un espace vectoriel euclidien. Un endomorphisme symétrique u est positif lorsque

$$\forall x \in E \qquad \langle x | u(x) \rangle \geqslant 0.$$

Il est défini positif lorsque $\langle x | u(x) \rangle$ n'est nul que pour $x = 0$:

$$\forall x \in E \setminus \{0\} \qquad \langle u(x) | x \rangle > 0.$$

On note $\mathscr{S}^+(E)$ l'ensemble des endomorphismes symétriques positifs de E, et $\mathscr{S}^{++}(E)$ celui des endomorphismes symétriques définis positifs.

Remarques : Ces propriétés peuvent être caractérisées par le spectre du u (qui, rappelons-le, est diagonalisable dans une base orthonormée) : u est positif si et seulement si $\mathrm{Sp}(u) \subset \mathbb{R}^+$, tandis que u est défini positif si et seulement si $\mathrm{Sp}(u) \subset \mathbb{R}^{*+}$. ✦ Si u est symétrique positif, il vérifie également la relation

$$\|u\| = \|u^*\| = \sup_{\|x\| \leqslant 1} \langle u(x) | x \rangle = \rho(u),$$

où $\rho(u)$ est le rayon spectral de u. ✦ Un endomorphisme u est dit *négatif* si $-u$ est positif, et *défini négatif* si $-u$ est défini positif.

☞ Rayleigh.

Forme bilinéaire (définie) positive ☞ Forme bilinéaire.

Matrice symétrique (définie) positive Une matrice symétrique $M \in S_n(\mathbb{R})$ est dite positive si

$$\forall X \in \mathfrak{M}_{n,1}(\mathbb{R}) \qquad {}^tXAX \geqslant 0$$

et définie positive si

$$\forall X \in \mathfrak{M}_{n,1}(\mathbb{R}) \setminus \{0\} \qquad {}^tXAX > 0.$$

✦ On note $S_n^+(\mathbb{R})$ l'ensemble des matrices positives, et $S_n^{++}(\mathbb{R})$ celui des matrices définies positives.

Remarque : Une matrice est symétrique (définie) positive si et seulement si elle est la matrice représentative, dans une base orthonormée, d'un endomorphisme symétrique (défini) positif d'un espace vectoriel euclidien. ✦ Par conséquent, une matrice symétrique est positive si et seulement si son spectre est inclus dans $\mathbb{R}^+$, et définie positive si et seulement si son spectre est inclus dans $\mathbb{R}^{*+}$.

☞ Endomorphisme *positif.

Partie positive ☞ Partie.

PPCM

PPCM de deux entiers a et b Générateur positif, noté $a \vee b$, de l'idéal $a\mathbb{Z} \cap b\mathbb{Z}$. ✦ Notamment, $a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}$. ✦ C'est également le plus petit multiple positif commun à a et à b (plus petit au sens de la divisibilité).

PPCM de deux polynômes A et B Générateur normalisé de l'idéal $A\mathbb{K}[X] \cap B\mathbb{K}[X]$. ✦ Notamment, $A\mathbb{K}[X] \cap B\mathbb{K}[X] = (A \vee B)\mathbb{K}[X]$. ✦ C'est également le plus petit (au sens de la divisibilité) multiple normalisé commun à A et à B.

☞ Bézout, Générateur, Idéal, PGCD.

PRÉHILBERTIEN

Espace préhilbertien réel Espace vectoriel réel muni d'une forme bilinéaire symétrique définie positive (produit scalaire).

Exemple : L'espace E des fonctions continues sur $[a\,;\,b]$ et à valeurs réelles, muni du produit scalaire défini par $\langle f | g \rangle = \int_a^b fg$, est un espace préhilbertien réel.

Espace préhilbertien complexe Espace vectoriel complexe muni d'une forme sesquilinéaire, à symétrie hermitienne, définie positive (produit scalaire).

Exemple : L'espace E des fonctions continues sur $[a\,;\,b]$ et à valeurs complexes, muni du produit scalaire défini par $\langle f | g \rangle = \int_0^1 f\bar{g}$, est un espace préhilbertien complexe.

☞ Produit scalaire, Espace *hermitien.

PREMIER

Décomposition en facteurs premiers ☞ Décomposition.

Entier premier Entier naturel différent de 1, et n'admettant aucun autre diviseur que 1 et lui-même. ✦ C'est donc un entier naturel admettant exactement deux diviseurs. ✦ On note parfois $\mathbb{P}$ ou $\mathcal{P}$ l'ensemble des nombres premiers. ✦ Un entier qui n'est pas premier est dit *composé*.

Remarques : L'ensemble des nombres premiers est infini. ✦ Un nombre premier p divise un produit ab si, et seulement si, il divise l'un des facteurs. ☞ Gauss. ✦ La série $\sum 1/p$, où

p parcourt l'ensemble des entiers premiers, est divergente. Sa divergence est extrêmement lente, puisque

$$\sum_{\substack{p\in\mathbb{P}\\ p\leqslant n}} \frac{1}{p} \underset{n\to\infty}{\sim} \ln(\ln n).$$

✦ Le nombre $\pi(n)$ des nombres premiers inférieurs ou égaux à n est équivalent à $n/\ln n$ lorsque $n \to \infty$ ☞ Théorème des nombres *premiers. ✦ La notion de nombre premier se généralise aux polynômes ☞ Polynôme *irréductible.

☞ Décomposition en facteurs premiers, PGCD, PPCM.

