# Divers

Marc SAGE

## Table des matières

# 1 AC pour Baire

Tu construis une suite de boules en choisissant à chaque étape une boule suffisament petite incluse dans l'intersection de l'ouvert dense et de la boule précédente.

David avait expliqué qu'on peut se passer de l'axiome du choix en se restreignant aux boules de centre et rayon rationels (dans un R^n, mais on peut généraliser à un complet dans lequel on dispose d'une base de voisinages dénombrable), on fixe une bijection avec N, et comme fonction de choix, on prend simplement la plus petite pour l'ordre hérité de N par la bijection.

# 2 Ensemble totalement ordonné où toute partie dénombrable est majoré

Un des résultats qui m'a le plus marqué, c'est l'existence d'un ensemble totalement ordonné dans lequel toute partie dénombrable est majorée, c'était une question que j'avais posée au thé, en début de première année, et Joël R. m'avait expliqué ça, en particulier il y avait trois fois par phrase le mot "cofinal".

Yves, 13 mars 2004, 16h

# 3 Ordre total sur les corps

Let me start with some definitions : an ordering on a field is exactly what you think it is (a field with a total order <= such that a<=b implies a+x<=b+x and 0<=a,b implies 0<=ab). A rather wonderful result is that a field admits an ordering iff -1 isn't a sum of squares in the field. Of course fields may admit many orderings : for example the field Q(sqrt(2)) admits two natural maps into the reals, giving two rather different orderings on it.

If a field admits an ordering then it has characteristic zero, and the induced ordering on the copy of the rationals living in the field is the usual one. Say that an ordering on a field F is "archimedean" if, for all f in F, there's a rational number r with r>f. To put an archimedean ordering on a field is just to give an embedding of that field into the reals (the rationals are going to be dense in F, so, for f in F, consider the set of rationals that are less than f etc etc).

Let's say that an ordering that is not archimedean is "non-archimedean". Note that this isn't the kind of "non-archimedean" that people studying the p-adic numbers think about ; that's something a bit different (the p-adic numbers aren't an ordered field—indeed -1 is always a sum of squares). Non-archimedean orderings certainly can exist on fields : for example the field Q(X) (a rational function field in 1 variable) has lots of archimedean orderings (just map Q(X) into the reals by sending X to a fixed transcendental number) but also non-archimedean ones too (if f is in Q(X) then you can define an ordering by setting f>0 iff f(x) is ultimately always positive for x>>0, and then g>h iff g-h>0 (a trick I learnt on s.m.r a few months ago !) ; this way X is bigger than every rational number).

Finally, the question ! Say F is a field and x is in F.

If F admits an archimedean ordering such that x becomes positive, and F also admits a non-archimedean ordering such that x becomes negative, then does F admit an archimedean ordering such that x becomes negative ?

That is—if there's no algebraic obstruction to embedding F into the reals, and no algebraic obstruction to making x negative, can I do them both at once ?

I believe I have a counterexample.

Start with Q(x) (rational functions in one indeterminate x with rational coefficients) and adjoin a square root of each polynomial x(x+n) for each positive integer n. Let F be the resulting field (just to clarify : this means, obviously, that F adjoins the square root of every polynomial of the form (x+m)(x+n) for m and n nonnegative integers).

The existence of a square root guarantees that, for any ordering of F, the element x(x+n) is positive, so either x>0 either x<-n. So x must be either positive or less than any integer : so there is no archimedean ordering of F making x negative.

However, taking any positive transcendental real number value for x embeds F in the reals making x positive. But we can also embed it in, say, the field of Laurent series in 1/x, which can be ordered by making x negative and less than any integer.

# 4 Ordre total sur les ensembles

Theorem : Every partially ordered set can be extended to a total order.

If $(P, \leq)$ is a partial order, and we have a well-ordering on the set $P$, then we define :

$$I(x) = \{z \leq x \ ; \ z \in P\}$$

and extend $\leq$ by defining : $xRy$ si $x = y$ or if the least element of the symmetric difference between $l(x)$ and $l(y)$ (under the well-ordering of $P$) is $\leq y$.

Now $R$ is a total order and $x \leq y$ implies $xRy$.

Transitivité ?

For distinct $x, y, z$ (non-distinct transitivity is easy), proof by contradiction. We'll use "$P$" for the poset order and $<$ for our well-order. Assume : $xRy$ and $yRz$ and $zRx$.

