Logique(s) mystérieuse(s)

Pascal Dupont
pascal.dupont@uliege.be

ex-HEC•ULiège

Binche, Congrès SBPMef
20 aout 2025

Les mystères de l'induction

Induction ou récurrence ?

- L'appellation démonstration *par récurrence* est la plus courante.
- En fait, le concept de démonstation *par induction* est un peu plus général, comme nous le verrons.

Le cas de base

La forme la plus simple de démonstration par récurrence est basée sur le *principe de récurrence* :

Si la propriété P_n, indicée par un naturel n, satisfait les deux conditions suivantes :

[I] P_0 est vraie ;

[H] Chaque fois que P_n est vraie, P_{n+1} l'est également,

alors P_n est vraie pour tout naturel n.

Justification (1)

Il se fonde sur l'axiomatique de Peano des naturels :

1. Le nombre appelé *zéro* et noté 0 est un naturel ;
2. À chaque naturel n est associé un naturel appelé son *successeur* et noté $s(n)$;
3. 0 n'est le successeur d'aucun naturel ;
4. Deux naturels de même successeur sont égaux ;
5. Si une partie de l'ensemble de naturels contient 0 et le successeur de chacun de ses éléments, alors cette partie est l'ensemble de tous les naturels.

Giuseppe Peano
27/08/1858, Cuneo, Royaume de Sardaigne – 20/04/1932, Turin, Italie

Justification (2)

On notera que ceci ne peut pas être formulé dans ce qu'on appelle la logique *du premier ordre*, parce que le 5e axiome contient une quantification non pas sur les éléments de l'ensemble des naturels, mais sur toutes ses parties.

Pour rester dans le cadre de la logique du premier ordre, on peut remplacer l'axiome 5 par le *schéma d'axiome* :

5_P. Si $P(0)$ et si, pour tout n, $P(n)$ entraine $P(n+1)$, alors $P(n)$ pour tout n,

où $P(n)$ est n'importe quelle proposition contenant une variable (naturelle) n.

Comme il y a une infinité de telles propositions, notre axiomatique est maintenant du premier ordre, mais elle contient une infinité d'axiomes.

Définitions par récurrence

Noter que l'on peut aussi utiliser des *définitions* par récurrence.

Par exemple, les deux opérations de base sur les naturels sont définies par :

- Addition :
  - Pour tout m, $m + 0 := m$;
  - Pour tous m et n, $m + s(n) := s(m + n)$;
- Multiplication :
  - Pour tout m, $m \cdot 0 := 0$;
  - Pour tous m et n, $m \cdot s(n) := m \cdot n + m$.

Ou encore, la factorielle :

- $0! := 1$;
- $s(n)! := s(n) \cdot n!$.

Variantes du principe de récurrence

- Parfois, une propriété ne concerne que les naturels non nuls. L'initialisation est alors $P(1)$ plutôt que $P(0)$.
- On peut être amené à utiliser le principe sous la forme suivante :
  Si la propriété P_n, indicée par un naturel n, satisfait les trois conditions suivantes :
  [I_0] P_0 est vraie ;
  [I_1] P_1 est vraie ;
  [H_2] Chaque fois que P_n est vraie, P_{n+2} l'est également,
  alors P_n est vraie pour tout naturel n.

Récurrence forte

Une autre variante est la suivante :
Si la propriété P_n, indicée par un naturel n, satisfait la condition suivante :

[H*] Chaque fois que P_m est vraie pour tout $m < n$, P_n l'est également,

alors P_n est vraie pour tout naturel n.

On parle parfois de *récurrence forte*.

N.B. : Pas d'initialisation ici !

