REPERES - IREM . N° 29 - octobre 1997

LE RAISONNEMENT PAR L'ABSURDE

Henri Lombardi
IREM de Besançon

Résumé : De très nombreux raisonnements par l'absurde sont des raisonnements directs présentés à l'envers. D'autres sont des raisonnements directs à peine déguisés, qu'il est facile de transcrire sous forme directe. D'autres preuves, dites **par** l'absurde, ne sont que des preuves **de** l'absurde : comment démontrer qu'une hypothèse est toujours fausse, sinon en la réduisant à l'absurde ?

Enfin, il est des cas où, apparemment, on ne sait pas établir un fait de nature positive autrement qu'en réduisant à l'absurde l'hypothèse selon laquelle le fait en question serait faux. Ce sont là les vrais raisonnements par l'absurde. C'est souvent selon cette méthode qu'ont été établis, au moins en un premier temps, les "théorèmes d'existence" modernes depuis Cantor et Hilbert.

Pour établir une claire distinction entre le raisonnement direct et le raisonnement par l'absurde, il est nécessaire de prendre conscience qu'au moins intuitivement certains faits mathématiques peuvent être qualifiés "de type positif", et d'autres "de type négatif". C'est sur la base de cette intuition que l'on qualifie tel raisonnement de "raisonnement par l'absurde" et tel autre de "raisonnement direct".

Pour rendre compte de cette intuition, la logique classique n'est en tout cas d'aucun secours. C'est sans doute la raison pour laquelle la grande majorité des mathématicien(ne)s, imprégné(e)s de logique classique, ont déserté le terrain de la discussion philosophique sur la nature du raisonnement par l'absurde.

1. QUELQUES EXEMPLES CLASSIQUES : EUCLIDE ET ARCHIMÈDE

Nous commençons par quelques exemples classiques de raisonnements par l'absurde tirés des textes fondateurs grecs. Nous avons emprunté ces exemples à J.-L. Gardies (*Le raisonnement par l'absurde*, P.U.F., 1991), mais nous n'en faisons pas le même commentaire.

Le triangle isocèle

Un des premiers raisonnements par l'absurde répertoriés est celui-ci, extrait d'Euclide.

On veut démontrer qu'un triangle ABC ayant les angles en B et C égaux est isocèle. Dans l'explication qui suit, nous utiliserons les notations modernes (droite signifie droite et non segment de droite par exemple). Cependant "angle" signifiera "angle géométrique" et non angle orienté.

Selon notre explication, ce raisonnement par l'absurde est un *raisonnement direct retourné à l'envers*.

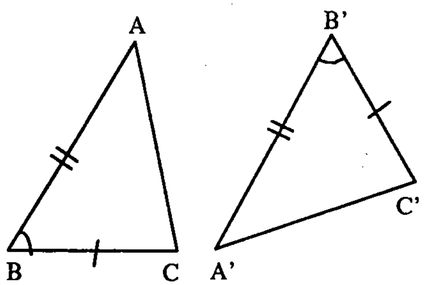


Fig. 1

On a déjà établi le premier cas d'égalité des triangles :

Deux triangles qui ont un angle égal entre deux côtés égaux sont égaux (figure 1 ci-dessus)

On considère alors un triangle ABC ayant les angles en B et C égaux.

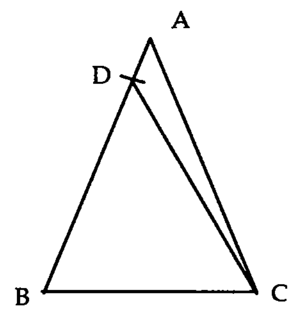


Fig. 2

On suppose (par l'absurde) que l'un des côtés AB ou AC est plus grand que l'autre. Par exemple AB > AC. On considère le point D du segment BA tel que BD = CA . Par le premier cas d'égalité, et par l'hypothèse sur les angles en B et C du triangle ABC , les triangles ACB et DBC sont égaux (les sommets se correspondant dans l'ordre indiqué). Mais le deuxième triangle est (d'aire) strictement plus petit(e) que le premier. Le tout est donc égal à la partie, ce qui est absurde. Et l'hypothèse de départ était donc fausse.

Ce raisonnement par l'absurde se transforme facilement en un raisonnement direct. On procède comme suit. Construisons sur la demi droite (B,BA) le point D tel que BD = CA . Par le premier cas d'égalité, les triangles ACB et DBC sont égaux. Donc les angles $\angle$ BCD et $\angle$ ABC sont égaux, donc aussi les angles $\angle$ BCD et $\angle$ BCA. Par construction A et D sont du même côté de la droite (BC). L'égalité des deux angles implique donc que les droites (CD) et (CA) coïncident. Donc les points A et D sont confondus et AB = DB = AC.

On notera par ailleurs que le raisonnement direct ne fait plus appel à l'axiome

"Le tout est [strictement] plus grand que la partie [stricte]".

Le premier raisonnement, sans faire aucune hypothèse absurde et en commençant comme le nôtre, pouvait conclure que l'aire du triangle CDA est nulle, ce qui impliquait que D soit en A . Les grecs ne pouvaient sans doute guère faire un tel raisonnement où il est question d'un "faux" triangle d'aire nulle, et ils lui ont préféré le raisonnement par l'absurde.

Dans notre rétablissement du raisonnement sous forme directe, nous avons introduit une «simplification» qui consiste à remplacer un raisonnement sur des aires égales par un raisonnement sur des angles égaux. C'est-à-dire que nous n'avons pas besoin d'avoir caché une théorie des aires dans les axiomes pour faire fonctionner la preuve. Une telle réticence vis à vis de la théorie des aires ne pouvait être partagée par les grecs, qui ne voyaient sans doute nulle nécessité de subordonner la théorie des aires à celle des angles et longueurs.

L'incommensurabilité du côté et de la diagonale du carré, par le pair et l'impair

Nous considérons maintenant l'un des plus célèbres des raisonnements par l'absurde. L'incommensurabilité du côté et de la diagonale d'un carré selon la preuve par le pair et l'impair.