Then the smallest element $u$ (in the well-ordering) of $i(x)\Delta i(y)$ is in $i(y)$

The smallest element $v$ of $i(y)\Delta i\,(z)$is in $i(z)$.

The smallest element w of $i(x)\Delta i(z)$ is in $i\,(x)$.

Now, if $w$ is in $i(y)$, then, since $w$ is not in $i(z)$, $w$ is in $i(y)\Delta i(z)$. So $v < w$, since the smallest element of $i(y)\Delta i\,(z)$ is in $i(z)$.

So we know that $v$ is in $i(x)$, or $v$ would be a smaller element of $i(x)\Delta i(z)$.

Since $v$ in $i(x)\setminus i(y)$, then $v$ has to be greater than $u$. So $u < v < w$.

If $w$ is not in $i(y)$, then $w$ is in $i(x)$ delta $i(y)$. So $u < w$.

In both cases, we see that $u < w$. But then, $xRy$ and $yRz$ and $zRx$ is symmetric. So this means that $u < w$, $w < v$, $v < u$. Contradiction.

Whew, that is much detail to pick through. In the mean time another proof was presented in sci.math. This one apears even more 'constructive' and is much simplier using known constructions and theorems of order theory.

Let $(P, \leq)$ be an (partial) ordered set.

Let $c_a = \{x \ ; \ x \leq a\}$

Let $(P, \leq_w)$be a well ordering of P.

Let $C := \{0,1\}^P$ and for $A \subset P$, let $c_A = \chi_A$

Let $(C, \leq_{lex})$ be $C$ lexicographically ordered by $0 < 1$ and $\leq$ :

for $f, g \in C$, let $m(f,g) = \min_{\leq_w} \{x, \ f(x) \neq g(x)\}$

and define $f <_{lex} g$ when $f(m(f,g)) < g(m(f,g))$

C is given the dictionary order, which is linear order.

For $x, y$ in $P$, define $x <<= y$ when $c_x \leq_{lex} c_y$.

$<<=$ is a total order extension of $\leq$ for $P$. Useful to show this is :

lex C linear order. $A \subset B \implies c_A \leq_{lex} c_B$.

$c_A = c_B \implies A = B$ ; $c_x = x_y \implies x = y$

# 5 Cantor-Schroeder-Bernstein

david,7 03 2006 15 48

Cantor n'a jamais démontré le théorème en question : il a vaguement pipoté (vers 1895) que ça devait aller avec un principe de trichotomie qu'il démontrerait ultérieurement (et qui a, en fait, été démontré par Zermelo vers 1908). La première démonstration correcte publiée est due à Bernstein (1898, dans le livre de Borel sur la théorie des fonctions), et il y en a une très semblable de Schröder (1897), mais cette dernière comporte semble-t-il une erreur (je n'ai pas trouvé la référence pour l'examiner).

Sauf qu'en fait le théorème a été démontré pour la première fois par Dedekind en 1887, mais cette démonstration n'a été publiée qu'en 1932, donc personne ne la connaissait, et elle a, entre temps, été redécouverte par

Zermelo en 1906. La terminologie « théorème de Schröder-Bernstein » est due à Zermelo (1906, ou en tout cas dans les *Untersuchungen über die Grundlagen der Mengenlehre* en 1908), ce qui lui donne quand même un cachet de respectabilité (et dans un certain sens c'est celui qui donne le nom qu a raison). Et il est complètement faux de dire que « tout le monde » dit « Cantor-Bernstein » : le Halmos (*Naïve Set Theory*), par exemple, dit « Schröder-Bernstein », et c'est un classique d'entre les classiques. Je n'arrive pas à trouver qui a lancé cette mode de dire « Cantor-Bernstein » à la place. (Bourbaki ne dit rien, puisque Bourbaki ne nomme pas ses théorèmes.)

Actuellement on semble se diriger vers le compromis « Cantor-Schröder-Bernstein » (ou toute autre permutation) : ce qui, somme toute, est assez injuste envers Dedekind qui est le premier à avoir prouvé ce truc, comme envers Zermelo qui est le premier à lui avoir donné un fondement vraiment rigoureux (et à avoir prouvé la trichotomie, et à avoir donné des axiomes à la théorie des ensembles...). Mais bon, « Cantor-Dedekind-Schröder-Bernstein-Zermelo » c'est un peu long, et « CDSBZ » c'est imprononçable...

