ἡὕβρις

Continuum mathématique des ENS

'You are sad,' the Knight said in an anxious tone: 'let me sing you a song to comfort you.'

'Is it very long?' Alice asked, for she had heard a good deal of poetry that day.

'It's long,' said the Knight, 'but very, very *beautiful. Everybody that hears me sing it – either it brings the* tears *into their eyes, or else – '*

'Or else what?' said Alice, for the Knight had made a sudden pause.

'Or else it doesn't, you know. The name of the song is called "Haddocks' Eyes."*'*

'Oh, that's the name of the song, is it?' Alice said, trying to feel interested.

'No, you don't understand,' the Knight said, looking a little vexed.

'That's what the name is called. *The name really* is "The Aged Aged Man."*'*

'Then I ought to have said "That's what the song *is called"?' Alice corrected herself.*

'No, you oughtn't: that's quite another thing! The song *is called* "Ways and Means"*: but that's only what it's* called, *you know!'*

'Well, what is *the song, then?' said Alice, who was by this time completely bewildered.*

'I was coming to that,' the Knight said. 'The song really is "A-Sitting on a Gate"*: and the tune's my own invention.'*

Lewis Carroll, Through the Looking Glass, *chapter 8*

Éditorial

Voici cinq ans qu'Hubris paraît irrégulièrement. En moyenne, un an se passe entre chaque numéro de notre revue théoriquement semestrielle.
Mais le principal est là : Hubris vit encore. Et il a besoin de sang neuf. De nouveaux rédacteurs. Ce nouveau numéro a été écrit exclusivement par des anciens élèves du département de mathématiques.
Pourtant, nul besoin d'être en thèse pour écrire un article dans Hubris. Le cursus du département de mathématiques nous amène très vite (dès la maîtrise, voire même avant) chacun sur des chemins assez différents. Le but – démesuré – d'Hubris était d'éclairer tous ces chemins pour y accueillir des visiteurs.
Toutes vos contributions sont donc les bienvenues. N'hésitez pas à nous contacter pour de plus amples informations, et à visiter notre site web
`www.dptmaths.ens-cachan.fr/eleves/Hubris/`

La Rédaction

Sommaire

Le comité de rédaction attend vos articles

`hubris@dptmaths.ens-cachan.fr`

Alexandre Boisseau (boisseau@lsv.ens-cachan.fr)
Hélène Davaux (davaux@darboux.math.univ-montp2.fr)
Gabriel Dos Reis (dosreis@cmla.ens-cachan.fr)
Nicolas Markey (markey@lsv.ens-cachan.fr)
Vincent Zoonekynd (zoonek@math.jussieu.fr)

Les bienfaits d'Epiménide

Alexandre Boisseau
boisseau@lsv.ens-cachan.fr

L'un d'eux, leur propre prophète[1], *l'a dit :*
Crétois, toujours menteurs, méchantes bêtes, cœurs blasés.
Saint Paul, Nouveau Testament, Epître à Tite (I,12)

Qu'est-ce qu'un paradoxe ? Ou plutôt, qu'est-ce qu'un paradoxe en mathématiques ? On peut en fait accorder à ce mot deux sens différents. Tout d'abord un paradoxe peut simplement être un résultat qui va à l'encontre de l'intuition. On peut citer par exemple le paradoxe de Banach-Tarski : il est possible de partitionner une boule en un nombre fini de morceaux puis de les réassembler différemment afin d'obtenir deux boules de même volume que la première. Un tel paradoxe met en relief certaines différences entre le monde mathématique, idéal sous certains aspects, et le monde réel. Un paradoxe peut également être un résultat qui s'avère être à la fois vrai et faux. Dans la plupart des cas, ceci intervient au cours d'un raisonnement par l'absurde et permet en fait de montrer que l'une des hypothèses faites est fausse. Plus rarement, les seules hypothèses sont celles communément admises et un tel cas de figure oblige à reconsidérer la théorie mathématique utilisée. Ce sont de tels paradoxes que nous nous proposons d'évoquer dans ce qui suit. Plus précisément, nous allons nous concentrer sur l'un deux, le paradoxe du menteur, et nous laisser guider par ses différentes applications, oscillant entre fondements des mathématiques et informatique. Avant d'entrer dans le vif du sujet, signalons que cet article a été rédigé suite à la lecture de [D] que l'on ne peut que conseiller à chacun, logicien ou non.