Nous défendrons ici le point de vue suivant :

à strictement parler, *il ne s'agit pas d'une preuve **par** l'absurde, mais d'une preuve **de** l'absurde*, en tout cas si on définit l'incommensurabilité comme l'impossibilité qu'existe une commune mesure.

La preuve par le pair et l'impair peut être présentée comme suit.

Supposons une commune mesure au côté et à la diagonale d'un carré. Supposons que le côté est égal à n fois cette commune mesure (1) et la diagonale à p fois cette commune mesure. Si n et p sont tous deux pairs, on peut multiplier la commune mesure par 2 et diviser n et p par 2 . On se ramène donc par un processus fini bien controlé (2) au cas où au moins un des deux nombres n et p est impair. Par le théorème de Pythagore $p^2 = 2n^2$. Donc p est pair et n est impair : $p = 2p_1$. Mais $p^2 = 2n^2$ implique alors $n^2 = 2p_1^2$, et n est pair. Ce qui est absurde. *Et c'est précisément ce que nous voulions démontrer.* Car l'incommensurabilité est *définie comme* signifiant l'impossibilité d'une commune mesure.

La double réduction à l'absurde pour prouver des égalités de rapports d'aires, de volumes, de longueurs

Nous rappelons tout d'abord brièvement pourquoi la théorie de la comparaison des rapports de grandeur attribuée à Eudoxe répond à une nécessité mathématique très forte.

Nous montrons ensuite que cette nécessité mathématique conduit à une conception *positive* de l'inégalité et une conception *négative* de l'égalité.

(1) Dans tout l'article, nous réservons les lettres m, n, p avec éventuellement des indices, pour désigner des nombres entiers.

(2) Depuis 1990, l'accent circonflexe n'est plus jamais obligatoire sur le "o", n'en déplaise à Messieurs Robert et Larousse.

Nous défendons enfin l'idée selon laquelle le procédé de double réduction à l'absurde, si habilement et systématiquement mis en oeuvre par Archimède, n'est qu'une manière à peine détournée d'appliquer la définition *négative* de l'égalité. En conséquence les preuves d'Archimède sont en fait des preuves **de** l'absurde et non des preuves **par** l'absurde.

Comparaison des aires de deux parallélogrammes

Considérons le théorème suivant :

Théorème : les aires de deux parallélogrammes compris entre deux droites parallèles (Δ) et (Δ') sont entre elles comme leurs bases

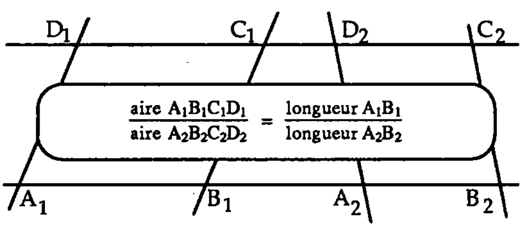


Fig. 3

Par un jeu de puzzle on se ramène au cas des rectangles

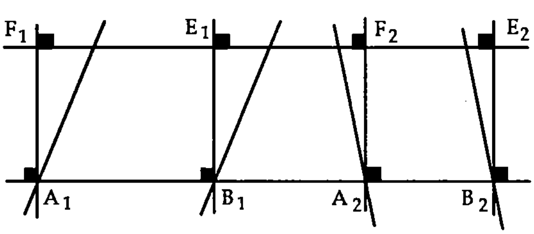


Fig. 4

Si maintenant A_1 B_1 et A_2 B_2 sont commensurables, l'égalité cherchée se démontre par un jeu de puzzle. (figure 5 ci-dessous pour un rapport de 3 à 5)

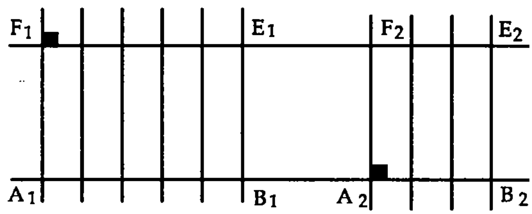


Fig. 5

Si on ne fait pas l'hypothèse d'existence d'une commune mesure, le même résultat ne peut être obtenu que par des raisonnements beaucoup plus sophistiqués.

Une solution est donnée par la théorie des rapports de grandeurs de même nature attribuée à Eudoxe. Nous commençons par un bref rappel de cette théorie.

Bref rappel de la théorie des grandeurs

Lorsque deux grandeurs sont de même nature, on peut les additionner, les comparer entre elles (3), retrancher la plus petite de la plus grande. Des propriétés de stabilité convenables sont également supposées, comme par exemple :

$$a = b \text{ et } a' > b' \Rightarrow a + a' > b + b'$$

En outre on suppose qu'une grandeur peut toujours être divisée en n parties

(3) Il faut remarquer que l'hypothèse selon laquelle deux grandeurs de même nature sont toujours comparables ne va pas totalement de soi lorsque par exemple il s'agit d'aires planes, de volumes, et encore moins lorsqu'il s'agit de longueurs de courbes ou d'aires non planes.

égales. Enfin, l'axiome d'Archimède doit être vérifié :

Si deux grandeurs a et e sont de même nature, il existe un entier n tel que $n\,e > a$

Eudoxe **définit** alors l'égalité de deux rapports a_1/a_2 et b_1/b_2 (a_1 et a_2 étant de même nature, ainsi que b_1 et b_2) en demandant, que :

$$\text{pour tous entiers m et p} \begin{cases} (ma_1 > pa_2 \text{ et } mb_1 > pb_2) \\ \text{ou bien} \\ (ma_1 > pa_2 \text{ et } mb_1 < pb_2) \\ \text{ou bien} \\ (ma_1 = pa_2 \text{ et } mb_1 = pb_2) \end{cases} \quad (1)$$

Lorsque les deux grandeurs a_1 et a_2 sont commensurables, la dernière équivalence suffit, pour un seul couple de valeurs de m et p . Sinon, il faut faire appel à une infinité de comparaisons pour établir une égalité (4).