## 6 Sur les théories consistante prouvant leur non-consistance

c'est essentiellement le contenu du théorème de Gödel : si ZFC n'est pas contradictoire alors (il n'implique pas Consis(ZFC), c'est-à-dire exactement que) ZFC+$\neg Consis(ZFC)n'estpasnonpluscontradictoire.Unethorietellque T =$ $ZFC+\neg Consis(ZFC)dmontresapropreinconsistance(ellea\neg Consis(ZFC)danssesaxiomes, quiimpliquetrivialement\neg Cons$ $commejeviensdeledire-consistantesiZFCl'est.L'ideestquedansunmodlequelconquedeT(quiexistepuisqueTestconsistante)il$ $standardquivrifieleprdicat´coderunedmonstration˘$.

## 7 sur l'omagé-consistance de ZFC

Ce qu'on attend de ZFC, en revanche, c'est qu'elle soit $\omega$-consistante, c'est-à-dire que si elle prouve « il existe un entier naturel x tel que F(x) » alors elle ne prouve pas $\neg F(0) et \neg F(1) et \neg F(2) etainsidesuite. C'estal'idequelesentiersnaturels$ consistance est beaucoup plus forte que la consistance (par exemple, si ZFC est consistante, alors ZFC+$\neg Consis(ZFC) estconsis$ consistante).

Pour une théorie classique, typiquement, même le fait qu'on ait une preuve de A \/ B ne signifie pas qu'on ait une preuve de A ou de B (prendre pour A l'énoncé de Gödel et pour B sa négation !). C'est beaucoup plus fort comme échec (prendre la fonction F(x) qui dit « si x=0 alors A, et si x=1 alors B » : on prouve qu'il existe un x tel que F(x), mais on ne prouve F(x) ni pour 0 ni pour 1...).

Tu me demandes les détails et les subtilités sur le fait que ZFC admette un modèle standard versus le fait qu'il soit $\omega$-consistant. Alors voilà [...]

« il existe un cardinal inaccessible » => « il existe un modèle standard de ZFC » => « ZFC est $\omega$-consistant » => « ZFC est consistant »

## 8 Sur les unions qui n'existent pas – Clôtures algébriques

Si tu as défini des ensembles $U_i$ pour i parcourant un ensemble $I$ (*), comment "construis"-tu la réunion des $U_i$ ?

[chose que tu as probablement souvent considérée, cf. plus bas]

Exercice : proprifier la "démonstration" suivante.

Quand on construit une clôture algébrique d'un corps, on commence souvent par dire : soit $K$ un corps, construisons une extension algébrique $K\prime/K$ tel que tout polynôme irréductible unitaire sur $K$ admette une racine dans $K\prime$. Ensuite, on dit : posons $K_0 = K$, puis par récurrence, $K_{n+1} = K'_n$, on note ensuite $K_\infty$ ="réunion des $K_n$" (ou mieux, une limite inductive dans la catégorie des anneaux), et alors $K_\infty$ est une clôture algébrique de $K$.

Une idée de solution : Ici, les $K_n$, même si on s'est arrangé pour que $K_n$ soit un sous-ensemble de $K_{n+1}$, ne sont *a priori* pas des sous-ensembles d'un grand ensemble donné au départ. On peut s'arranger pour que, à $K$ fixé, on ne retienne que les $K\prime$ parcourant un ensemble donné plus ou moins explicitement. De là, en utilisant

l'axiome de remplacement, on va pouvoir montrer que les $K_n$ vont parcourir un certain ensemble $A_n$. À la fin, on peut appliquer l'axiome des choix dépendants (DC) à cette suite $A_n$ pour trouver une famille compatible de $K_n$, et construire $K\infty$.

[Il y a certainement d'autres manières de s'en sortir dans ce cas précis en utilisant AC : montrer que le cardinal d'une extension algébrique de $K$ est majoré par un certain cardinal, fixer un gros ensemble $\Omega$ de ce cardinal et ne considérer pour les $K_n$ que des structures de corps sur des sous-ensembles de $\Omega$, etc. Une autre manière consiste à choisir pour tout polynôme non constant $P$, un corps de décomposition, prendre le produit tensoriel de tous ces corps de décomposition, et quotienter par un idéal maximal pour obtenir une clôture algébrique.]