On justifie la récurrence forte en appliquant la récurrence « de base » à la propriété

$$Q_n \coloneqq P_0 \wedge P_1 \wedge \cdots \wedge P_{n-1}.$$

Rappels : ordinaux (1)

Un *ordinal* est une classe d'équivalence d'ensembles bien ordonnés pour la relation d'équivalence « est en bijection croissante avec ».
Les premiers sont :

$$\begin{aligned}
0 &= \emptyset \\
1 &= \{0\}, \\
2 &= \{0,1\}, \\
&\vdots \\
\omega &= \{0,1,2,\ldots\}, \\
\omega+1 &= \{0,1,2,\ldots,\omega\}, \\
\omega+2 &= \{0,1,2,\ldots,\omega,\omega+1\}, \\
&\vdots \\
2\omega &= \{0,1,2,\ldots,\omega,\omega+1,\omega+2,\ldots\}, \\
2\omega+1 &= \{0,1,2,\ldots,\omega,\omega+1,\omega+2,\ldots,2\omega\}, \\
2\omega+2 &= \{0,1,2,\ldots,\omega,\omega+1,\omega+2,\ldots,2\omega,2\omega+1\}, \\
&\vdots \\
3\omega &= \{0,1,2,\ldots,\omega,\omega+1,\omega+2,\ldots,2\omega,2\omega+1,\ldots\}, \\
3\omega+1 &= \{0,1,2,\ldots,\omega,\omega+1,\omega+2,\ldots,2\omega,2\omega+1,\ldots,3\omega\}, \\
&\vdots \\
\omega^2 &= \{0,1,2,\ldots,\omega,\omega+1,\omega+2,\ldots,2\omega,2\omega+1,\ldots,3\omega,\ldots,4\omega,\ldots\}
\end{aligned}$$

N.B. : L'addition n'est pas commutative : $1+\omega = \omega \neq \omega+1$.

Rappels : ordinaux (2)

Tout ordinal est l'ensemble des ordinaux qui lui sont strictement inférieurs :

$$\alpha = \{\beta : \beta \text{ et un ordinal et } \beta < \alpha\}.$$

. Ils se rangent en trois catégories :

- 0 ;
- Ceux qui sont le successeur d'un autre : ils s'écrivent $\alpha = \beta + 1$;
- Les autres, dits *ordinaux limites*.

Induction transfinie (1)

L'*induction transfinie* (ou *récurrence transfinie*) est une méthode de preuve d'une proposition P_α qui dépend d'un ordinal α.

Si la propriété P_α, indicée par un ordinal α, satisfait les trois conditions suivantes :

[I] P_0 est vraie ;

[H] Pour tout ordinal successeur $\alpha + 1$, si P_α est vraie, alors $P_{\alpha+1}$ l'est également ;

[L] Pour tout ordinal limite λ, si P_α est vraie pour tout ordinal $\alpha < \lambda$, alors P_λ l'est également,

alors P_α est vraie pour tout ordinal α.

Induction transfinie (2)

Ou encore :

Si la propriété P_α, indicée par un ordinal α, satisfait la condition suivante :

[H*] Pour tout ordinal λ,
si P_α est vraie pour tout ordinal $\alpha < \lambda$,
alors P_λ l'est également,

alors P_α est vraie pour tout ordinal α.

C'est l'analogue de la récurrence forte.

Autre cas d'induction : l'induction sur la forme de la formule

Les formules de la *logique du premier ordre* sont définies de la manière (inductive) suivante :

- Si R est une relation n-aire et si t_1, ..., t_n sont des termes, alors $R(t_1, \cdots, t_n)$ est une formule (*atomique*) ;
- Si f est une formule, alors $\neg f$ est une formule ;
- Si f est g sont des formules, alors $f \wedge g$, $f \vee g$ et $f \rightarrow g$ sont des formules ;
- Si f est une formule, alors $(\forall x)\ f$ et $(\exists x)\ f$ sont des formules.

Dès lors, si on veut prouver que toutes les formules ont une certaine propriété, il suffit de vérifier que :

- Les formules atomiques ont la propriété ;
- Si f a la propriété, alors $\neg f$ l'a également ;
- Si f est g ont la propriété, alors $f \wedge g$, $f \vee g$ et $f \rightarrow g$ l'ont également ;
- Si f a la propriété, alors $(\forall x)\ f$ et $(\exists x)\ f$ l'ont également.

Autre cas d'induction : constructions géométriques

On peut prouver de manière inductive, entre (nombreux) autres :

- Le théorème de Pick ;
- Le théorème d'Euler-Descartes.

Les mystères de l'impossible

Qu'est-ce que prouver l'impossibilité d'une tâche ?