En bonne logique, la définition d'Eudoxe devrait être *précédée* du lemme suivant qui justifie réellement cette définition :

Lemme préliminaire : étant données trois grandeurs a , b , c de même nature avec $a > b$ on peut trouver deux entiers m et p tels que $m\,a > p\,c > m\,b$ (c.-à-d. on peut établir que a/c n'est pas égal à b/c au sens de la définition d'Eudoxe)

La preuve de ce lemme repose sur l'axiome d'Archimède. Soit en effet un entier m tel que $m\,(a - b) > 2c$. Considérons la grandeur c/m et soit p le plus petit entier tel que $p\,(c/m) > b$. D'après les hypothèses on a $a > p\,(c/m) > b$ c.-à-d. $m\,a > p\,c > m\,b$

Le caractère négatif de l'égalité des rapports dans la définition d'Eudoxe

La définition de l'égalité des rapports selon Eudoxe (qui pour l'essentiel coïncide avec la définition actuelle de l'égalité de deux nombres réels) implique la situation apparemment paradoxale suivante.

Lorsque a_1 et a_2 sont incommensurables, et que $a_1/a_2 = b_1/b_2$, l'égalité est *a priori* impossible à constater selon un processus fini. L'infinité des couples (m,p) intervenant dans la définition ote à celle-ci tout caractère directement opératoire (5). Par contre, si les deux rapports sont inégaux, cela se constatera au moyen d'un seul test :

pour deux entiers m et p convenables,

$$m\,a_1 > p\,a_2 \text{ et } m\,b_1 < p\,b_2 \qquad (2)$$

La condition ci-dessus, qui s'interprète comme $a_1/a_2 > p/m > b_1/b_2$, donne une condition suffisante simple permettant de distinguer deux rapports, tandis que l'égalité de deux rapports est essentiellement

(4) Notre commentaire est manifestement "anachronique": il n'y a sans doute pas conscience chez les Grecs du quantificateur universel que nous lisons aujourd'hui dans la définition. Et cette infinité potentielle de vérifications sous-tendue en principe par la définition d'Eudoxe aurait sans doute été pour eux un cauchemar. Cependant, le fait qu'ils n'aient pas réfléchi à l'égalité des rapports de grandeur avec cet infini potentiel en tête ne signifie pas qu'ils aient eu raison quant au fond. Nous prétendons au contraire qu'une analyse sérieuse de leur définition de l'égalité ne peut éviter en aucune manière le recours à cet infini potentiel.

(5) Insistons sur le mot «constater». Une preuve bien faite est un processus fini, pas nécessairement compliqué, qui permet de certifier une égalité de deux rapports irrationnels, mais une preuve n'est pas une constatation.

définie comme l'impossibilité de les distinguer selon la procédure simple ci-dessus.

Résumons nous. La définition (2) de l'inégalité, (qui est presque sous cette forme chez Eudoxe), a un caractère positif, fini, directement opératoire. La définition (1) de l'égalité a un caractère infini et se révèle être une *définition par l'absurde* : deux rapports sont égaux si et seulement si il est impossible de les distinguer [(6)].

Nous allons maintenant voir comment fonctionne la définition d'Eudoxe en pratique, mais plutot que de traiter le cas des aires de parallélogrammes, nous examinons le cas plus intéressant des aires enfermées par des courbes planes.

Comparaison d'aires enfermées par des courbes

Considérons le cas des aires de deux cercles de rayons r et 2r .

Alors que pour les carrés de côté r et 2r il est facile de montrer que le rapport des aires est égal à 4 en utilisant un puzzle, on voit bien qu'il ne peut guère être question d'une telle preuve pour le cas des deux cercles, à cause des bords des deux cercles.

Une théorie sophistiquée des rapports de grandeur s'avère donc maintenant indispensable même dans le cas où les rapports sont rationnels.

En d'autres termes, et bien que ceci ne soit devenu apparent que fort tard, il y a inévitablement un côté "purement conventionnel" dans la définition de l'égalité de deux aires limitées par des courbes : cette égalité ne peut pas être établie de manière aussi incontestable que l'égalité des aires de deux rectangles ayant leurs côtés tous commensurables, ou que l'inégalité de deux aires enfermées par des courbes. Certes, l'axiome d'Archimède semble sauver en partie la mise (au regard de la preuve du *lemme préliminaire* donné plus haut), mais lorsqu'il s'applique à des aires, il s'agit d'un nouvel axiome par rapport à celui qui s'applique à des longueurs. L'axiome d'Archimède pour les aires permet de faire l'économie de la théorie des aires des domaines quarrables du plan (c.-à-d. essentiellement l'intégrale de Riemann), mais du coup, il cache le caractère "conventionnel" de la définition de l'égalité des aires.

Voici alors la preuve que les aires de deux cercles sont entre elles comme celles des carrés construits sur leurs rayons. Notons $\mathcal{A}_1$, $\mathcal{C}_1$, $\mathcal{A}_2$, $\mathcal{C}_2$ les aires respectives des cercles et des carrés. Supposons que le rapport des aires des carrés soit supérieur à celui des cercles correspondants : $\mathcal{A}_1 / \mathcal{A}_2 > \mathcal{C}_1 / \mathcal{C}_2$, ou ce qui revient au même en introduisant une quatrième proportionnelle "abstraite" $\mathcal{A}'_1$, supposons que

$$\mathcal{A}_1 / \mathcal{C}_1 > \mathcal{A}'_1 / \mathcal{C}_1 = \mathcal{A}_2 / \mathcal{C}_2.$$

On peut alors trouver un polygone P_1 inscrit dans le cercle C_1 et dont l'aire $\mathcal{P}_1$ vérifie :

$$\mathcal{A}_1 / \mathcal{C}_1 > \mathcal{P}_1 / \mathcal{C}_1 > \mathcal{A}'_1 / \mathcal{C}_1 = \mathcal{A}_2 / \mathcal{C}_2.$$

Mais en considérant l'aire $\mathcal{P}_2$ du polygone correspondant P_2 inscrit dans le cercle C_2 on obtient

$$\mathcal{P}_1 / \mathcal{C}_1 = \mathcal{P}_2 / \mathcal{C}_2 \text{ et } \mathcal{A}_2 / \mathcal{C}_2 > \mathcal{P}_2 / \mathcal{C}_2$$

(6) La situation est donc paradoxale au regard du langage usuel qui donne une connotation de négation à l'inégalité. En fait, l'opposition du langage usuel indiscernable/discernable serait ici plus adéquate que l'opposition égal/inégal.

ce qui est absurde. L'inégalité dans l'autre sens se réduirait à l'absurde de la même manière. Ainsi, bien qu'on ne soit pas retourné à la définition stricto sensu de l'égalité, puisque le rapport intercalé $\mathcal{P}_1/\mathcal{C}_1$ n'est pas rationnel, la preuve constitue en soi le même genre de réduction à l'absurde que celui réclamé par la définition.