26.10.07 12h15

29.199.72.99, dans le message (sciences.maths :16138), a écrit :

Ton exemple me paraît douteux. En effet, si tu prends un élément $x$ de $K_2$, il est algébrique sur $K_1$ et donc sur une extension finie de $K_0$ (celle engendrée par les éléments qui appraissent dans le polynôme minimal de $x$). Du coup, $x$ est déjà algébrique sur $K$, et $K_2 = K_1$.

Mon exemple n'est pas douteux : c'est comme ça qu'Illusie avait construit la clôture algébrique dans son cours d'Algèbre II (et c'est aussi comme ça que fait Lang dans _Algebra_ par exemple). On doit effectivement pouvoir montrer (au moins si $K$ est parfait) que $K_2 = K_1$, mais ton argument me semble insuffisant : si $x$ est un élément de $K_2$, alors certainement $K_1$ contient un conjugué de $x$, mais a priori, il n'est pas tautologique que $K_1$ les contienne tous.

[Si $P$ est un polynôme non nul à coefficients dans $K_0$, on peut construire un corps de décomposition $D/K_0$ de $P$, en en prenant un élément primitif, on peut écrire $D$ comme le corps de rupture d'un autre polynôme, et finalement $K_1$ "contient" le corps de décomposition $D$, de sorte que $P$ est scindé sur $K_1$.]

On peut se demander pourquoi est-ce qu'à ce stade d'un cours, on ne nous dit pas que $K_2 = K_1$ : parce qu'on a pas encore forcément vu la notion de corps de décomposition et montré que cela existait.

Si $K$ n'est pas supposé parfait, je présume qu'au pire, on a $K_3 = K_2$, puisque $K_1$ devrait probablement contenir au moins la clôture parfaite de $K$.

26.10.07 15h13

# 9 Sur les grosses catégories définies par des formules ensemblistes

Tout le monde a la flemme de définir une "grosse" catégorie comme étant donnée par des formules logiques de la théorie des ensembles, par exemple des formules $O(X)$, $F(X,Y,f)$, $C(X,Y,Z,f,g,h)$ :

- un objet de la catégorie $C$ est un ensemble $X$ vérifiant $O(X)$ ;
- si $X$ et $Y$ sont deux objets de $C$, une flèche $X->Y$ est un ensemble $f$ vérifiant $F(X,Y,f)$ ;
- si $X$, $Y$ et $Z$ sont deux objets de $C$, $f : X->Y$ et $g : Y->Z$ des flèches, il existe une unique flèche $h : X->Z$ satisfaisant $C(X,Y,Z,f,g,h)$, c'est ce qu'on appelle la composée de $f$ et de $g$ ;
- [insérer ici les autres axiomes : associativité, existence des identités].

Dire que les Hom doivent être des ensembles, cela s'écrira rigoureusement dans ce cadre en disant : pour tous objets $X$ et $Y$, il existe un ensemble $\mathrm{Hom}(X,Y)$ tel que pour tout ensemble $f$, $f$ appartient à $\mathrm{Hom}(X,Y)$ si et seulement si $F(X,Y,f)$ est vrai.

# 10 Une équivalence avec AC

Montrer que $\bigcup_I \bigcap_J A_{i,j} = \bigcap_{J^I} \bigcup_f A_{i,f(i)}$ Je ne vois vraiment pas comment montrer une inclusion sans AC.

De fait, cet énoncé est exactement équivalent à AC : s'il existe une famille $X_i$ d'ensembles non vides dont le produit cartésien est vide, j'appelle $J$ la réunion des $X_i$ et je pose $A_{i,j} = \emptyset \mathrm{ou} \{\emptyset\}$ selon que $j \in X_i$ ou non. Alors $\bigcup_I \bigcap_J A_{i,j} = \emptyset$, tandis que l'autre est $\{\emptyset\}$ (puisque, par hypothèse, pour tout $f$ dans $J^I$ il existe un $i$ pour lequel $f(i) \notin X_i$).

## 11 Demo intuitive de Zorn

La démonstration du Jech avec ordinaux est quand même plus simple :

Théorème (« lemme de Kuratowski-Zorn »). Soit $(P, <)$ un ensemble partiellement ordonné non vide tel que toute chaîne de $P$ ait un majorant : alors $P$ a un élément maxima.

