Contre-exemples & modèles :
comment prouver l'impossible

Marc SAGE

jeudi 30 janvier 2020

Intro : *Éléments* d'Euclide, volonté de réduire les axiomes, impossibilité pratique de réduire le 5e postulat.

COMMENT PROUVER UNE TELLE IMPOSSIBILITÉ ?

RQ : on utilisera "(**c**)**eg**"[1] pour abréger "(**contre-**)**exemple**".

1 ceg pur

Une affirmation "générique" s'énonce souvent $\forall a,\ \overset{\text{prémisse}}{P} \Longrightarrow \overset{\text{conclusion}}{Q}$, çàd « chq objet vérifiant P vérifie Q ».

Un ***eg*** de cette assertion est un objet a vérifiant la prémisse P et la conclusion Q.

Un ***ceg*** est un objet a vérifiant P MAIS PAS Q, çàd niant l'implication $P \Longrightarrow Q$.

Exhiber un tel a est le moyen canonique de ***réfuter*** ladite généralité.

EG (au sens *illustration*, pas au sens précédent ^^) : regardons $\forall c \in \mathbf{C},\ c^2 \in \mathbf{R}_+$. Exemplifié par chq réel. Mais chq imaginaire pur ($\neq 0$) en est un ceg. Ainis, vu la conjonction $\left\{\begin{array}{l} i \in \mathbf{C} \\ i^2 \notin \mathbf{R} \end{array}\right.$, on a *réfuté* l'énoncé $\forall c \in \mathbf{C},\ c^2 \in \mathbf{R}_+$: impossible de le prouver sans introduire de contradction, çàd sans *tout* établir !

★★ Un CEG d'une généralité G signe la mort subite de toute tentative de preuve de G. ★★

2 guide de preuve

Cherchons les $f : \mathbf{R} \longrightarrow \mathbf{R}$ additives. Des eg sont les homothéties (c'est dire que $\times$ se distribue sur $+$). Par csqt, quoi que l'on prouve sur un tel f, chq homthétie *doit* le vérifier. Impossible dans ces conditions de mq eg $f(1) = 42$! Ainsi, dans une preuve, les eg sont autant de garde-fous à des preuves vouées d'avance à l'échec.

★★ Ce que j'aimerais avoir, est-ce que déjà les eg *simples* le vérifient ? ★★

EG : trouver les $c : \mathbf{R} \longrightarrow \mathbf{R}$ telle ques $\forall t \in \mathbf{R},\ c(2t) = 2c(t)^2 - 1$. Les cosinus forment une famille $(t \mapsto \cos \omega t)_{\omega \in \mathbf{R}}$ de solutions (le cas $\omega = 0$ donnant la solution constante 1). Peut-on montrer que ce sont les seules ? NON ! en effet parmi exemples simples, eg polynômes, eg constants, il y a aussi $\frac{1}{2}$!

[1] *e. g.* = *exempli gratia* = par exemple

3 force d'une hypothèse (maths & rebours)

Typique : l'importance d'une hypothèse s'établit en exhbitant un ceg au "théorème-où-l'on-a-enlevé-ladite-hypothèse-des-prémisses" (lequel n'est alors plus un théorème !)

EG : chq fonction complexe continue sur un segment y est bornée. Sans la continuité, prolonger "inverser" sur $[-1,1]$ par $0 \mapsto 0$; sans le segment restreindre $t \mapsto \frac{1}{t(1-t)}$ à $]0,1[$ (ou ath à $]-1,1[$...).

★★ GARDE : un ceg *ne* montre *pas* la *nécessité* de l'hypothèse
(au sens où chq objet vérifiant la conclusion *doit* vérifier l'hypothèse),
il est juste **un ceg de la réciproque** du thm ★★

EG : on montre aisément $\forall f$ inj, $\forall A \subset \operatorname{Dom} f,\ f^{-1}(f(A)) = A$. Nécessité de l'hypothèse INJ ?

On a un ceg : si $f = t \mapsto t^2$ alors on a un ceg : si $A = \mathbf{R}_+$ on a alors $f^{-1}(f(A)) = f^{-1}(\mathbf{R}_+) = \mathbf{R} \neq A$
Plus généralement : si f pas inj alors $\exists a \neq b,\ f(a) \neq f(b)$ et $a \in f^{-1}(f(\{b\}))$ mais $a \notin \{b\}$. On a ainsi montré la réciproque (çàd la *nécessité au sens fort* de l'hypothèse).