Pour le profane, sans doute, c'est chercher
« assez longtemps » pour pouvoir s'écrier

« *J'ai* ***vraiment*** *tout essayé !* »…

Mais les mathématiciens ne voient pas les choses de cette oreille — nespa ?

Une méthode générale

Une stratégie utilisable est de montrer qu'une solution du problème devrait posséder deux propriétés,
et que celles-ci sont contradictoires.

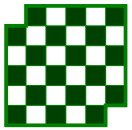
C'est ainsi que l'on démontre l'insolubilité des trois célèbres problèmes de la géométrie grecque :

- Duplication du cube,
- Trisection de l'angle,
- Quadrature du cercle.

Utilisations de la méthode

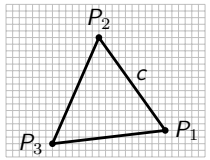
En particulier, il y a les célèbres techniques de parité.

Exemple : *Est-il possible de recouvrir le carré mutilé ci-dessous par des dominos 2×1 ?*



Un second cas

Exemple : *Dans le plan $\mathbf{R}^2$, existe-t-il un triangle équilatéral dont les trois sommets ont des coordonnées entières ?*
Supposons qu'il en existe un, de sommets $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, $P_3 = (x_3, y_3) \in \mathbf{Z}^2$; soit c son côté.



Son aire peut se calculer de deux manières :

$$\mathcal{A} = \begin{cases} \frac{\sqrt{3}}{4} c^2 = \frac{\sqrt{3}}{4} \left[(x_2 - x_1)^2 + (y_2 - y_1)^2 \right] \in \mathbf{R} \setminus \mathbf{Q} ; \\ \left| \frac{1}{2} \sum_{\text{cycl.}} (x_i y_{i+1} - x_{i+1} y_i) \right| \in \mathbf{Q}. \end{cases}$$

Les mystères des superpouvoirs

1. Qui peut le moins peut le plus

Il est bien clair que si un problème général est prouvé, tous ses cas particuliers en découlent.

Mais parfois, un cas particulier implique le cas général.

Exemples :

- Une application linéaire est injective si et seulement si son noyau est le sous-espace nul.
- Soit a un réel strictement positif ; $a^x \cdot a^y = a^{x+y}$ est vrai pour tous réels x et y si et seulement si $a^m \cdot a^n = a^{m+n}$ est vrai pour tous naturels m et n.

2. Aller & retour pour le prix de l'aller simple

Dans certaines situations, pour prouver qu'une condition est nécessaire et suffisante, il suffit de prouver l'une des deux implications, sa réciproque s'en déduisant (presque) immédiatement.

Exemples :

- Théorème de Pythagore : Le triangle ABC est rectangle en A si et seulement si $|BC|^2 = |AB|^2 + |AC|^2$.
- Théorème de Desargues : Deux triangles sont perspectifs à partir d'un point si et seulement s'ils sont perspectifs à partir d'une droite.

3. Deux propriétés pour le prix d'une seule

Dans plusieurs branches des mathématiques, on dispose d'un *principe de dualité* qui permet de déduire de chaque propriété démontrée une propriété « duale », qu'il n'y a plus besoin de démontrer.

Exemples :

- La géométrie projective (disons plane) ;
- La théorie des catégories.

Les mystères du pluriel

La logique ou *des* logiques ?

Il semblerait normal qu'il y ait *une* logique :
la manière de raisonner doit (devrait ?) être la même pour tout le monde (même hors des mathématiques).

Or ce n'est pas le cas :

- Logique du premier ordre *vs.* logique(s) d'ordre supérieur ;
- Logique(s) modale(s) ;
- Logiques non-binaires ;
- Intuition(n)isme/constructivisme ;
- …

Une multitude de logiques…

Différentes logiques peuvent être étudiées ; ce n'est pas plus choquant que la situation des géométries.

En pratique, l'immense majorité des mathématiciens ne s'en soucie pas — pas plus que du choix d'*une* théorie des ensembles.

Mais quelquefois, le fond de la barque racle un peu les récifs…

(C'est tout.)

Merci pour votre attention.