Démonstration : En utilisant une fonction de choix pour les parties non vides de $P$, on définit par induction $a_\alpha$ =un élément de $P$ tel que $a_\alpha > a_{x_i}$ pour tout $x_i < \alpha$ s'il y en a un.

Clairement, si $\alpha > 0$ est un ordinal limite alors $\{a_{x_i}\ ;\ x_i < \alpha\}$ est une chaine dans $P$ donc $a_\alpha$ existe par hypothèse.

À terme, il existe un $\theta$ tel qu'il n'existe pas de $a_{\theta+1}$ vérifiant $a_{\theta+1} > a_\theta$ : ce $a_\theta$ est alors maximal.

On conviendra que c'est immensément plus court à écrire *et* plus simple à comprendre (puisque ça suit exactement l'intuition « on prend un élément plus grand tant que c'est possible, et on va forcément finir par tomber sur un élément maximal »).

Il me semble que tu glisses sous le tapis la démonstration de l'existence de $\theta$ tel que $a_\theta$ soit maximal. Je présume qu'une manière de le voir consiste à dire que si tel n'était pas le cas, on pourrait injecter la classe des ordinaux dans $P$ en envoyant $\theta$ sur $a_\theta$, du coup, les ordinaux formeraient un ensemble $Ord$, et on pourrait obtenir une contradiction (si $x$ désigne la réunion des éléments de $Ord$, $x$ est un ordinal, donc $x + 1$ aussi, ce qui donnerait finalement que $x$ appartient à $x$, ce qui est exclu par l'axiome de fondation). Ce bout de la démonstration (s'il est juste) me paraît relativement peu intuitif...

24/10/07, 17h58

C'est effectivement l'idée. Je suppose que Jech le passe sous silence parce que c'est un truc qui revient tout le temps avec les ordinaux et qu'on pourrait formuler de façon intuitive comme maxime « on ne tombera jamais à court d'ordinaux (ce serait trop grotesque), au moins quand on manipule des ensembles ».

En l'occurrence, on peut dire la chose comme ceci : à chaque $x$ de $P$ on associe $v(x)$ = le plus petit $\alpha$ tel que $x \leq a_\alpha$ s'il y en a un. L'ensemble de ces $v(x)$ est stable par diminution (puisque $v(a_\alpha) = \alpha$), donc c'est un ordinal, appelons-le $\theta$, et alors $a_\theta$ ne peut pas être défini car on aurait $v(a_\theta) = \theta$...

24/10/07 19h20

## 12 Sur le choix de rationnels

On peut mettre un bon ordre sur $\mathbb{Q}$ (en explicitant une bijection entre $\mathbb{Q}$ et $\mathbb{N}$) et choisir comme point particulier de l'intervalle le plus petit rationnel (pour le bon ordre en question) lui appartenant.

(David 12 12 2002 23h03) De même, je sais qu'on peut construire un modèle de ZF où R est réunion dénombrable d'ensembles dénombrables, ce qui fout un peu la merde quand il s'agit de définir la mesure de Lebesgue ;-) .

## 13 Rant sur énoncés $\Sigma_k$

En fait, ça n'a rien de très subtil.

D'abord, des considérations générales : une proposition (ou un prédicat, s'il y a des variables libres) « $\Pi_0$ » ou « $\Sigma_0$ » sur l'arithmétique est une proposition (ou un prédicat) construite à partir des opérations usuelles, des égalités et des inégalités, des connecteurs logiques, et des quantificateurs _bornés_ - c'est-à-dire des quantificateurs de la forme « pour tout x inférieur à t » (où t est soit un terme, soit une expression dans les variables libres à ce niveau-là). La véracité d'une proposition $\Pi_0$ est testable algorithmiquement en temps fini par un algorithme (et même par un programme primitif récursif), et pour un prédicat $\Pi_0$, il est testable pour toute valeur des variables libres.

Exemple : l'affirmation « 2+2=4 » ou encore « 10^(1020)+1728 n'est pas somme de deux nombres premiers [implicitement : "inférieurs à lui", ce qui borne les quantificateurs] » ou encore « l'entier formé des 1042 premières décimales en base 10 du nombre pi est un nombre premier » sont des propositions $\Pi_0$. Quant à « 2x n'est pas somme de deux nombres premiers », c'est un prédicat $\Pi_0$ de la variable x.