Entiers premiers entre eux Deux entiers a et b sont premiers entre eux si les seuls diviseurs communs à a et à b sont -1 et $+1$, c'est-à-dire si $a \wedge b = 1$. ✦ Les entiers a et b sont premiers entre eux si, et seulement si, ils vérifient l'identité de Bézout : il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$. ✦ Synonyme : entiers *étrangers*.

Exemples : Les entiers 21 et 10 sont premiers entre eux. ✦ En revanche, 21 et 18 ne le sont pas, car ils admettent 3 comme facteur commun.

☞ Bézout, Gauss, PGCD.

Entiers premiers entre eux dans leur ensemble Entiers $a_1, \ldots, a_n$ dont les seuls diviseurs communs sont -1 et $+1$.

Polynômes premiers entre eux Deux polynômes P et Q non nuls sont dits premiers entre eux si les seuls diviseurs communs à P et Q sont les polynômes de degré 0 (polynôme constants non nuls). ✦ Autrement dit, ils sont premiers entre eux si et seulement si $\mathrm{P} \wedge \mathrm{Q} = 1$.

Exemple : $(\mathrm{X}^2 + 1)$ et $(\mathrm{X} - 3)(\mathrm{X} - 2)$ sont premiers entre eux dans $\mathbb{R}[\mathrm{X}]$.

Remarque : Si P et Q sont deux polynômes complexes non nuls, alors ils sont premiers entre eux si, et seulement si, ils ne possèdent pas de racine commune. ✦ Cette propriété ne se généralise pas à $\mathbb{R}[\mathrm{X}]$: ainsi, $\mathrm{P} = (\mathrm{X}^2 + 1)$ et $\mathrm{Q} = (\mathrm{X}^2 + 1)^2$ ne partagent aucune racine commune (ils n'ont aucune racine réelle) mais ne sont pas premiers entre eux : P est un diviseur commun à P et Q.

☞ Bézout, PGCD.

Théorème des nombres premiers Notons $\pi(n)$ le nombre d'entiers premiers inférieurs ou égaux à n. Les mathématiciens *Gauss et *Legendre ont conjecturé que $\pi(n) \sim n/\ln n$; il fallut attendre la toute fin du XIXe siècle pour que les mathématiciens français *Hadamard et de La Vallée-Poussin démontrent, indépendamment, en 1896, cette conjecture, dans un véritable tour de force analytique. ✦ En 1914, le mathématicien anglais Littlewood, remarquant que la fonction *logarithme-intégral $\mathrm{Li}(x)$ donne un équivalent de meilleure qualité de $\pi(x)$, étudia la différence des deux quantités et prouva que $\pi(n) - \mathrm{Li}(n)$ change de signe une infinité de fois. Ce résultat est d'autant plus remarquable que Gauss avait conjecturé que $\pi(n)$ était toujours strictement inférieur à $\mathrm{Li}(n)$, et que, jusqu'à $n = 10^8$, on sait que cette inégalité stricte est toujours vérifiée.

Remarque : Ce théorème est profondément lié à d'autres branches (apparemment éloignées) des mathématiques, et notamment à la répartition des zéros de la fonction ζ de Riemann. ☞ Zeta.

PRESQUE NULLE

Une famille $(x_i)_{i\in\mathrm{I}}$ de vecteurs est dite presque nulle, ou *à support fini*, lorsqu'il n'existe qu'un nombre fini d'indices i tels que $x_i \neq 0$. ✦ Si l'on note $(i_1, \ldots, i_n)$ le support de cette famille (ensemble des indices i tels que $x_i \neq 0$), alors on pose

$$\sum_{i\in\mathrm{I}} x_i = \sum_{k=1}^{n} x_{i_k}.$$

C'est donc, malgré l'écriture, une somme finie, qui est parfaitement définie.

Exemple : Un polynôme s'écrit sous la forme $\mathrm{P} = \sum_{n=0}^{\infty} a_n X^n$, où $(a_n)_{n\in\mathbb{N}}$ est une suite presque nulle de complexes ; on peut écrire, par exemple, $\mathrm{P}(1) = \sum_{n=0}^{\infty} a_n$.

☞ Support.

PRESQUE SÛR

Un événement est dit presque sûr lorsqu'il est de probabilité 1. ✦ Une propriété est vraie presque sûrement lorsque sa réalisation est un événement de probabilité 1. ✦ Synonyme : *quasi certain*.

Exemple : Une variable aléatoire X est dite presque sûrement positive si $\mathbf{P}[\mathrm{X} \geqslant 0] = 1$.

Convergence presque sûrement Une suite $(\mathrm{X}_n)_{n\in\mathbb{N}}$ de variables aléatoires converge presque sûrement vers une variable aléatoire X si la suite numérique $\big(\mathrm{X}_n(\omega)\big)_{n\in\mathbb{N}}$ converge vers $\mathrm{X}(\omega)$ pour presque tout ω de Ω. ✦ En d'autres termes, il existe une partie N de Ω telle que $\mathbf{P}(\mathrm{N}) = 0$ et telle que, pour tout $\omega \in \Omega \setminus \mathrm{N}$, on ait $\lim_{n\to\infty} \mathrm{X}_n(\omega) = \mathrm{X}(\omega)$.

☞ Loi forte des *grands nombres.