Le paradoxe du menteur

L'hypothétique Epiménide dont il est question aurait été un grec, crétois de surcroît, qui aurait énoncé la phrase suivante :

« Tous les Crétois sont des menteurs. »

Le caractère (faussement) paradoxal de cet énoncé apparaît lorsqu'on tient le raisonnement suivant :

– soit cette phrase est vraie, dans ce cas les crétois étant des menteurs et Epiménide un crétois, il se doit de mentir, en particulier lorsqu'il prononce cette phrase, qui par conséquent est fausse,
– soit cette phrase est fausse, ainsi les crétois ne sont pas des menteurs, en particulier Epiménide, et cette phrase doit donc être vraie.

Ce raisonnement n'est correct qu'en apparence, en effet il faut prendre garde au fait que si « être un menteur » désigne le contraire de « toujours dire la vérité », alors un menteur est simplement quelqu'un qui ne dit pas toujours la vérité. Ainsi le raisonnement suivant devient exempt de contradiction :

– soit la phrase prononcée par Epiménide est vraie, dans ce cas les crétois sont des menteurs et Epiménide un crétois, or l'hypothèse nous dit qu'il est en train de dire la vérité, ce qui n'est pas contradictoire (une fois n'est pas coutume...)
– soit cette phrase est fausse, ainsi il y a au moins un crétois qui n'est pas un menteur et tout ce qu'on peut en conclure c'est que ce n'est pas Epiménide.

Ce pseudo-paradoxe possède de nombreuses variantes (réellement paradoxales pour leur part) (on pourra consulter [G], relativement ludique), les plus simples, pour aller à l'essentiel, sont :

« Je mens » (sous-entendu : en ce moment même),

« Cette phrase est fausse ».

R. Smullyan présente dans ses livres [S_1, S_2] une autre manière d'obtenir des paradoxes à partir d'énoncés presque semblables à ceux d'Epiménide qu'il n'applique qu'à des personnes qui possèdent la propriété suivante : soit elles disent toujours la vérité (les « purs »), soit elles mentent toujours (les « pires »). Ainsi, il ne rencontre personne pouvant dire :

« Je suis un pire »

et si quelqu'un vient à dire :

« J'ai entendu quelqu'un dire qu'il était un pire »

alors c'est un pire (et il n'a jamais entendu cette phrase...). On peut varier les situations et les raisonnements à l'infini. Le dénominateur commun à tous ces paradoxes est l'autoréférence (considérer le mot « cette » qui fait référence à la phrase elle-même, ou bien le fait qu'Epiménide, en parlant des crétois, parle en particulier de lui-même, *etc*). C'est cette caractéristique qui rend si intéressante et fructueuse leur transposition à des problèmes mathématiques.

[1]Epiménide de Cnosse, poète et philosophe, VII^e et VI^e siècles avant J.C.

Vers la théorie des ensembles

En 1905, Russel construit un ensemble « paradoxal » rappelant le paradoxe du menteur[2]. En effet, l'ensemble considéré par Russel est le suivant :

$$\Omega = \{x \mid x \notin x\}$$

(l'ensemble des ensembles qui ne s'appartiennent pas) et on peut faire un raisonnement semblable à celui que l'on a fait à propos du paradoxe d'Epiménide :

- soit Ω est élément de lui-même (*i.e.* $\Omega \in \Omega$) ce qui veut dire, par définition de Ω que $\Omega \notin \Omega$ ce qui est contradictoire,
- soit Ω n'est pas élément de lui-même (*i.e.* $\Omega \notin \Omega$) et on a alors par définition $\Omega \in \Omega$ ce qui est également contradictoire.