2. UNE ANALYSE PLUS DÉTAILLÉE

Dans cette section nous présentons une analyse plus détaillé de la signification, positive ou négative, des énoncés mathématiques. Nous nous appuyons sur cette analyse pour donner un exemple de vraie preuve par l'absurde, et pour discuter la question du retournement des preuves par l'absurde en preuves directes.

Une définition un peu plus formalisée du positif et du négatif

Nous avons parlé dans la section 1, de manière informelle, du caractère « positif et fini » de certaines assertions, opposé au caractère « négatif et infini » de certaines autres. Ceci était basé sur une intuition qui est suffisante dans beaucoup de cas concrets. Nous essayons maintenant d'en donner une approche un peu plus formalisée. Cette approche tient compte des acquis de l'histoire, qui a mis les entiers naturels au premier rang pour tout ce qui concerne les questions de l'infini, au point de subordonner sur le plan logique toutes les mathématiques au cas paradigmatique des entiers (7). Ce n'est d'ailleurs que le prolongement naturel du "début de l'histoire" dans laquelle le cas difficile du rapport des grandeurs a été ramené à des considérations sur les entiers naturels.

(7) C'est seulement une illusion langagière qui peut laisser croire que les ensembles sont à la base des mathématiques.

Nous considérons donc un "corps de mathématiques" dans lequel interviennent les entiers naturels ainsi que des "mécanismes" fonctionnant à partir des entiers naturels. Nous notons m, n, p, q pour des entiers naturels et α: $(m,n,p) \mapsto \alpha(m,n,p)$ pour un "mécanisme". Par exemple un mécanisme typique chez Archimède est la production d'aires successives connues qui approchent une aire inconnue avec une précision toujours plus grande et bien controlée (la précision double au moins à chaque étape).

Pour simplifier la discussion, nous supposons que le mécanisme α produit en sortie un entier naturel (en pratique, le mécanisme produit souvent un résultat du type Vrai ou Faux, et ces valeurs de vérité peuvent être codées par 0 et 1).

Une assertion de caractère positif, fini, concernant le mécanisme α est de l'un des types suivants :

type immédiat (m, n, p, q sont des entiers précisés)

$$\alpha(m,n,p) = q \qquad \text{(I)}$$

type purement existentiel (n, p, q sont des entiers précisés)

$$\exists\, m\ \alpha(m,n,p) = q \qquad (E_1)$$

Par contre, une assertion du type purement universel suivant est de caractère négatif (infini)

$$\forall\, m\ \alpha(m,n,p) = q \qquad (U_1)$$

Il est à noter qu'on ne change pas le type logique d'une telle assertion si on remplace la relation d'égalité par une autre relation facile à tester.

Le lecteur ou la lectrice constatera donc que beaucoup, pour ne pas dire la plupart, des théorèmes mathématiques sont des énoncés de caractère infini.

Le caractère infini d'un énoncé n'est pas un obstacle pour une preuve convaincante : les preuves par récurrence sont très convaincantes. C'est seulement un obstacle à sa vérification par un simple calcul.

Il se présente aussi naturellement des assertions de caractère plus compliqué que les précédents comme par exemple : (p, q sont des entiers précisés)

$$\exists m \; \forall n \; \alpha(m,n,p) = q \qquad (E_2)$$
$$\forall m \; \exists n \; \alpha(m,n,p) = q \qquad (U_2)$$

ou, plus compliqué encore, (q étant un entier précisé)

$$\exists m \; \forall n \; \exists p \; \alpha(m,n,p) = q \qquad (E_3)$$
$$\forall m \; \exists n \; \forall p \; \alpha(m,n,p) = q \qquad (U_3)$$

Et on peut considérer des énoncés dont le caractère de complication logique sera supérieur à tous les types (E_n) ou (U_n) en utilisant la méthode diagonale de Cantor par exemple.

La surprise est sans doute que les grandes conjectures mathématiques sont (équivalentes à) des énoncés du type (U_1) (théorème de Fermat, conjecture de Riemann sur les zéros de la fonction Zéta, conjecture de Poincaré sur la topologie de la sphère) ou (U_2) (conjecture P ≠ NP en informatique théorique) mais très rarement d'un type plus compliqué.

Toutes les preuves d'énoncés du type (U_1) ou d'un autre type plus compliqué impliquent une infinité de vérifications (ou des infinités imbriquées de vérifications). Dans ces cas, une vérification directe est difficile à concevoir. On ne peut guère espérer exclure des preuves la méthode de réduction à l'absurde.

En effet, la *signification* d'une assertion du type (U_1) n'est rien d'autre que la possibilité de réduire à l'absurde une assertion de type (E_1).

Nous sommes donc conduits à établir une distinction entre preuves **par** l'absurde et preuves **de** l'absurde selon la thèse informelle suivante :

> Les *vraies preuves par l'absurde* sont des preuves qui utilisent plus de réduction à l'absurde que ne le réclame la signification même de l'assertion qu'on veut prouver.

Le cas le plus simple d'une *vraie preuve par l'absurde* est celui d'un énoncé de type (E_1) qu'on démontre en réduisant à l'absurde l'énoncé de type (U_1) correspondant. Supposons par exemple qu'on ait réduit à l'absurde l'hypothèse

(B) $\quad \forall m \; \alpha(m) \geq 3$

La preuve que (B) se réduit à l'absurde ne fournit pas en général d'entier m *tel que* $\alpha(m) \leq 2$ et donc *ne réalise pas la signification naturellement attachée à l'énoncé*

(A) $\quad \exists m \; \alpha(m) \leq 2$

La signification de (B) n'est autre que l'absurdité de (A), sauf à admettre que l'infinité des vérifications naïvement comprises dans l'énoncé (B) puisse se produire "en acte" dans quelque univers mathématique idéal mais inaccessible à l'entendement humain. Toute preuve de (B) (ou d'un énoncé du même type) est donc une preuve **de** l'absurde et non une preuve **par** l'absurde.