Une affirmation $\Pi_1$, c'est quelque chose qui s'obtient en rajoutant un quantificateur universel non borné devant une affirmation $\Pi_0$, et une affirmation $\Sigma_1$ c'est quelque chose qui s'obtient en rajoutant un quantificateur

existentiel non borné devant une affirmation $\Pi_0$. Et $\Sigma_2$ c'est existentiel devant $\Pi_1$ et $\Pi_2$ c'est universel devant $\Sigma_1$, et ainsi de suite.

Comme on peut toujours ramener les quantificateurs en tête de proposition, et qu'on peut regrouper plusieurs quantificateurs de même type en un seul (en codant des n-uplets d'entiers par des entiers), on peut facilement voir que toute proposition arithmétique est (algorithmiquement) démontrablement équivalente à une certaine proposition de la hiérarchie $\Pi_i$ ou $\Sigma_i$ (bien sûr, $\Sigma_i$ et $\Pi_i$ sont inclus dans tous les $\Sigma_j$ et $\Pi_j$ avec $j > i$).

Maintenant, une proposition $\Pi_0$ est testable en temps fini. Si une proposition $\Pi_1$ est fausse (sa négation est une proposition $\Sigma_1$), il existe un contre-exemple, et le test du contre-exemple se fait en temps fini, ce qui constitue une démonstration. Donc une proposition $\Pi_1$ fausse est toujours réfutable (et une proposition Sigma_1 vraie est toujours démontrable). Du coup, si une proposition $\Pi_1$ est indécidable, elle est vraie. Et cette démonstration-*là*, que je viens de faire, du fait qu'elle est vraie, utilise quoi ? Uniquement la consistance de l'arithmétique.

Donc une démonstration de l'indécidabilité d'une proposition $\Pi_1$ fournit, en ajoutant la consistance de l'arithmétique au système d'axiomes, une démonstration de la proposition elle-même. (La proposition construite par le théorème de Gödel est une proposition $\Pi_1$, ce qui montre que le cas se présente effectivement.

Et c'est ainsi qu'on voit que la consistance de l'arithmétique n'est pas prouvable dans l'arithmétique. Voir mon post sur le sujet, <URL : http ://www.eleves.ens.fr :8080/home/madore/misc/best_of_GroTeXdieck/Goedel> également sur forum sous le Message-ID <9ifar2$bno$1@clipper.ens.fr> ou bien message 936 de forum sciences.)

Voir aussi mon post sur le platonisme sur <URL :http ://www.eleves.ens.fr :8080/home/madore/misc/best_of_GroTeXdieck
ou sur forum <82gm3q$nvq$1@clipper.ens.fr> aka sciences.maths :1498, où je m'interroge sur le sens philosophique de la véracité des affirmations Pi_n et Sigma_n.

Mais revenons à Riemann. A priori ce n'est pas une affirmation arithmétique. Mais en fait, précisément tout ce qui peut se tester algorithmiquement par un programme primitif récursif peut s'écrire comme un prédicat $\Pi_0$ : c'est facile, il suffit d'écrire l'affirmation arithmétique qui dit que le programme trouve tel résultat.

Or l'affirmation « le k-ième zéro de la fonction zêta est situé à une distance au moins 10^-r de l'axe critique » est testable algorithmiquement. En effet, s'agissant d'une fonction holomorphe, il est facile, par le théorème de Cauchy et par intégration numérique, de prouver qu'il existe un zéro dans une certaine région (disons, polygonale), et il est aussi facile de prouver qu'il n'y a pas de zéro dans une certaine région. Bref.

Donc l'affirmation « il existe un k et il existe un r tels que le k-ième zéro de la fonction zêta soit situé à une distance au moins 10^-r de l'axe critique » est une affirmation $\Sigma_1$ sur l'arithmétique, et c'est précisément la négation de l'hypothèse de Riemann, qui est donc $\Pi_1$. On en déduit ce que j'ai dit.

Mais j'insiste sur le fait que ça n'a rien de profond. C'est juste que si HR est fausse on peut donner un contre-exemple numérique explicite, qui constitue une preuve de ce fait. Donc si HR n'est pas falsifiable (modulo la consistance de l'arithmétique), c'est qu'elle est vraie - et la démonstration de ce fait utilise juste la consistance de l'arithmétique.