Ainsi, la théorie mathématique considérée à cette époque était contradictoire puisqu'elle autorisait la définition d'un tel ensemble. Par la suite, différentes restrictions furent énoncées afin déviter de tels paradoxes, citons en seulement deux :

- dans la théorie de Zermelo-Fraenkel (qui est celle communément utilisée), on ne peut construire l'ensemble :

  $$\{x \mid P(x)\}$$

  (P désignant une propriété de x) que lorsqu'il a été établi au préalable qu'il existe un ensemble A tel que tout x satisfaisant P est dans A (ce qui n'était pas le cas pour l'ensemble Ω),
- en analysant le paradoxe, Russel et Whitehead ont observé qu'il découlait du cercle vicieux qui apparaît lorsqu'on considère l'expression $x \notin x$. Pour éviter la formation de telles expressions, ils ont donc mis au point une théorie (dite « théorie des types ») dans laquelle chaque objet possède un type (qui est un entier), les objets de type 0 étant appelés « objets de base » et les objets de type $n+1$ étant par définition les ensembles d'objets de type n. L'appartenance d'un objet à un autre est alors une (famille de) relation(s) entre objets de type n et objets de type $n+1$ et l'expression $x \notin x$ n'est pas une expression correcte.

Russel avait déduit sa construction de l'ensemble paradoxal Ω à partir de la démonstration du résultat de Cantor qui énonçait en 1890 que tout ensemble est strictement plus petit que l'ensemble de ses parties[3] (démonstration qui utilisait elle aussi une variante du paradoxe du menteur). De ce résultat, Cantor déduisait entre autres que l'ensemble des réels n'est pas dénombrable et qu'il existe des suites infinies strictement croissantes d'ensembles (en considérant pour un ensemble A quelconque :

$$A < \mathcal{P}(A) < \mathcal{P}(\mathcal{P}(A)) < \ldots)$$

Nous n'allons pas donner ici la démonstration du fait que $A < \mathcal{P}(A)$, mais nous allons prouver le résultat suivant, qui est assez semblable :

Théorème (du point fixe). — ***Pour un ensemble*** A ***quelconque, s'il existe une bijection de*** A ***dans*** A^A ***(l'ensemble des applications de*** A ***dans*** A***) alors toute application de*** A ***dans*** A ***possède un point fixe.***

En fait, lorsque l'ensemble A est infini, $\mathcal{P}(A)$ est en bijection avec A^A et ce résultat est donc équivalent à $A < \mathcal{P}(A)$.

Considérons donc une bijection de A dans A^A (on désignera par $[a]$ l'image de $a \in A$ par cette bijection) ainsi qu'une application :

$$F : \quad A \quad \to \quad A$$

et montrons que F possède un point fixe. Pour $a \in A$, $[a]$ est une application de A dans A et on peut donc considérer $[a](a)$ qui est un élément de A. On pose ensuite $G(a) = F([a](a))$ ce qui définit une application G de A dans A que l'on écrit $G = [g]$ avec $g \in A$. On pose enfin $a_0 = G(g)$ et on obtient :

$$a_0 = G(g) = F([g](g)) = F(G(g)) = F(a_0)$$

ce qui montre que a_0 est un point fixe pour F.