PRIMITIVE

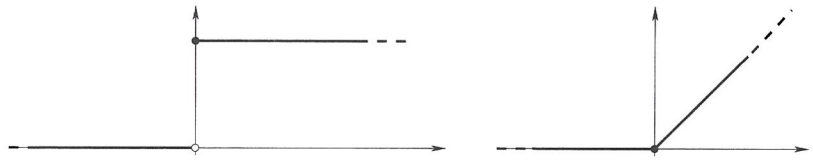
Primitive d'une fonction continue f Soit $f : \mathrm{I} \to \mathrm{E}$ une fonction continue, définie sur un intervalle I et à valeurs dans un espace vectoriel normé E ; une primitive de f est une fonction F définie et dérivable sur I, dont la dérivée est $\mathrm{F}' = f$. ✦ Si $a \in \mathrm{I}$, toute primitive de f est de la forme $x \mapsto \int_a^x f(t)\,\mathrm{d}t + \mathrm{C}^{\text{te}}$. ✦ Notamment, l'application $x \mapsto \int_a^x f(t)\,\mathrm{d}t$ est l'unique primitive de f qui s'annule en a. ✦ Alors, pour tout $b \in \mathrm{I}$, $\int_a^b f(t)\,\mathrm{d}t = \mathrm{F}(b) - \mathrm{F}(a)$.

Remarque : Si $f : \mathrm{I} \to \mathrm{E}$ est une fonction quelconque, une primitive de f est une fonction $\mathrm{F} : \mathrm{I} \to \mathrm{E}$, dérivable, et telle que $\mathrm{F}' = f$. Une telle primitive n'existe pas toujours dans ce sens restreint (mais on peut élargir la notion de primitive pour des fonctions continues par morceaux, voir ci-dessous). Si elle existe, elle n'est même pas forcément donnée par la fonction $x \mapsto \int_*^x f$ en gardant le sens habituel de l'intégrale (intégrale de Riemann, ou de Lebesgue). Toutefois, d'autres constructions de l'intégrale (celle de Denjoy-Kurzweil-Henstock notamment) permettent d'assurer cette propriété.

☞ Théorème *fondamental de l'analyse, Intégral.

Primitive d'une fonction continue par morceaux Si $f : \mathrm{I} \to \mathrm{E}$ est continue par morceaux sur l'intervalle I, une primitive de f est une fonction F *continue* sur I, et telle que, en tout point $x \in \mathrm{I}$ en lequel f est continue, F est dérivable et vérifie $\mathrm{F}'(x) = f(x)$. ✦ Si $a \in \mathrm{I}$, toute primitive de f est de la forme $x \mapsto \int_a^x f(t)\,\mathrm{d}t + \mathrm{C}^{\text{te}}$.

Exemple : Une primitive de la fonction de Heaviside définie par $\mathrm{H}(t) = 0$ si $t < 0$ et $\mathrm{H}(t) = 1$ si $t \geqslant 1$ est la fonction F définie par $\mathrm{F}(t) = 0$ si $t \leqslant 0$ et $\mathrm{F}(t) = t$ si $t \geqslant 1$.



Primitive d'une forme différentielle ω Si ω est une forme différentielle exacte sur un ouvert U de $\mathbb{R}^n$, toute fonction $f : \mathbb{R}^n \to \mathbb{R}$ dont la différentielle $\mathrm{d}f$ est égale à ω est appelée primitive de ω.

Remarque : Si U est connexe par arcs, toutes les primitives de ω diffèrent d'une constante. Dans le cas contraire, on peut choisir une constante par composante connexe par arc de ω.

Exemple : Si $\omega(x,y) = 2xy\,\mathrm{d}x + (x^2+3y^2)\,\mathrm{d}y$, une primitive de ω est $f(x,y) = x^2y + y^3 + C^{\text{te}}$ sur $\mathbb{R}^2$ tout entier.

PRINCIPAL

Anneau principal ☞ ANNEAU.

Idéal principal ☞ IDÉAL.

Inconnues principales ☞ PIVOT.

PRINCIPE

☞ LEMME DES BERGERS, RÉCURRENCE, TIROIRS, ZÉROS ISOLÉS.

PROBABILISABLE

Espace probabilisable Couple $(\Omega, \mathscr{T})$, où Ω est un ensemble, appelé *espace des épreuves* ou *univers* (des possibles), et $\mathscr{T}$ est la *tribu des événements*, c'est-à-dire un ensemble de parties de Ω, dont sont éléments Ω et l'ensemble vide, stable par passage au complémentaire et par union dénombrable. Autrement dit,

$$\mathscr{T} \subset \mathfrak{P}(\Omega), \qquad \Omega \in \mathscr{T}, \qquad \varnothing \in \mathscr{T}, \qquad \forall A \in \mathscr{T} \quad A^c \in \mathscr{T}$$

et, pour toute suite $(A_n)_{n\in\mathbb{N}}$ à valeurs dans $\mathscr{T}$, $\bigcup_{n\in\mathbb{N}} A_n$ est élément de $\mathscr{T}$. ✦ Un élément de $\mathscr{T}$ est appelé *événement* (un tel élément est donc une partie de Ω). Un élément $\omega \in \Omega$ est parfois appelé *épreuve*, ou *résultat de l'expérience* Ω, et un événement de la forme $\{\omega\}$ est appelé *événement atomique*. ✦ Lorsqu'une épreuve ω est élément d'un événement $A \in \mathscr{T}$, on dit qu'elle *réalise* l'événement A.

REMARQUE : Lorsque l'on définit un espace probabilisable, on doit choisir un ensemble de parties de Ω sur lequel définir une probabilité. Si Ω est un ensemble fini ou dénombrable, inutile de se poser des questions métaphysiques, il suffit de prendre l'ensemble de *toutes* les parties de Ω : $\mathscr{T} = \mathfrak{P}(\Omega)$ ✦ Lorsque Ω n'est pas dénombrable, il est nécessaire (pour des raisons techniques) de restreindre ce choix. Notamment, si l'on veut décrire des événements du type $X \in A$, où X est une variable aléatoire et A une partie de $\mathbb{R}$, il est nécessaire, pour les mêmes raisons, de restreindre le choix des ensembles A que l'on peut considérer. En pratique, cette restriction n'empêche personne de respirer : tout ce que l'on peut construire à partir des intervalles avec des unions ou des intersections dénombrables et des passages au complémentaire est autorisé ! Les parties A acceptables au sens précédent forment ce qu'on appelle la *tribu des boréliens*.