L'eg ci-dessus permettait d'aller jusqu'au bout des questions de force des hypothèses (hint –> *reverse maths*...) : pas toujours possible ni facile – ni même pertinent !

4 polysémie

Quel est le principe du *fonctionnment* du ceg ? dans un prédicat (eg $1 + a^2 \geq 0$), la lettre libre (ici a) peut être librement interprétée.

Mais pourquoi pas les autres symboles ? (individus $0, 1, 2$; opérations $+$, $\hat{}$; relation $\geq$)

Parce qu'on leur *présuppose* une interprétation. Or les énoncés sont ***polysémiques*** !

EG 1 $\quad \forall^2 a < b,\ \exists n,\ a < n < b$ est vrai dans $\mathbf{Q}, \mathbf{R}$ mais faux dans $\mathbf{N}, \mathbf{Z}$ (avec interprétations "naturelles")

EG 2 $\quad \forall^2 a < b,\ a \leq b + 1$ c'est l'inverse !

EG 3 $\quad \forall a, b,\ ab = ba$ est vrai dans $\mathbf{C}$ mais faux dans $\mathbf{H}$, M_2, $\mathfrak{S}_3$

EG 4 le 5e postulat ! en interprétant "plan" comme *disque unité ouvert*, "point" par *point du "plan"* et "droite" par *arc de cercle orthogonal à la frontière du "plan"*, on peut vérifier chaque axiome d'Euclide mais nier le 5e postulat (convaiquant sur un dessin)

★★ La *polysémie* découle de la *diversité* des interprétations possibles,
çàd des *contextes* d'interprétation de TOUS les symboles. ★★

5 modèles

Un langage formel (de *forme* : *a priori* vide de sens, prêt à en recevoir) est

$$\text{la donnée de symboles} \begin{cases} \text{d'individu : } 0, \emptyset, \mathbf{N}, \exp, \overrightarrow{0}, \mathrm{Id} \\ \text{d'opération : } + \times - \cup \cap \circ\ \{,\} \\ \quad \text{(mais aussi \textbf{singulaire} : } \mathfrak{P}\text{, carré, successur, racine)} \\ \text{de relation : } \leq | \subset \text{ (les rel. singulaires codent des 1-prédicats)} \end{cases} .$$

Une ***structure*** (de ce langage) est un "cadre d'interprétation" de ses énoncés, lequel leur confèrent une ***valeur de vérité*** ("vrai"/"faux") (sans invoquer de "vérité" métaphysique, on aurait pu choisir "jaune/violet", ou d'autres valeurs "chromatiques", d'autres "couleurs")

Un ***modèle*** d'un énoncé est une structure où ledit énoncé est *vrai.*

PRINCIPE : chaque preuve formelle doit répandre/transmettre le "vrai", donc

chque modèle de E doit vérifier chque théorème prouvé formelement à partir de E
(si $E \vdash \theta$, chaque modèle de E doit $\models \theta$)

Parallèle avec les sous-suites : si $a \longrightarrow l$, alors chq ss de a doit $\longrightarrow l$. Application : montrer une divergence en exhibant deux ss tendants vers deux valeurs $\neq$. Application parallèle :

★★ *pour montrer une* impossibiltié *de prouver E,*
exhiber deux structures "divergeant" sur la valeur de vérité de E ★★

EG : mq les axiomes de groupe ne pvent ni ne réfutent l'abélianité. Il y a des groupes abéliens (eg $\{1\}$) donc pas réfutable, il y a des groupes anabéliens ($\mathfrak{S}_3$) donc pas prouvable. On dit alors que l'abélianité est ***indépendante*** des autres axiomes.

EG (dur) : AC indépendant de ZF

★★★ **GARDE!!!** Dans tout ce qui précède (sauf "sphère primitive"), **"vrai" signifie prouvable dans ZFC**.
Donc toutes les impossibiltiés sont *relatives à la consistance de ZFC* (ou autre cadre choisi). ★★★