Bien entendu, comme il existe clairement des applications de A dans A qui ne possèdent pas de point fixe (dès que A n'est pas un singleton) on en déduit que A n'est pas en bijection avec A^A. Remarquons que pour construire son ensemble paradoxal, Russel considère les x tels que :

$$\neg(x \in x)$$

tandis que nous considérons la fonction qui à x associe :

$$F([x](x)).$$

En fait, les constructions $x \in x$ et $[x](x)$ sont très semblables, à chaque fois on tente d'« appliquer x à lui-même ». D'autre part, ce qui joue le rôle de F

[2]Les développements historiques évoqués dans cette section et les suivantes sont extraits de [B_5]

[3]On dit q'un ensemble A est strictement plus petit qu'un ensemble B (et on note $A < B$) si et seulement si il existe une injection de A dans B mais pas de bijection, à ne pas confondre avec A strictement inclus dans B

dans la construction de Russel est l'opérateur de négation. De manière très informelle, on peut donc dire que l'obtention du paradoxe découle de la construction d'un point fixe pour la négation.

Ce résultat de point fixe peut paraître peu intéressant puisque les prémisses ne semblent pas pouvoir être satisfaites, excepté dans des cas triviaux. En fait, il prend toute sa valeur si on ne considère pas l'ensemble A^A tout entier mais seulement un sous-ensemble $\mathcal{F} \subseteq A^A$ qui se trouve être en bijection avec A (et posséder en plus certaines propriétés de stabilité). On obtient alors naturellement un théorème d'existence de point fixe pour les éléments de $\mathcal{F}$. De telles constructions sont essentiellement considérées en informatique, dans le cadre de la sémantique du λ-calcul[4]. Contentons-nous ici d'esquisser deux exemples :

- en 1969, D. Scott considère un espace topologique A et montre que sous certaines conditions l'espace des fonctions continues de A dans A est isomorphe à A,
- en 1972, G. Plotkin utilise P_ω (l'ensemble des parties de $\mathbf{N}$), l'ensemble des fonctions associé étant l'ensemble des fonctions $f : P_\omega \to P_\omega$ telles que pour $A \subseteq \mathbf{N}$:

$$f(A) = \bigcup_{I \in \mathcal{P}_F(\mathbf{N})} f(I)$$

  (où $\mathcal{P}_F(\mathbf{N})$ désigne l'ensemble des parties finies de $\mathbf{N}$).

Tout ceci est encore très abstrait, mais nous allons voir dans la section suivante des applications informatiques plus concrètes du paradoxe du menteur.

Vers la calculabilité

Restons pour l'instant dans des considérations de points fixes et considérons un langage de programmation très simple[5] constitué d'expressions e qui sont construites de la manière suivante :

- si x est une variable, alors x est une expression,
- si e est une expression et x une variable, alors :

$$\texttt{fun}\ x \to e$$

  est une expression qui représente la fonction qui à x associe l'objet décrit par l'expression e,
- si e et e' sont deux expressions, alors :

$$e(e')$$

  est une expression qui représente l'application de e à e' (en général, e sera de la forme $\texttt{fun}\ x \to e''$ et dans ce cas la valeur de $e(e')$ est celle de e'' où l'on a remplacé tous les x par e).

Par exemple les expressions suivantes :

$$\texttt{fun}\ x \to x$$
$$\texttt{fun}\ f \to (\texttt{fun}\ x \to f(x))$$

désignent respectivement l'identité et la fonction qui applique son premier argument au deuxième. Dans ce langage de programmation, on peut appliquer n'importe quelle expression à n'importe quelle autre, en particulier à elle-même. On peut ainsi réaliser les mêmes constructions que celles qui nous ont permis d'obtenir des points fixes. On vérifie sans peine que si e est une expression, alors :

$$(\texttt{fun}\ x \to e(x(x)))(\texttt{fun}\ x \to e(x(x)))$$

est un point fixe pour e. Par suite si on considère l'expression :

$$\texttt{fun}\ f \to (\texttt{fun}\ x \to f(x(x)))(\texttt{fun}\ x \to f(x(x)))$$

notée Y, alors quelle que soit l'expression e que l'on considère, $Y(e)$ est un point fixe pour e, *i.e.* :

$$Y(e) = e(Y(e)).$$

Ainsi dans ce langage il y a un moyen uniforme de construire des points fixes. Nous allons voir que ceci permet en particulier de définir des fonctions par récurrence. Considérons par exemple la fonction factorielle fact : $\mathbf{N} \to \mathbf{N}$ définie par :

$$\begin{cases} \mathrm{fact}(0) = 1, \\ \mathrm{fact}(n) = n \times \mathrm{fact}(n-1) \text{ si } n \geq 1. \end{cases}$$