☞ ÉVÉNEMENT.

PROBABILISÉ

Espace probabilisé Encore appelé *espace probabiliste*. Triplet $(\Omega, \mathscr{T}, \mathbf{P})$ où $(\Omega, \mathscr{T})$ est un espace probabilisable et $\mathbf{P}$ une probabilité sur $(\Omega, \mathscr{T})$.

PROBABILITÉ

Soit $(\Omega, \mathscr{T})$ un espace probabilisable. Une application $\mathbf{P} : \mathscr{T} \to [0\,;1]$ est une probabilité sur $(\Omega, \mathscr{T})$ si $\mathbf{P}(\Omega) = 1$ et si elle est σ-additive : pour toute famille dénombrable $(A_n)_{n\in\mathbb{N}}$ d'événements de $\mathscr{T}$ deux à deux disjoints,

$$\mathbf{P}\Big(\bigcup_{n\in\mathbb{N}} A_n\Big) = \sum_{n\in\mathbb{N}} \mathbf{P}(A_n). \qquad (\sigma\text{-additivité})$$

✦ $(\Omega, \mathscr{T}, \mathbf{P})$ est un *espace probabilisé*. ✦ Notamment, $\mathbf{P}(A^c) = 1 - \mathbf{P}(A)$ pour tout événement A et, en particulier, $\mathbf{P}(\varnothing) = 0$.

REMARQUE : La σ-additivité est une extension de la notion d'additivité (si $A \cap B = \varnothing$, alors $\mathbf{P}(A \cup B) = \mathbf{P}(A) + \mathbf{P}(B)$) au cas dénombrable. On ne peut en revanche pas l'étendre au cas non dénombrable. Par exemple, si X est une variable aléatoire suivant la loi uniforme $\mathscr{U}([0\,;1])$, alors $\mathbf{P}[X \in [0\,;1]] = 1$, mais $\mathbf{P}[X = x] = 0$ pour tout $x \in [0\,;1]$, donc

$$\mathbf{P}\Big(\bigcup_{x\in[0\,;1]} [X = x]\Big) \neq \text{« } \sum_{x\in[0\,;1]} \mathbf{P}[X = x] \text{ »}$$

(avec des guillemets car la notion n'est pas correctement définie !)

Formule des probabilités composées Soient A et B deux événements. On suppose que $\mathbf{P}(A) \neq 0$; alors $\mathbf{P}(A \cap B) = \mathbf{P}(A) \cdot \mathbf{P}_A(B)$. ✦ Plus généralement, si $A_1, \ldots, A_n$ sont des événements de probabilité non nulle, alors

$$\mathbf{P}(A_1 \cap \cdots \cap A_n) = \mathbf{P}(A_1) \cdot \mathbf{P}_{A_1}(A_2) \cdots \mathbf{P}_{A_1\cap\cdots\cap A_{n-1}}(A_n).$$

Probabilité conditionnelle Soit $(\Omega, \mathscr{T}, \mathbf{P})$ un espace probabilisé. Soit A un événement de probabilité non nulle. Alors l'application $\mathbf{P}_A$ définie sur $\mathscr{T}$ par

$$\mathbf{P}_A : B \longmapsto \frac{\mathbf{P}(A \cap B)}{\mathbf{P}(A)}$$

est une probabilité sur $(\Omega, \mathscr{T})$, appelée *probabilité conditionnée par* A. ✦ Si B est un événement, alors $\mathbf{P}_A(B)$ s'appelle probabilité de B conditionnée par A ou *probabilité de* B *sachant* A. ✦ On la note également $\mathbf{P}(A \mid B)$.

☞ INDÉPENDANCE.

Formule des probabilités totales Soient $(A_n)_{n\in\mathbb{N}}$ un système complet ou quasi complet d'événements, et B un événement. Alors

$$\mathbf{P}(B) = \sum_{n=0}^{\infty} \mathbf{P}(A_n \cap B). \qquad \textit{(forme 1)}$$

Si de plus $\mathbf{P}(A_n) > 0$ pour tout $n \in \mathbb{N}$, alors

$$\mathbf{P}(B) = \sum_{n=0}^{\infty} \mathbf{P}(A_n)\, \mathbf{P}_{A_n}(B) \qquad \textit{(forme 2)}$$

PROBLÈME

Problème de Cauchy ☞ CAUCHY.

PRODUIT

Produit cartésien Soient A et B deux ensembles. Le produit cartésien de A et B est

$$A \times B = \big\{(a,b)\ ;\ a \in A \text{ et } b \in B\big\}.$$

REMARQUES : Si E et F sont deux espaces vectoriels, alors $E \times F$ est muni d'une structure naturelle d'espace vectoriel, l'addition et la multiplication par un scalaire étant

$$(a,b) + (a',b') = (a+a', b+b') \qquad \text{et} \qquad \lambda(a,b) = (\lambda a, \lambda b).$$

✦ Si E et F sont tous deux de dimension finie, alors $E \times F$ est également de dimension finie et $\dim E \times F = \dim E + \dim F$.

☞ TOPOLOGIE PRODUIT.