## 14 théorie des jeux

dans tout jeu fini à deux joueurs (ou quelque chose comme cela), il y a toujours un des deux joueurs qui a une stratégie gagnante (*).

il suffit de faire une récurrence sur le nombre maximal de coups avant la fin de la partie ; on regarde alors les coups que le joueur qui commence peut faire et on utilise l'hypothèse de récurrence pour distinguer deux cas : soit l'autre joueur obtient une stratégie gagnante quoi que le premier fasse et alors c'est le deuxième joueur qui a une stratégie gagnante, soit le premier joueur peut jouer un coup qui le met dans une situation d'avoir une stratégie gagnante ensuite auquel cas en commençant par ce coup il a une stratégie gagnante.

Dans le jeu de la gauffe, *le premier joueur a toujours une strategie gagnante* quelles que soient les dimensions n x p du rectangle. C'est juste que dans le cas carre (n=p) cette strategie est tres facile a expliciter (comme l'a indique Thomas).

Dans le cas general il y a une demonstration diabolique de ce resultat : par l'absurde, si le deuxieme joueur avait une strategie gagnante, eh bien alors le premier joueur n'a qu'a reprendre cette strategie a son compte en imaginant que c'est maintenant lui le deuxieme joueur et qu'il doit repondre au premier coup de son adversaire qui se serait contente d'enlever une seule case au coin du tableau.

# 15 Il est consistant dans ZF que toute fonction $\mathbb{Q}$-linéaire de $\mathbb{R}$ vers $\mathbb{Q}$ est identiquement nulle

on, pour éviter d'invoquer des théorèmes compliqués de Solovay, Pincus, Sacks et Shelah, voilà en gros comment on démontre ça. Sauf qu'en fait je vais prouver un résultat un peu différent, mais du même style, à savoir qu'il est consistant dans ZF que toute fonction $\mathbb{Q}$-linéaire de R vers $\mathbb{Q}$ est identiquement nulle. Je suis sûr qu'une modification assez mineure de l'argument ci-dessous doit permettre de prouver qu'il est consistant que toute fonction $\mathbb{Q}$-linéaire de $\mathbb{R}$ vers $\mathbb{R}$ est $\mathbb{R}$-linéaire (et, du coup, que tout automorphisme de corps de $\mathbb{C}$ est soit l'identité soit la conjugaison complexe), mais j'ai la flemme de continuer à chercher (déjà que j'ai eu plus de mal que prévu pour arriver au résultat ci-dessous, mon intérêt n'est pas tel que je vais encore y passer des heures).

Je considère l'ensemble des produits $I_0 \times I_1 \times I_2 \times ...$, où tous les $I_k$ sont des intervalles ouverts non vides de $\mathbb{Q}$, et où tous sauf un nombre fini sont égaux à $\mathbb{Q}$ lui-même. Cet ensemble est partiellement ordonné pour l'inclusion (enfin, l'inclusion réciproque si on veut les conventions habituelles), et je le prends pour notion de forcing. Il est facile de voir que cette notion équivaut à ajouter $\omega$ réels génériques comme on le fait d'habitude : je la formule avec des intervalles rationnels pour plus de commodité.

J'appelle $(x_0, x_1, x_2, ...)$ la suite de réels génériques ainsi rajoutés, et $(X_0, X_1, X_2, ...)$ leurs noms canoniques (dans le modèle à valeurs booléennes) : on a $(x_0, x_1, x_2, ...)$ dans $I_0 \times I_1 \times I_2 \times ...$ si et seulement si $I_0 \times I_1 \times I_2 \times ...$ est dans l'ultrafiltre générique ; ou encore, $I_0 \times I_1 \times I_2 \times ...$ force $(X_0, X_1, X_2, ...)$ dans $I_0 \times I_1 \times I_2 \times ...$

Là-dessus, je rajoute un groupe de permutations. Soit $G$ le produit d'une famille dénombrable de copies du groupe additif des rationnels, que l'on fait opérer de façon évidente (*i. e.* par addition sur chaque facteur) sur la notion de forcing. On considère le filtre (normal) de sous-groupes de $G$ engendré par les sous-groupes fixant un nombre fini de composantes.

Manifestement, si $h = (r_0, r_1, r_2, ...)$ appartient à $G$, et si $X_k$ est le nom canonique de $x_k$ (dans le modèle à valeurs booléennes), on a $h(X_k) = X_k - r_k$, avec le sens évident de cette expression (disons que la valeur de vérité de « $h(X_k)$ est dans I » est la même que celle de « $X_k$ est dans $I + r_k$ » pour tout intervalle rationnel $I$ ; ou encore, tout $p = I_0 \times I_1 \times I_2 \times ...$ force $h(X_k) = X_k - r_k$.