La factorielle peut alors être considérée comme le point fixe de la fonctionnelle :

$$\begin{array}{rccc} T: & (\mathbf{N} \to \mathbf{N}) & \to & (\mathbf{N} \to \mathbf{N}) \\ & f & \mapsto & \begin{bmatrix} \mathbf{N} & \to & \mathbf{N} \\ 0 & \mapsto & 1 \\ n \geq 1 & \mapsto & n \times f(n-1) \end{bmatrix} \end{array}$$

Dans notre langage de programmation, en supposant qu'on dispose des entiers et de l'instruction conditionnelle $\texttt{if} \ldots \texttt{then} \ldots \texttt{else} \ldots$, T se définirait par :

$$\begin{array}{l} T = \texttt{fun}\ f \to \\ \quad \texttt{fun}\ n \to \\ \quad\quad \texttt{if}(n = 0) \\ \quad\quad\quad \texttt{then}\ 1 \\ \quad\quad\quad \texttt{else}\ n \times f(n-1) \end{array}$$

[4] On pourra se reporter à [B₁] ou [L] pour plus de détails sur le λ-calcul

[5] Il pourrait s'agir d'un sous-langage de Lisp

et compte tenu du fait que Y permet d'obtenir des points fixes, la factorielle est définie par :

$$\text{fact} = Y(T).$$

On voit donc ici que l'autoapplication donne une grande puissance au langage en permettant la construction de fonctions définies par récurrence. La contrepartie à cette puissance est qu'on ne peut pas en général assurer que tous les programmes terminent (considérer par exemple le programme :

$$Y(\texttt{fun}\ f \to \texttt{fun}\ x \to f(x))).$$

Il est d'ailleurs amusant de constater que la théorie des types qui est peu employée dans les mathématiques en général, trouve ici sa pleine application : en effet un moyen classique d'empêcher que des programmes puissent s'appliquer à eux mêmes est d'utiliser une notion de typage, qui doit tout de même rester suffisamment souple pour garder des programmes expressifs.

En fait, savoir si un programme termine[6] ou non sur une entrée est indécidable, *i.e.* il n'existe pas de programme m à deux arguments tel que $(m(e))(e')$ nous indique si le programme e termine ou non sur l'entrée e'. Nous allons montrer ce résultat car c'est encore un bel exemple d'utilisation du paradoxe du menteur faisant intervenir l'autoapplication. Pour savoir si un programme e termine sur l'entrée e' il suffirait que l'on dispose d'un programme m possédant la propriété suivante :

> $(m(e))(e')$ termine si et seulement si $e(e')$ ne termine pas

(en effet, il suffirait alors de lancer les deux calculs $(m(e))(e')$ et $e(e')$ en parallèle et on serait assuré que l'un des deux termine).

Supposons donc que l'on dispose d'un tel programme et considérons alors le programme m' définit par :

$$m' = \texttt{fun}\ x \to (m(x))(x)$$

et on regarde ce qui se passe pour $m'(m')$:
- soit $m'(m')$ termine, or $m'(m') = (m(m'))(m')$ qui par définition de m termine si et seulement si $m'(m')$ ne termine pas, ce qui est contradictoire,
- soit $m'(m')$ ne termine pas ce qui par définition de m entraîne que $m'(m')$ termine et on obtient là aussi une contradiction.

On en déduit qu'un tel programme m ne peut pas exister. On va voir dans la section suivante que ces considérations d'aspect pratique possèdent des conséquences mathématiques capitales.