Produit de Cauchy ☞ CAUCHY.

Produit de composition ☞ COMPOSITION.

Produit de convolution ☞ CONVOLUTION.

Produit infini Soit $(u_n)_{n\in\mathbb{N}}$ une suite de complexes tous non nuls. On note, pour tout entier n, $\mathrm{P}_n = \prod_{k=0}^{n} u_k$. On dit que le produit infini $\prod u_n$ converge si la suite $(\mathrm{P}_n)_{n\in\mathbb{N}}$ admet une limite *non nulle* et, dans ce cas, on note

$$\prod_{n=0}^{\infty} u_n = \lim_{n\to\infty} \prod_{k=0}^{n} u_k.$$

REMARQUE : Si $(a_n)_{n\in\mathbb{N}}$ est une suite réelle qui tend vers 0, il existe un entier $\mathrm{N} \geqslant 1$ à partir duquel $u_n = 1 + a_n > 0$; la suite $(\mathrm{P}_n)_{n\geqslant \mathrm{N}}$ est alors de signe constant ; on écrit alors

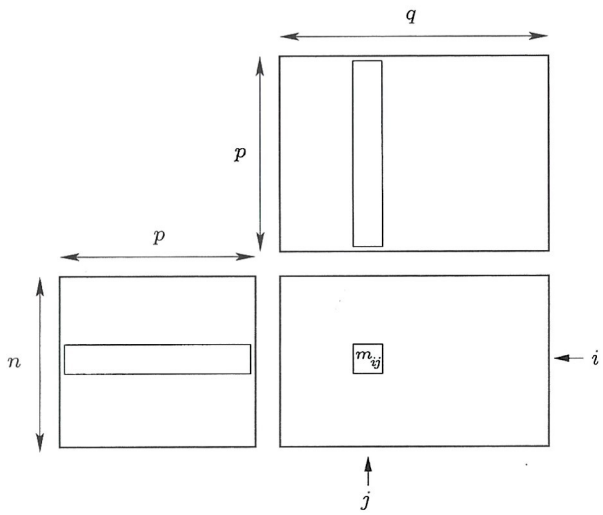
$$\forall n \geqslant \mathrm{N} \qquad \mathrm{P}_n = \mathrm{P}_{\mathrm{N}-1} \cdot \prod_{k=\mathrm{N}}^{n} (1 + a_k)$$

et on prend le logarithme de $\mathrm{P}_n/\mathrm{P}_{\mathrm{N}-1}$: l'étude de la convergence du produit est alors ramenée à l'étude de la série $\sum_{n\geqslant \mathrm{N}} \ln(1 + a_k)$.

Produit de Kronecker ☞ KRONECKER.

Produit matriciel Soient A une (n, p)-matrice, et B une (p, q)-matrice sur le même corps commutatif $\mathbb{K}$. Le produit de A par B est la (n, q)-matrice $\mathrm{M} = (m_{ij})_{ij}$ définie par

$$\forall (i,j) \in [\![1\,;\,n]\!] \times [\![1\,;\,q]\!] \qquad m_{ij} = \sum_{k=1}^{p} a_{ik}\, b_{kj}.$$



✦ Ce produit matriciel permet notamment de représenter le produit de composition d'applications linéaires. Si E, F et G sont des espaces vectoriels de dimensions respectives q, p et n, munis de bases $\mathcal{B}$, $\mathcal{C}$ et $\mathcal{D}$, si $u \in \mathscr{L}(\mathrm{E}, \mathrm{F})$ et si $v \in \mathscr{L}(\mathrm{F}, \mathrm{G})$, et si l'on note $\mathrm{U} = \mathrm{mat}_{\mathcal{B},\mathcal{C}}(u)$ et $\mathrm{V} = \mathrm{mat}_{\mathcal{C},\mathcal{D}}(v)$, alors la matrice représentative de $v \circ u$ dans les bases $\mathcal{B}$ et $\mathcal{D}$ est

$$\underset{\mathcal{B},\mathcal{D}}{\mathrm{mat}}(v \circ u) = \mathrm{VU}.$$

Produit mixte Soient $\boldsymbol{u}$, $\boldsymbol{v}$, $\boldsymbol{w}$ trois vecteurs de l'espace euclidien orienté $\mathbb{R}^3$. Leur produit mixte est

$$[\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w}] \overset{\text{déf.}}{=} \mathrm{Det}(\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w}) = \boldsymbol{u} \cdot (\boldsymbol{v} \wedge \boldsymbol{w}).$$

✦ Il mesure algébriquement le volume du parallélépipède engendré par les trois vecteurs $\boldsymbol{u}$, $\boldsymbol{v}$ et $\boldsymbol{w}$.

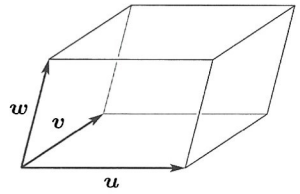


Fig. 81 — Parallélépipède engendré par les vecteurs $\boldsymbol{u}$, $\boldsymbol{v}$ et $\boldsymbol{w}$.

☞ DÉTERMINANT, PRODUIT VECTORIEL.

Produit scalaire Un produit scalaire sur un espace vectoriel réel E est une forme bilinéaire symétrique définie positive, c'est-à-dire une application $\varphi : \mathrm{E} \times \mathrm{E} \to \mathbb{R}$ linéaire par rapport à chaque variable, et telle que :

- $\varphi(x, y) = \varphi(y, x)$ pour tous $x, y \in \mathrm{E}$;
- $\varphi(x, x) \geqslant 0$ pour tout $x \in \mathrm{E}$;
- $\varphi(x, x) = 0$ si et seulement si $x = 0$.