Soit $N$ le sous-modèle du modèle générique formé des éléments qui ont un nom héréditairement symétrique. Manifestement, les $x_k$ sont tous dans $N$ (en revanche, l'ensemble des $x_k$ n'est pas dans $N$). J'affirme que dans $N$ il n'y a pas de fonction $\mathbb{Q}$-linéaire $\mathbb{R} \longrightarrow \mathbb{Q}$ autre que la fonction nulle. Pour cela, il suffit manifestement de montrer qu'il n'existe pas de fonction $\mathbb{Q}$-linéaire $f : \mathbb{R} \longrightarrow \mathbb{Q}$ telle que $f(1) = 1$.

Supposons que $f$ soit une telle fonction, et $F$ un nom héréditairement symétrique de $f$ dans le modèle à valeurs booléennes. Soit $E$ un ensemble fini de naturels tel que si $h$ de $G$ fixe tout élément de $E$ alors il fixe $F$. Soit $p_0$ une condition de forcing qui force $F$ à être une fonction $\mathbb{Q}$-linéaire $\mathbb{R} \longrightarrow \mathbb{Q}$ et à vérifier $F(1) = 1$. Soit $n$ n'appartenant pas à $E$ ni au support de $p_0$, et soit $s = f(x_n)$. Soit $p$ une condition de forcing plus forte que $p_0$ qui force $s = F(X_n)$. Soit $J$ l'intervalle rationnel non nul à la $n$-ième composante de $p$, soit $r$ un rationnel non nul tel que $J$ rencontre $J + r$, et soit $h = (0, 0, ..., r, ...)$ (où le $r$ est à la $n$-ième position). Alors $p_0$ (donc $p$ aussi) force « $F$ est une fonction $\mathbb{Q}$-linéaire de $\mathbb{R}$ vers $\mathbb{Q}$ vérifiant $F(1) = 1$ » ; $p$ force « $F(X_n) = s$ » ; $h(p)$ force « $(h(F))(h(X_n)) = s$ », soit « $F(h(X_n)) = s$ » puisque $F$ est fixé par $h$, soit encore « $F(X_n - r) = s$ », $p \cap h(p)$ force « $F$ est une fonction $\mathbb{Q}$-linéaire de $\mathbb{R}$ vers $\mathbb{Q}$ vérifiant $F(1) = 1$ et $F(X_n) = s$ et $F(X_n - r) = s$ » (avec $s$ rationnel et $r$ rationnel non nul), ce qui est une contradiction car $p \cap h(p)$ n'est pas vide (puisque $J$ rencontre $J + r$).

Facile et joli.

# 16 axiomatisation de la logique

Il existe de nombreuses autres présentations d'un tel système que nous n'avons pas abordées, comme par exemple les quatre axiomes d'Hilbert-Ackermann, les trois axiomes de Frege-Lukasiewicz. Il existe des systèmes a 9 ou 11 axiomes. On a dénombré une vingtaine de présentations axiomatiques différentes du calcul des propositions. Citons pour la performance le système à un axiome basé uniquement sur l'incompatibilité :

[p | (q | r)] | [(t | (t | t)) | ((s | q) | ((p | s) | (p | s)))]

bien sur il faut modifier la règle de détachement comme suit :

Si a est une thèse et a | (b | c) est aussi une thèse alors on peut admettre c comme thèse.

On peut donner cet axiome sans parenthèses en utilisant la notation de Lukasiewicz :

DDpDqrDDtDttDDsqDDpsDps

http ://www.brouty.fr/Maths/logique1.html

# 17 Pourquoi les théories du second ordre ne peuvent avoir de théorème de complétude

l'ennui, c'est qu'on n'a pas de bonne notion de démonstration pour les théories logiques du second ordre : il ne peut rien y avoir qui vérifie le théorème de complétude de Gödel (pour une raison simple - si on avait une bonne théorie de la démonstration pour la logique du second ordre, alors les énoncés démontrables seraient ceux vrais dans tous les modèles (c'est le théorème de complétude), et ici il n'y en a qu'un, donc on aurait une théorie de la démonstration qui permet algorithmiquement de savoir si un énoncé sur les entiers naturels est vrai ou faux, et c'est évidemment impossible).