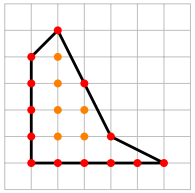
Voici le détail de la justification.

1. Initialisation :
   On a bien Q_0, qui est une conjonction vide, donc le vrai.
   N.B. : Voilà pourquoi il n'y a pas d'initialisation ; en fait, elle y est quand même.
2. Hérédité :
   Si on a $Q_n = P_0 \wedge P_1 \wedge \cdots \wedge P_{n-1}$, par H^*, on a P_n ;
   et de $P_0 \wedge P_1 \wedge \cdots \wedge P_{n-1}$ et P_n, on déduit
   $P_0 \wedge P_1 \wedge \cdots \wedge P_{n-1} \wedge P_n = Q_{n+1}$.

Ainsi, on a Q_n pour tout n, donc Q_{n+1} pour tout n.
Or, $Q_{n+1} = P_0 \wedge P_1 \wedge \cdots \wedge P_{n-1} \wedge P_n$, entraine P_n.

Théorème de Pick :
Soit P un polygone simple dans le plan, dont tous les sommets sont à coordonnées entières. L'aire de P est $\mathcal{A}(P) = i + b/2 - 1$, où i est le nombre de points à coordonnées entières intérieurs à P et b le nombre de points à coordonnées entières situés sur le bord de P.

Exemple :



$$\left.\begin{array}{l} i = 6 \\ b = 13 \end{array}\right\} \mathcal{A}(P) = 6 + \tfrac{13}{2} - 1 = \tfrac{23}{2}.$$

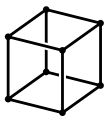
Théorème d'Euler-Descartes :
Pour tout polyèdre convexe,

$$s - a + f = 2,$$

où s est le nombre de sommets, a le nombre d'arêtes et f le nombre de faces.

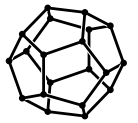
Exemples :

Cube :



$s = 8$
$a = 12$
$f = 6$

Dodécaèdre :



$s = 20$
$a = 30$
$f = 12$

Théorème de Wantzel (1837) :
Un segment de longueur a peut être construit à la règle et au compas à partir d'une unité donnée si et seulement s'il existe une liste $(K_0, K_1, \ldots, K_n)$ de corps telle que

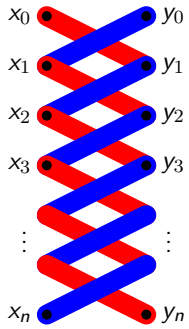
- $K_0 = \mathbf{Q}$;
- K_i *est une extension quadratique de* K_{i-1} $(1 \leqslant i \leqslant n)$;
- $a \in K_n$.

Pour que la duplication du cube soit possible (à la règle et au compas), il faudrait que $\sqrt[3]{2}$ satisfasse ces conditions ;
pareil avec $\cos(\theta/3)$ pour la trisection de l'angle θ
(bien sûr, pour certains θ particuliers, cela marche) ;
et avec $\sqrt{\pi}$ pour la quadrature du cercle.

Le polygone plan $P = (P_1, P_2, \cdots, P_n)$, où $P_0 = P_n$ et $P_k = (x_k, y_k)$ $(0 \leqslant k \leqslant n)$ a pour aire orientée

$$\mathcal{A}_{\text{or}}(P) = \frac{1}{2} \sum_{1 \leqslant k \leqslant n} (x_{k-1} y_k - x_k y_{k-1}).$$

(Formule de Gauss — en anglais, *shoelace formula*).



Soit $f : V \longrightarrow W$ une application linéaire entre les e.v. V et W.
On se souvient que $f(0_V) = 0_W$.

(1) f est injective signifie :
$(\forall\, v \in V)\ (\forall\, v' \in V)\ f(v) = f(v') \Rightarrow v = v'$.

(2) Le noyau de f, $\ker f$, est l'ensemble des vecteurs dont l'image par f est $0_W = f(0_V)$; dire que ce noyau est le sous-espace nul $\{0_V\}$, c'est donc dire que :
$(\forall\, v \in V)\ f(v) = f(0_V) \Rightarrow v = 0_V$.