Exemples : L'espace $\mathscr{C}([0\,;\,1], \mathbb{R})$ des fonctions continues sur $[0\,;\,1]$ et à valeurs réelles peut être muni du produit scalaire défini par $\langle f|g\rangle = \int_0^1 fg$. ✦ Si $a_0, \ldots, a_n$ sont des réels distincts, l'espace $\mathbb{R}_n[\mathrm{X}]$ peut être muni du produit scalaire $\langle \mathrm{P}|\mathrm{Q}\rangle = \sum_{k=0}^{n} \mathrm{P}(a_k)\,\mathrm{Q}(a_k)$. Pour ce produit scalaire, la famille $(\mathrm{L}_0, \ldots, \mathrm{L}_n)$ de polynômes élémentaires de *Lagrange est orthonormée.

Produit scalaire hermitien Soit E un $\mathbb{C}$-espace vectoriel. On appelle produit scalaire hermitien sur E toute application $\varphi : \mathrm{E} \times \mathrm{E} \to \mathbb{C}$ telle que

- φ est une forme *sesquilinéaire* : linéaire à droite, mais *semi-linéaire* (ou : *anti-linéaire*) à gauche : $\varphi(\lambda x + x', y) = \overline{\lambda}\,\varphi(x, y) + \varphi(x', y)$.
- φ est à *symétrie hermitienne* : $\varphi(y, x) = \overline{\varphi(x, y)}$;
- $\varphi(x, x) \geqslant 0$ pour tout $x \in \mathrm{E}$;
- $\varphi(x, x) = 0$ si et seulement si $x = 0$.

Exemples : L'espace $\mathscr{C}([0\,;\,1], \mathbb{C})$ des fonctions continues sur $[0\,;\,1]$ et à valeurs complexes peut être muni du produit scalaire défini par $\langle f|g\rangle = \int_0^1 \overline{f}g$. ✦ L'espace $\mathrm{E} = \ell^2(\mathbb{N})$ des suites complexes $(u_n)_{n\in\mathbb{N}}$ telles que $\sum |u_n|^2$ converge est muni de sa structure préhilbertienne canonique en posant $\langle u|v\rangle = \sum_{n=0}^{\infty} \overline{u_n}\, v_n$ pour toutes suites u et v de E. (☞ ℓ^2.)

Produit tensoriel Un cas particulier de produit tensoriel est le produit de Kronecker. ☞ KRONECKER.

Produit vectoriel Soient $\boldsymbol{x}$ et $\boldsymbol{y}$ deux vecteurs de l'espace euclidien orienté $\mathbb{R}^3$. Leur produit vectoriel $\boldsymbol{u} = \boldsymbol{x} \wedge \boldsymbol{y}$ est l'unique vecteur tel que $\langle \boldsymbol{u}|\boldsymbol{z}\rangle = \mathrm{Det}(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z})$ pour tout $\boldsymbol{z} \in \mathbb{R}^3$. ✦ Il vérifie notamment $\boldsymbol{x} \wedge \boldsymbol{y} = -\boldsymbol{y} \wedge \boldsymbol{x}$ et

$$\|\boldsymbol{x} \wedge \boldsymbol{y}\| = \|\boldsymbol{x}\|\,\|\boldsymbol{y}\|\,\big|\sin(\widehat{\boldsymbol{x}, \boldsymbol{y}})\big|.$$

✦ Dans une base orthonormée directe, si $\boldsymbol{x}$ a pour coordonnées (x, y, z) et si $\boldsymbol{x}'$ a pour coordonnées (x', y', z'), alors $\boldsymbol{x} \wedge \boldsymbol{y}$ a pour coordonnées

$$(yz' - y'z\ ,\ zx' - z'x\ ,\ xy' - x'y).$$

✦ Le vecteur $\boldsymbol{x} \wedge \boldsymbol{y}$ est orthogonal à la fois à $\boldsymbol{x}$ et à $\boldsymbol{y}$.

☞ PRODUIT MIXTE.

Norme produit ☞ NORME.

Topologie produit ☞ TOPOLOGIE.

PROJECTION/PROJECTEUR

Soit E un espace vectoriel, et soient V et W deux sous-espaces supplémentaires dans E : $\mathrm{E} = \mathrm{V} \oplus \mathrm{W}$. Tout vecteur $x \in \mathrm{E}$ se décomposant de manière unique dans la somme directe $\mathrm{V} \oplus \mathrm{W}$, si l'on note $x = v + w$, on pose alors $p(x) = v$. L'application $p : x \mapsto v$ ainsi définie est appelée *projection* sur V parallèlement à W. Elle vérifie notamment

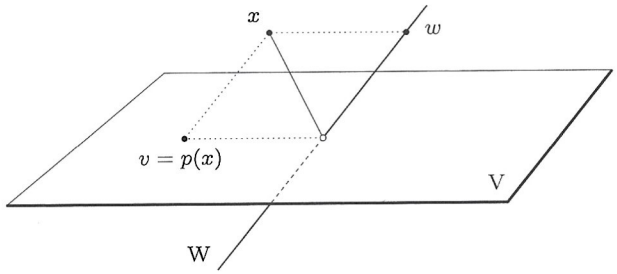
$$\mathrm{V} = \operatorname{Im} p \qquad \mathrm{W} = \operatorname{Ker} p \qquad \text{et} \qquad p \circ p = p.$$

✦ Tout endomorphisme $p \in \mathscr{L}(\mathrm{E})$ vérifiant $p \circ p = p$ est appelé *projecteur*. ✦ Son noyau et son image sont supplémentaires : $\mathrm{E} = \operatorname{Im} p \oplus \operatorname{Ker} p$. La décomposition d'un vecteur x sur cette somme directe est simplement $x = p(x) + \big[x - p(x)\big]$. ✦ Géométriquement, un projecteur p est la projection sur $\operatorname{Im} p$, parallèlement à $\operatorname{Ker} p$. ✦ Parfois, les mots « projection » (notion géométrique) et « projecteur » (notion algébrique) sont employés l'un pour l'autre.