Par contre la signification de (A) est supérieure à l'absurdité de (B). Prouver (A) par l'absurde c'est prouver que l'absurdité de (A) se réduit à l'absurde, mais cela ne fournit pas l'entier réclamé.

Nous allons présenter un cas concret lié à l'irrationalité de $\sqrt{2}$.

Positif et négatif : le cas de l'irrationalité d'un nombre réel

Tout d'abord quelques définitions dans la lignée de la théorie d'Eudoxe.

Un nombre réel x est considéré comme donné par une suite x_n de rationnels qui converge vers x avec

$$|x_n - x_{n+1}| \leq 1/2^{n+1} \text{ (d'où } |x - x_n| \leq 1/2^n)$$

Deux réels représentés par les suites x_n et y_n sont (définis comme) égaux si

$$\forall n \ |y_n - x_n| \leq 2/2^n$$

Il s'agit d'une notion de type (U_1).
Ils sont distincts si

$$\exists n \ |y_n - x_n| > 2/2^n$$

Il s'agit d'une notion purement existentielle, de type (E_1).

Démontrer que deux nombres réels sont distincts en réduisant à l'absurde l'hypothèse selon laquelle ils seraient égaux, c'est faire une vraie preuve par l'absurde, qui ne réalise pas complètement la signification de l'énoncé démontré.

Un nombre réel x est dit positivement irrationnel s'il est distinct de tout nombre rationnel. C'est une notion de type (U_2).

Le nombre x est dit négativement irrationnel s'il est absurde qu'il soit égal à un nombre rationnel.

Lorsqu'on démontre qu'un nombre réel x est négativement irrationnel, il s'agit d'une vraie preuve par l'absurde du fait qu'il est positivement irrationnel. Plus précisément, pour chaque rationnel r on a une preuve par l'absurde du fait $x \neq r$, qui est de nature (E_1).

Dans la section précédente, nous avons montré que le carré d'un rationnel n'est jamais égal à 2 . On en déduit que $\sqrt{2}$ est négativement irrationnel. En effet, si deux réels sont égaux, leurs carrés aussi. Mais le carré d'un rationnel n'est jamais égal à 2 (preuve de la section 1). Pour autant, nous n'avons pas prouvé l'irrationalité positive de $\sqrt{2}$, *i.e.* nous n'avons pas précisé de combien $\sqrt{2}$ s'écarte de chaque nombre rationnel. Prouver l'irrationalité positive de $\sqrt{2}$ c'est donner une procédure explicite qui minore l'écart entre $\sqrt{2}$ et un rationnel arbitraire $r = m/p$. Cette procédure n'a pas été donnée, mais elle peut néanmoins être facilement déduite :

Puisque m^2 et $2p^2$ sont deux entiers distincts on a $|m^2 - 2p^2| \geq 1$. Donc

$$\begin{aligned} &|m^2 - 2p^2|/p^2 \\ &= |r^2 - 2| \\ &= |r - \sqrt{2}|(r + \sqrt{2}) \geq 1/p^2 \end{aligned}$$

Comme $1,4 < \sqrt{2} < 1,5$ on se ramène au cas où $1 < r < 2$ (donc $1 < r + \sqrt{2} < 3$) et alors

$$| r - \sqrt{2} | \geq 1/3p^2 .$$

Le cas que nous venons d'examiner est assez typique des "vraies preuves par l'absurde" qui foisonnent dans les livres de mathématiques. Bien qu'il soit souvent facile de fournir la preuve directe donnant toute l'information souhaitée, on se contente d'une preuve par l'absurde qui ne réalise pas pleinement la signification de l'énoncé.

Positif et négatif : un peu d'algèbre linéaire réelle

Il n'est pas évident de trouver des exemples élémentaires (8) de "vrais raisonnements par l'absurde" dans les cours de mathématiques.

C'est peut être en algèbre linéaire qu'on est le plus immédiatement tenté d'en faire.

Considérons une matrice réelle A de type $n \times n$ et notons f l'application linéaire associée. On munit l'espace $\mathbb{R}^n$ d'une norme usuelle. On peut alors démontrer les deux chaînes d'équivalence suivantes (9).

$$\text{A est inversible} \Leftrightarrow \text{f est surjective} \Leftrightarrow \det(A) \neq 0 \Leftrightarrow \forall x \,(\| x \| \neq 0 \Rightarrow \| f(x) \| \neq 0) \Leftrightarrow \exists c > 0\ \forall x\ \| f(x) \| \geq c \| x \|$$

et

$$\text{non} (\det(A) = 0) \Leftrightarrow \forall x \,(\| f(x) \| = 0 \Rightarrow \| x \| = 0) \quad \text{(c.-à-d. Ker(f) = \{0\})}$$

Reformulé en termes d'indépendance linéaire, la première chaîne d'équivalence correspond à une notion positive d'indépendance linéaire des colonnes de A, tandis que la deuxième chaîne correspond à une notion négative d'indépendance linéaire (10). Lorsqu'on considère des matrices à coefficients rationnels, les deux notions sont les mêmes parce qu'il y a un test d'égalité à zéro pour un nombre rationnel. Par contre, pour des matrices à coefficients réels, les deux notions ne coïncident pas et il est souvent tentant de prouver l'indépendance linéaire sous la forme faible : une combinaison linéaire qui s'annule a nécessairement tous ses coefficients nuls.

(8) Les exemples plus sophistiqués sont monnaie courantes. Souvent un autre ingrédient de la perte d'effectivité dans le raisonnement est alors l'axiome du choix, qui réclame une autre analyse spécifique.