Clairement, (2) est un cas particulier de (1).
Donc (1) implique (2).
Mais la réciproque est également vraie, car

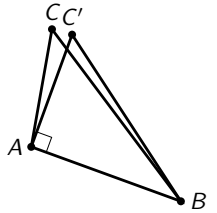
$$\begin{aligned} f(v) = f(v') &\Rightarrow f(v) - f(v') = 0_W \\ &\Rightarrow f(v - v') = 0_W \\ &\overset{(2)}{\Rightarrow} v - v' = 0_V \\ &\Rightarrow v = v'. \end{aligned}$$

On veut montrer que, pour tout réel a strictement positif,
$(\forall\, x, y \in \mathbf{R})\ a^x \cdot a^y = a^{x+y} \Leftrightarrow (\forall\, m, n \in \mathbf{N})\ a^m \cdot a^n = a^{m+n}$. $\Rightarrow$ est clair (cas particulier).
$\Leftarrow$:

1. Si $m, n \in \mathbf{N}$, $a^m / a^n = a^{m-n}$, car
   - Si $m \geqslant n$, $a^{m-n} \cdot a^n = a^{(m-n)+n} = a^m$, donc $a^m / a^n = a^{m-n}$;
   - Si $m < n$, $a^m / a^n = 1/(a^n / a^m) = 1/a^{n-m} = a^{m-n}$.
2. Si $x \in \mathbf{N}$ et $y \in \mathbf{Z}^*_-$: $x = m$, $y = -n$, avec $m, n \in \mathbf{N}$; alors,
   $a^x \cdot a^y = a^m \cdot a^{-n} = a^m \cdot 1/a^n = a^m / a^n = a^{m-n} = a^{x+y}$.
3. Si $x, y \in \mathbf{Z}^*_-$: $x = -m$, $y = -n$, avec $m, n \in \mathbf{N}$; alors,
   $a^x \cdot a^y = a^{-m} \cdot a^{-n} = \dfrac{1}{a^m} \cdot \dfrac{1}{a^n} = \dfrac{1}{a^m \cdot a^n} = \dfrac{1}{a^{m+n}} = a^{-(m+n)} = a^{x+y}$.
4. Si $x, y \in \mathbf{Q} \setminus \mathbf{Z}$: $x = m/p$, $y = n/q$,
   avec $m, n \in \mathbf{Z}$, $p, q \in \mathbf{N} \setminus \{0, 1\}$, $m \wedge p = n \wedge q = 1$; alors,
   $a^x \cdot a^y = a^{m/p} \cdot a^{n/q} = \sqrt[p]{a^m} \sqrt[q]{a^n} = \sqrt[pq]{a^{mp}} \sqrt[pq]{a^{nq}} =$
   $= \sqrt[pq]{a^{mp} \cdot a^{nq}} = \sqrt[pq]{a^{mp+nq}} = a^{(mp+nq)/(pq)} = a^{m/p+n/q} = a^{x+y}$.
5. Si $x, y \in \mathbf{R} \setminus \mathbf{Q}$, en supposant d'abord que $a > 1$:
   $a^x \cdot a^y = \sup_{\substack{p \in \mathbf{Q} \\ p < x}} a^p \cdot \sup_{\substack{q \in \mathbf{Q} \\ q < y}} a^q = \sup_{\substack{p,q \in \mathbf{Q} \\ p < x, q < y}} a^p \cdot a^q = \sup_{\substack{p,q \in \mathbf{Q} \\ p+q < x+y}} a^{p+q} \overset{(*)}{=} \sup_{\substack{r \in \mathbf{Q} \\ r < x+y}} a^r = a^{x+y}$;
   $(*)$: car $\{p + q : p, q \in \mathbf{Q}, p < x, q < y\} = \{r : r \in \mathbf{Q}, r < x + y\}$.
   Pour $a = 1$, l'égalité est évidente et pour $0 < a < 1$, on remplace les sup par des inf.

On suppose prouvé le théorème de Pythagore direct : si le triangle ABC est rectangle en A, alors $|BC|^2 = |AB|^2 + |AC|^2$, et en déduit la réciproque.

Soit ABC un triangle tel que $|BC|^2 = |AB|^2 + |AC|^2$.