REMARQUES : Si E est de dimension finie, la matrice représentative de p dans une base adaptée à la décomposition $\mathrm{E} = \operatorname{Im} p \oplus \operatorname{Ker} p$ est de la forme

$$\begin{pmatrix} \mathrm{I}_r & 0 \\ 0 & 0 \end{pmatrix}.$$

✦ Notamment, le rang d'un projecteur est égal à sa trace : $\operatorname{rg} p = \operatorname{tr} p$. ✦ Si E est un espace vectoriel quelconque et p un projecteur de E, traduire l'hypothèse « $x \in \operatorname{Im} p$ » par « il existe $y \in \mathrm{E}$ tel que $x = p(y)$ » est juste, mais maladroit : il vaut bien mieux écrire directement $x = p(x)$.

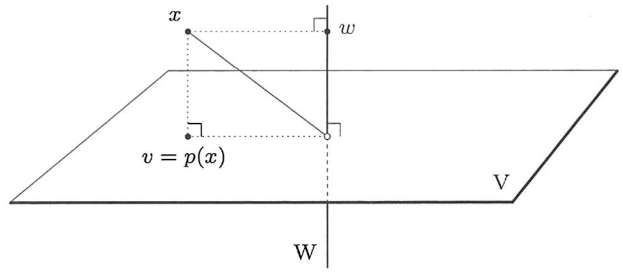


Projection orthogonale D'un point de vue géométrique, considérons un espace préhilbertien E ; une projection orthogonale est une projection sur un sous-espace vectoriel V, parallèlement à un sous-espace vectoriel W tel que $\mathrm{W} \perp \mathrm{V}$. Les espaces V et W sont alors supplémentaires orthogonaux. ✦ D'un point de vue algébrique, un projecteur orthogonal est un projecteur de E qui est également un endomorphisme symétrique, c'est-à-dire vérifiant $\big\langle p(x) \big| y \big\rangle = \big\langle x \big| p(y) \big\rangle$ pour tous $x, y \in \mathrm{E}$. C'est un projecteur caractérisé par la relation

$$\mathrm{E} = \operatorname{Ker} p \overset{\perp}{\oplus} \operatorname{Im} p.$$

✦ Si E est un espace euclidien, un projecteur orthogonal est un endomorphisme caractérisé par les relations $p = p^* = p^2$.

Exemple : Soit $n \in \mathbb{N}^*$. L'espace $\mathrm{E} = \mathfrak{M}_n(\mathbb{R})$ des matrices carrées d'ordre n peut être muni du produit scalaire $\langle \mathrm{M} | \mathrm{N} \rangle = \operatorname{tr}({}^{\mathrm{t}}\mathrm{M}\mathrm{N})$. Alors E est somme directe orthogonale du sous-espace vectoriel $\mathrm{S}_n(\mathbb{R})$ des matrices symétriques et du sous-espace vectoriel $\mathrm{A}_n(\mathbb{R})$ des matrices antisymétriques. L'application $\mathrm{M} \mapsto \frac{1}{2}(\mathrm{M} + {}^{\mathrm{t}}\mathrm{M})$ est le projecteur orthogonal sur $\mathrm{S}_n(\mathbb{R})$, parallèlement à $\mathrm{A}_n(\mathbb{R})$.



Famille de projecteurs associée à une somme directe Soit E un espace vectoriel, soient $\mathrm{E}_1, \dots, \mathrm{E}_k$ des sous-espaces vectoriels de E tels que

$$\mathrm{E} = \bigoplus_{i=1}^{k} \mathrm{E}_i.$$

Tout vecteur x de E peut se décomposer de manière unique dans cette somme directe :

$$x = \sum_{i=1}^{k} x_i \qquad x_i \in \mathrm{E}_i.$$

Pour tout $i \in [\![1\,;\,k]\!]$, l'application $p_i : x \mapsto x_i$ est un projecteur, d'image E_i et de noyau $\bigoplus_{j \neq i} \mathrm{E}_j$. La famille $p_1, \dots, p_k$ de projecteurs vérifie $\sum_{i=1}^{k} p_i = \mathrm{Id}_{\mathrm{E}}$ et $p_i \circ p_j = \delta_{ij}\, p_j$ pour tout $(i, j) \in [\![1\,;\,k]\!]^2$.