(9) Nous donnons les preuves de ces équivalences en annexe

(10) L'indépendance linéaire forte d'un système de vecteurs signifie que si une combinaison linéaire a au moins un coefficient non nul (hypothèse de type (E1)) elle est un vecteur non nul (c.-à-d. de norme non nulle, conclusion de type (E1)). L'indépendance linéaire faible signifie la contraposée de l'implication précédente: si une combinaison linéaire est nulle (hypothèse de type (U1)) alors tous les coefficients sont nuls (conclusion de type (U1)).

Prenons par exemple l'espace E des polynomes réels de degré < n. Soient x_1, x_2, ... , x_n des réels distincts, et considérons l'application linéaire suivante :

$$f : E \to \mathbb{R}^n, P \mapsto (P(x_1), \dots , P(x_n))$$

Il est agréable (et élégant) de démontrer que Ker(f) = {0} en disant qu'un élément P dans le noyau doit être divisible par $(X - x_1) \dots (X - x_n)$. Cependant, pour démontrer que f est surjective, il vaut mieux utiliser les polynomes d'interpolation de Lagrange.

3. TOUT RAISONNEMENT PAR L'ABSURDE SE RETOURNE EN UN RAISONNEMENT DIRECT SI ON ADMET LE PRINCIPE DU TIERS EXCLU

La remarque selon laquelle tout raisonnement «par l'absurde» peut se retourner en un raisonnement direct a souvent été faite. Nous allons mettre en évidence qu'elle s'appuie sur un principe général de tiers exclu qui nie la distinction naturelle entre assertions de types logiques différents.

Prenons un énoncé (A) de type (E_1) se situant dans un contexte général que nous résumons en (H) (les hypothèses données par le contexte).

Supposons que nous ayons prouvé (A) par l'absurde en utilisant un raisonnement structuré comme suit *(figure 6)* :

Des hypothèses (H) on déduit les théorèmes, T, S, U.
De T et non A on déduit C.
De S et C on déduit D.
De U et C on déduit E.
De D on déduit F et de E on déduit G.
De F et de G on déduit l'absurdité 1 = 0.

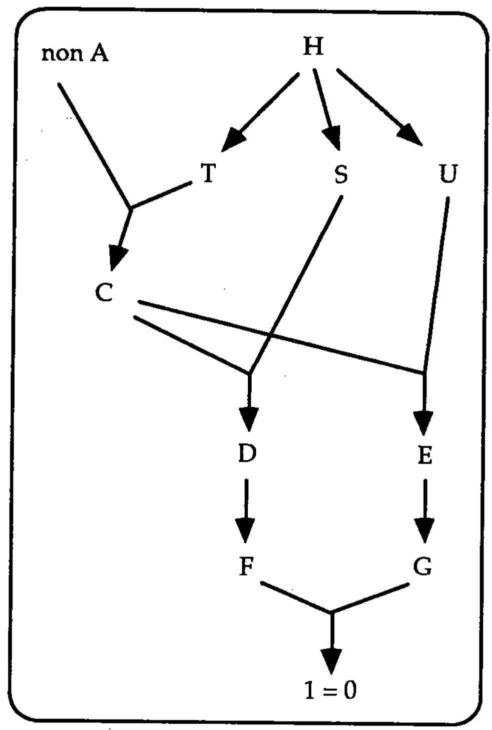


Fig. 6

Une "preuve directe" déduite de la précédente consiste à retourner partiellement l'arbre initial de la preuve à l'envers pour aboutir à la conclusion non non A.

Ce retournement est basé sur les principes (incontestables) que

si on a (H, C, D) $\Rightarrow$ E
alors on a (H, C, non E) $\Rightarrow$ non D

si on a (H, C, D) $\Rightarrow$ non E
alors on a (H, C, E) $\Rightarrow$ non D

En outre, avec l'exemple que nous avons pris, on a besoin du principe (contestable) du tiers exclu sous la forme suivante :

si F et G sont incompatibles alors on a non F ou non G

La preuve examine séparément les deux cas (*a priori* non exclusifs) possibles : non F d'une part, non G d'autre part.

Dans chaque cas elle établit non non A.

Enfin le fait qu'on puisse déduire A de non non Arésulte également du principe du tiers exclu (11). Le renversement de la preuve en "preuve directe" donne alors le résultat suivant :

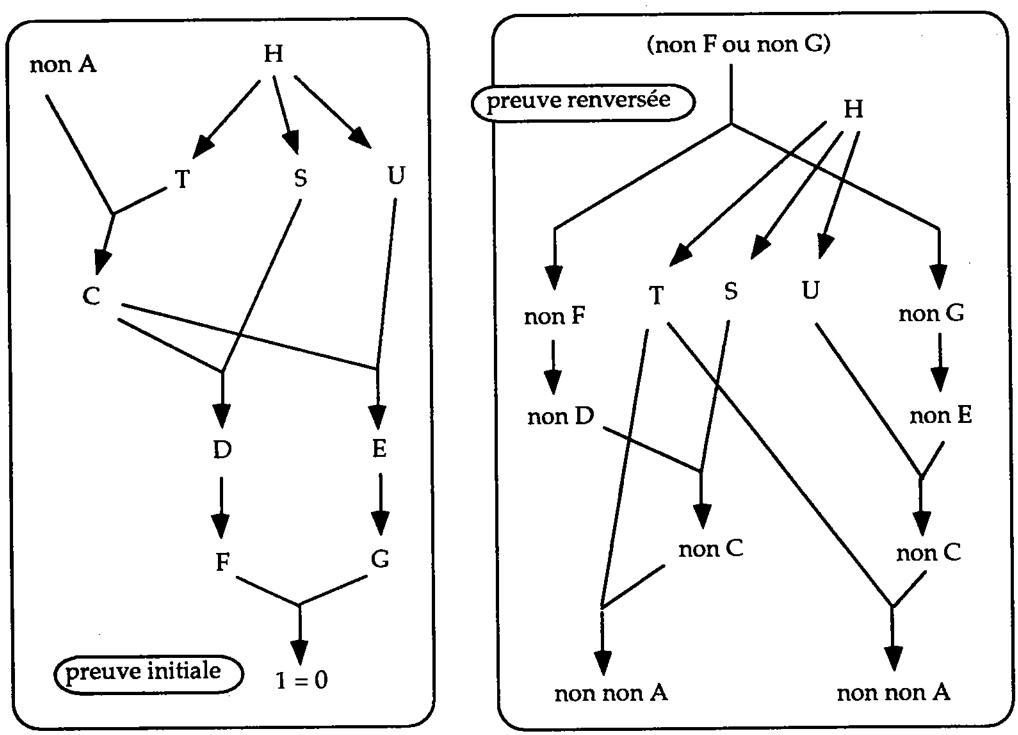


Fig. 7

Comme nous l'avons déjà signalé, deux opérations cruciales et problématiques dans ce renversement sont d'une part le remplacement de l'absurdité de F et G par la disjonction non F ou non G *(fig. 8)*.