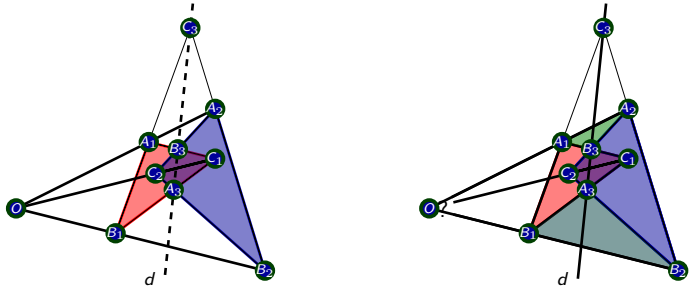
Sur la perpendiculaire à AB en A, soit C' tel que $|AC'| = |AC|$.
Alors,

$$|BC'|^2 = |AB|^2 + [AC']^2 = |AB|^2 + |AC|^2 = |BC|^2,$$

et les deux triangles ABC et ABC' ont leurs côtés de même longueur ; ils sont donc isométriques, et l'angle $\widehat{BAC}$ est droit.

Les triangles $A_1B_1C_1$ et $A_2B_2C_2$ sont *perspectifs à partir du point O* si celui-ci est aligné avec A_1 et A_2, avec B_1 et B_2, et avec C_1 et C_2 ; ils sont *perspectifs à partir de la droite d* si celle-ci concourt avec A_1B_1 et A_2B_2, avec B_1C_1 et B_2C_2, et avec C_1A_1 et C_2A_2.

Le sens direct du thm de Desargues affirme que la 1re propriété entraine la 2nde. Montrons que la réciproque en découle.



En géométrie projective plane, on a des points, des droites et une relation d'incidence (notée $\triangleleft$), satisfaisant aux axiomes :

[PP_1] Étant donné deux points distincts, il existe une droite incidente aux deux ;

[PP_2] Étant donné deux droites distinctes, il existe un point incident aux deux ;

[PP_3] Si deux points sont incidents à deux droites, alors les deux points sont confondus ou les deux droites sont confondues.

[PP_4] Il existe des points P, Q, R, et des droites d, e, f, tels que $P \triangleleft d$, $P \triangleleft e$, $P \not\triangleleft f$, $Q \triangleleft d$, $Q \not\triangleleft e$, $Q \not\triangleleft f$, $R \not\triangleleft d$, $R \not\triangleleft e$, $R \triangleleft f$.

Le *dual* d'un énoncé s'obtient en y intervertissant points et droites. Exemples : Le dual de [PP_1] est [PP_2], et inversement. [PP_3] et [PP_4] sont leurs propres duaux.

Comme les duaux des axiomes sont des théorèmes, le dual de tout théorème est aussi un théorème. C'est le *principe de dualité* de la géométrie projective plane.

Une *catégorie* est donnée par des *objets* et des *flèches* entre eux, avec une flèche identité sur chaque objet et une composition des flèches consécutives, associative.

Exemples : La catégorie des ensembles et applications, la catégorie des ensembles ordonnés et applications croissantes, la catégorie des K-e.v. et applications K-linéaires, ...

En retournant toutes les flèches, on obtient une nouvelle catégorie, dite *duale*. On a donc ici encore un *principe de dualité*, qui permet de ne prouver que la moitié des théorèmes.

S'il n'a pas un nom par ailleurs, le concept dual est souvent nommé avec le préfixe *co-*. D'où la blague :
A comathematician is someone who turns cotheorems into fee.

Logique(s) modale(s) :

Il est question ici d'ajouter des *modalités*, qui sont des opérateurs unaires sur les propositions ; par exemple,

$$P \nearrow \Box P \text{ « il est nécessaire que } P \text{ »}$$
$$P \searrow \Diamond P \text{ « il est possible que } P \text{ »}$$

avec des règles telles que

$$\neg(\Box P) \equiv \Diamond(\neg P) \text{ et } \neg(\Diamond P) \equiv \Box(\neg P).$$

Ceci définit la logique modale dite *aléthique*, qui remonte à Aristote. Il y en a d'autres...