Famille de projecteurs associée à un endomorphisme diagonalisable Soit E un espace vectoriel de dimension finie n et soit $u \in \mathscr{L}(\mathrm{E})$ un endomorphisme diagonalisable. La famille de projecteurs associée à u est la famille de projecteurs associée à la somme directe $\mathrm{E} = \bigoplus_{\lambda \in \operatorname{Sp} u} \mathrm{E}_\lambda(u)$. ✦ Si $\mathcal{B}$ est une base propre dans laquelle la matrice de u est de la forme diagonale par blocs :

$$\underset{\mathcal{B}}{\operatorname{mat}}(u) = \begin{pmatrix} \lambda_1 \mathrm{I}_{d_1} & & \\ & \lambda_2 \mathrm{I}_{d_2} & \\ & & \ddots \\ & & & \lambda_k \mathrm{I}_{d_k} \end{pmatrix}$$

alors les projecteurs $\mathrm{P}_1, \dots, \mathrm{P}_k$ ont pour matrices, dans cette même base :

$$\mathrm{P}_1 = \begin{pmatrix} \mathrm{I}_{d_1} & & \\ & 0 & \\ & & \ddots \\ & & & 0 \end{pmatrix} \qquad \cdots \qquad \mathrm{P}_k = \begin{pmatrix} 0 & & \\ & \ddots & \\ & & 0 \\ & & & \mathrm{I}_{d_k} \end{pmatrix}.$$

Théorème de projection orthogonale Soit F un sous-espace vectoriel de dimension finie d'un espace préhilbertien E. Alors $F^\perp$ est un supplémentaire orthogonal de F : $E = F \overset{\perp}{\oplus} F^\perp$. De plus, si $(e_1, \dots, e_n)$ est une base de F, alors le projeté orthogonal d'un vecteur x sur F est

$$x_F = \sum_{k=1}^{n} \langle e_k | x \rangle \; e_k.$$

✦ Ce projeté est l'unique point réalisant la distance de x à F :

$$\left\| x - p_F(x) \right\| = d(x \; ; \; F) = \inf_{y \in F} \|x - y\| .$$

Exemple : Notons E l'espace vectoriel des fonctions complexes, continues sur $\mathbb{R}$, et 2π-périodiques, muni du produit scalaire $\langle f | g \rangle = (1/2\pi) \int_0^{2\pi} \bar{f}\, g$. Soit p un entier naturel. Notons F_p le sous-espace vectoriel de E des polynômes trigonométriques de degré au plus p. Alors le projeté orthogonale d'une fonction f de E sur F_p est sa somme partielle de Fourier d'ordre p.

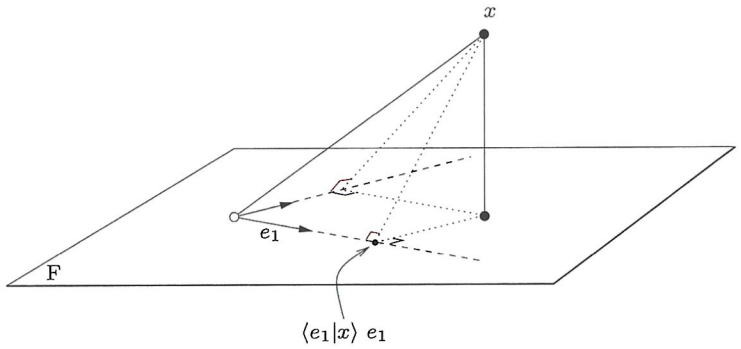


Fig. 82 — Projection orthogonale d'un vecteur x sur un sous-espace vectoriel de dimension finie, muni d'une base orthonormée.

PROPRE

☞ Base propre, Sous-espace propre, Sous-groupe propre, Valeur propre, Vecteur propre.

PYTHAGORE VI^E SIÈCLE AV. J-C

(Mathématicien, philosophe, mystique et thaumaturge grec)

Théorème de Pythagore Soit E un espace préhilbertien, soient $x, y \in E$ deux vecteurs orthogonaux. Alors $\|x + y\|^2 = \|x\|^2 + \|y\|^2$. ✦ De manière plus générale, pour toute famille orthogonale finie $(x_1, \dots, x_p)$, on a

$$\left\| \sum_{k=1}^{p} x_k \right\|^2 = \sum_{k=1}^{p} \|x_k\|^2 .$$

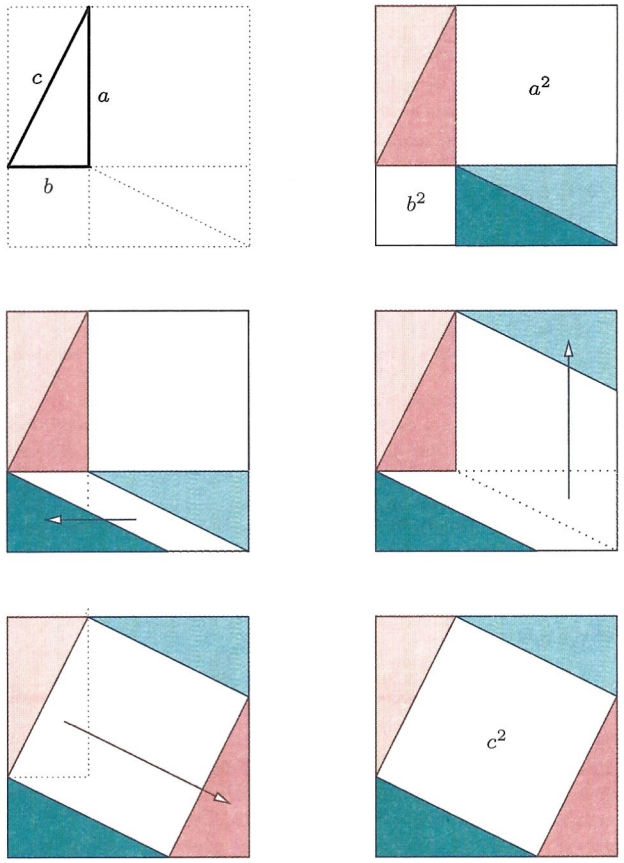


Fig. 83 — Démonstration « visuelle » du théorème de Pythagore. Sur la première figure colorée, les deux carrés blancs sont d'aire a^2 et b^2 respectivement. Sur la dernière figure, le carré central est d'aire c^2.