(11) Le raisonnement usuel est le suivant : puisque on a A ou nonA, on peut traiter les deux cas séparément. Dans le premier cas, A est vrai par hypothèse. Dans le deuxième cas, on aurait à la fois nonA et non nonA, donc ce cas ne peut pas se produire.

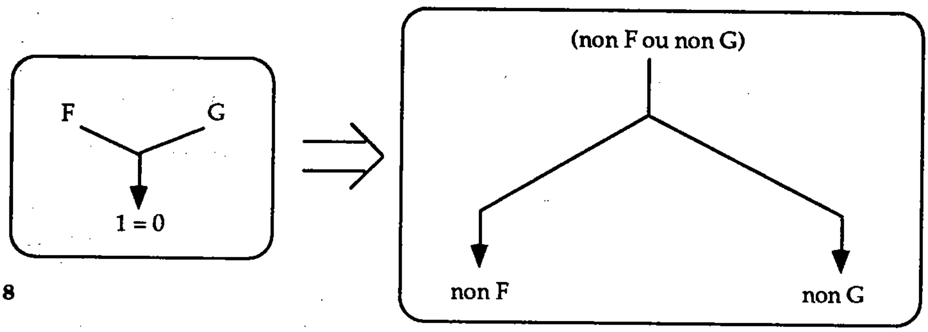


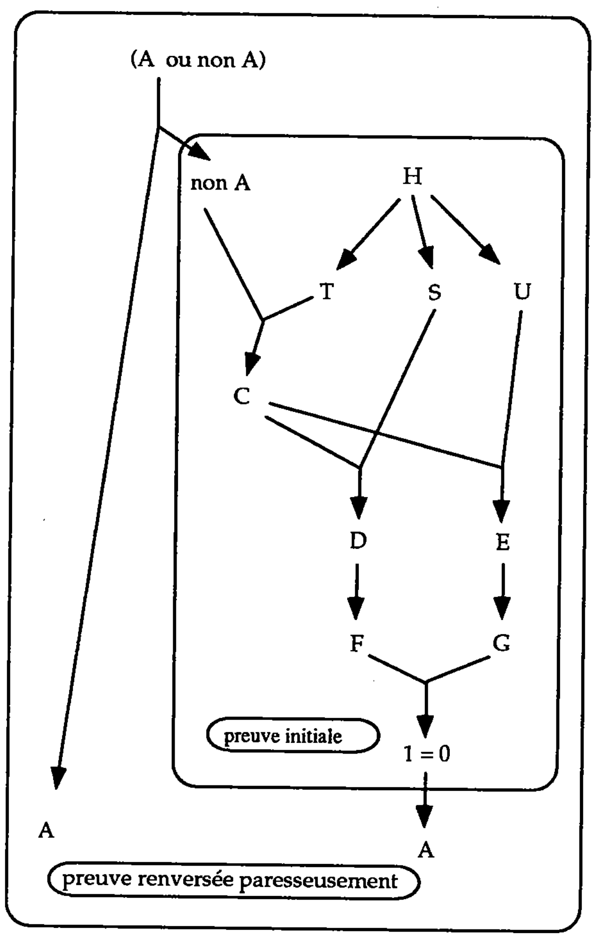
Fig. 8

et d'autre part le passage de non non A à A.

Pour montrer à quel point le renversement proposé ci-dessus nous paraît peu convaincant, nous en proposons un autre, nettement plus provocateur, mais basé au fond sur les mêmes principes. La preuve "directe" suivante est elle aussi basée sur le principe de tiers exclu :

> On examine séparément ce qui se passe dans les deux seuls cas possibles : A d'une part, non A d'autre part.
> On démontre dans les deux cas que A est vérifié.
> Le deuxième cas est examiné selon la preuve précédente, puis A est déduit de l'absurdité 1 = 0.

Beaucoup de gens ne trouvent cependant pas cette preuve très directe, malgré le fait d'expérience bien établi qu'on peut prouver n'importe quoi à partir de l'absurde (il est par exemple facile de prouver 7 < 3 à partir de 1 = 0 par des raisonnements incontestables).



CONCLUSION

Les raisonnements par l'absurde peuvent être classés en deux catégories distinctes.

Ceux qui réalisent pleinement la signification de l'énoncé recherché : cette signification est que quelque chose est absurde, et la preuve est alors une preuve de l'absurde.

D'autre part, ceux qui ne réalisent pas pleinement la signification de l'énoncé recherché. Dans ce cas, l'utilisation du principe du tiers exclu permet de rétablir une preuve sous forme directe. Mais l'utilisation du principe du tiers exclu conduit à une étude cas par cas alors même que la signification de cette disjonction n'est pas réalisable en pratique. Au bout du compte, le rétablissement sous forme directe n'est qu'illusoire au regard du but recherché.

Remerciements : Merci à René Guitart pour sa relecture attentive et ses suggestions pertinentes.

PETITE BIBLIOGRAPHIE

BISHOP E., BRIDGES D. : *Constructive Analysis*, Springer-Verlag, 1985.

BRIDGES D., RICHMAN F. : *Varieties of Constructive Mathematics,* London Math. Soc. LNS 97, Cambridge University Press, 1987.

MINES R., RICHMAN F., RUITENBURG W. : *A Course in Constructive Algebra,* Springer-Verlag, Universitext, 1988.

LOMBARDI H. : *Mathématiques Constructives*, Brochure de l'IREM de Besançon, 1994.

ANNEXE

Nous donnons ici des preuves d'algèbre linéaire sur $\mathbb{R}$ qui ont été promises.
On considère une matrice réelle A de type $n \times n$ et on note f l'application linéaire associée. On munit l'espace $\mathbb{R}^n$ d'une norme usuelle, par exemple la norme euclidienne canonique. On doit montrer les deux chaînes d'équivalence suivantes.

(i) A est inversible $\Leftrightarrow$ (ii) f est surjective $\Leftrightarrow$ (iii) $\det(A) \neq 0 \Leftrightarrow$
(iv) $\forall x\ (\ \| x \| \neq 0 \Rightarrow \| f(x) \| \neq 0\ )$ $\Leftrightarrow$ (v) $\exists c > 0\ \forall x\ \| f(x) \| \geq c \| x \|$

et

(vi) non $(\det(A) = 0) \Leftrightarrow$ (vii) $\forall x\ (\ \| f(x) \| = 0 \Rightarrow \| x \| = 0\ )$ (c.-à-d. $\mathrm{Ker}(f) = \{0\}$)

On montre d'abord la première chaîne d'équivalence. On dit qu'un vecteur est "non nul" pour dire qu'au moins une de ses coordonnées est un réel distinct de 0 , ce qui revient à dire que la norme du vecteur est distincte de zéro (c'est donc une notion positive, de type purement existentiel).
On note A* la matrice "transposée des cofacteurs" de A.

(i) $\Leftrightarrow$ (iii) Les identités

$$\det(AB) = \det(BA) = \det(A).\det(B)$$

et

$$A\,A^* = \det(A)\,I_n = A^*\,A$$

prouvent les équivalences suivantes valables dans le cadre plus général des matrices carrées à coefficients dans un anneau commutatif arbitraire

A inversible à droite $\Leftrightarrow$ A inversible à gauche $\Leftrightarrow$ det(A) inversible

On conclut en remarquant qu'un réel est non nul si et seulement si il est inversible.

(i) $\Rightarrow$ (ii) est immédiat

(ii) $\Rightarrow$ (i) est généralement vrai pour n'importe quel anneau commutatif : on considère des vecteurs $y_1, \dots, y_n$ qui ont pour images les vecteurs de la base canonique $e_1, \dots, e_n$, on définit une application linéaire u en demandant que $u(e_i) = y_i$. On a par construction $u \circ f = \mathrm{Id}$ donc f est inversible.

(i) $\Rightarrow$ (v) Considérons la matrice A^{-1} (qui représente f^{-1}). Une constante c convenable peut être calculée explicitement à partir d'une majoration des coefficients de A^{-1}, donc à partir d'une majoration des coefficients de A et d'une minoration de la valeur absolue de det(A).

(v) $\Rightarrow$ (iv) est immédiat.

(iv) $\Rightarrow$ (i) Supposons (iv). Soient $x_1, \dots, x_n$ les colonnes de A , c.-à-d. les images $f(e_i)$ des vecteurs de la base canonique. Montrons qu'on peut appliquer le procédé d'orthogonalisation de Schmidt à ce système de vecteurs. Au départ $x_1 \neq 0$ parce que $e_1 \neq 0$. On suppose qu'on a construit un système orthonormé $g_1, \dots, g_k$ engendrant le même espace que $x_1, \dots, x_k$ (plus précisément pour $i = 1, \dots, k$, $g_i = f(h_i)$ où h_i est une combinaison linéaire explicite de $e_1, \dots, e_i$) on considère

$$y_{k+1} = x_{k+1} - (< g_1,x_{k+1} > g_1 + \dots + <g_k,x_{k+1}> g_k)$$

on a

$$y_{k+1} = f(e_{k+1} - (<g_1,x_{k+1}> h_1 + \dots + <g_k,x_{k+1}> h_k))$$

le vecteur ($<g_1,x_{k+1}> h_1 + \cdots + <g_k,x_{k+1}> h_k$) est une combinaison linéaire de $e_1, \dots, e_k$ donc y_{k+1} est non nul comme image par f d'un vecteur non nul. On peut donc poser

$$g_{k+1} = y_{k+1} / \| y_{k+1} \|$$

A la fin du processus on a construit une base orthonormée de R^n qui est triangulaire par rapport à $x_1, \dots, x_n$. Donc A est inversible.
Montrons maintenant le deuxième type d'équivalence.

(vi) $\Rightarrow$ (vii) On suppose qu'il est absurde que det(A) = 0 . Soit X un vecteur colonne tel que AX = 0 . On veut montrer que X est nul, c.-à-d. réduire à l'absurde l'hypothèse selon laquelle il serait non nul. Supposons le donc non nul. On a

$$0 = A^*0 = A^*AX = \det(A)\,X$$

Comme X est non nul, cela implique det(A) = 0 , ce qui est absurde par hypothèse.

(vii) $\Rightarrow$ (vi) On suppose maintenant Ker(A) = {0} et det(A) = 0 et on veut montrer que c'est absurde. On écrit le théorème de Cayley Hamilton, avec det(A) = 0

$$A^n + s_1 A^{n-1} + s_2 A^{n-2} + \dots + s_{n-1} A = 0$$
$$A (A^{n-1} + s_1 A^{n-2} + s_2 A^{n-3} + \dots + s_{n-1} I_n) = 0$$

donc comme Ker(A) = {0} tout vecteur dans l'image de

$$A^{n-1} + s_1 A^{n-2} + \dots + s_{n-1} I_n$$

est nul, c.-à-d.

$$A^{n-1} + s_1 A^{n-2} + \dots + s_{n-1} I_n = 0$$

donc $s_{n-1} \neq 0$ car si s_{n-1} _ 0 A est inversible. Donc

$$A^{n-1} + s_1 A^{n-2} + \dots + s_{n-2} A = 0$$

En recommençant le même raisonnement, on tue les uns après les autres les coefficients s_i tout en faisant descendre le degré du polynome qui annule A . On aboutit à A = 0 ce qui est absurde puisque Ker(A) = {0}.