Vers les théorèmes d'incomplétude

Nous allons ici montrer comment à partir d'un résultat d'indécidabilité on peut obtenir le premier théorème d'incomplétude de Gödel. Ce théorème montre que dans toute théorie mathématique raisonnable, il existe des énoncés qui ne sont ni prouvables ni réfutables. La présentation que l'on va donner est en partie inspirée de [S_3] et [CL].

Une théorie mathématique T peut être vue comme la donnée :
- d'un ensemble $\mathcal{E}$ dont les éléments sont appelés les énoncés de la théorie T, muni d'une involution calculable $\neg$ (*i.e.* une application $\neg : \mathcal{E} \to \mathcal{E}$ telle que $\neg\neg e = e$ pour tout énoncé e, $\neg e$ sera appelé la négation de e),
- une notion de prouvabilité qui est représentée par une partie $\mathcal{P}$ de $\mathcal{E}$. On dira qu'un énoncé e est prouvable (respectivement réfutable) dans T si et seulement si $e \in \mathcal{P}$ (respectivement $\neg e \in \mathcal{P}$).

Une telle théorie est dite :
- cohérente si, et seulement si, il n'existe pas d'énoncé qui soit à la fois prouvable et réfutable,
- complète si, et seulement si, tout énoncé est soit prouvable soit réfutable,
- énumérable si, et seulement si, il existe un programme qui consiste à afficher la liste (éventuellement infinie) des énoncés prouvables,
- décidable si, et seulement si, il existe un programme qui pour chaque énoncé e indique si il est prouvable ou non dans la théorie.

Le résultat clé est le suivant :

Théorème. — ***si une théorie est cohérente, complète et enumérable, alors elle est décidable.***

Pour le montrer, construisons (informellement) un programme qui prend en entrée un énoncé e et qui nous dit si e est prouvable ou non. La première chose à faire est de lancer le programme qui énumère tous

[6] Il faudrait définir formellement les notions d'« exécution » et de « terminaison » pour un programme. On préférera se contenter ici d'une notion intuitive. Le lecteur pourra bien entendu se reporter à [B_1] ou [L] pour une définition formelle ou à [B_3] pour une simple introduction

les énoncés prouvables. Comme la théorie est complète, on sait que l'on verra apparaître soit e soit $\neg e$ au bout d'un temps fini. Deux cas se présentent :

- soit on voit apparaître e, dans ce cas e est prouvable,
- soit on voit apparaître $\neg e$, dans ce cas e est réfutable et comme la théorie est cohérente, il n'est pas prouvable.

Dans chacun des cas on peut répondre, soit « e est prouvable », soit « il ne l'est pas ».

Considérons maintenant une théorie dans laquelle il est possible de « faire » des mathématiques. En particulier, cette théorie doit satisfaire un certain nombre de conditions :

- elle est enumérable puisque les énoncés prouvables sont obtenus à partir d'axiomes (qui sont énumérables) en appliquant des règles de déduction qui sont elles aussi énumérables,
- elle doit être suffisamment puissante, en particulier elle doit contenir l'arithmétique et, ce faisant, elle ne peut pas être décidable[7].

En appliquant le résultat précédent, on voit donc qu'une telle théorie ne peut pas être à la fois cohérente et complète. Par conséquent, si on suppose que la théorie que l'on utilise est cohérente, il existe des énoncés qui ne sont ni prouvable ni réfutables. Ce résultat constitue le premier théorème d'incomplétude de Gödel. Le second théorème consiste à expliciter un tel énoncé. On construit pour cela un énoncé noté coh_T qui exprime la cohérence de la théorie T en ce sens que si coh_T est réfutable dans T, alors T n'est pas cohérente. On montre ensuite que si la théorie considérée est cohérente, coh_T n'est pas prouvable (et puisque T est cohérente, il n'est pas réfutable non plus).

Quelques remarques à propos de ces résultats :

- le premier théorème nous dit que si on note $\mathcal{P}$ et $\mathcal{R}$ les énoncés prouvables et réfutables, alors $(\mathcal{P}, \mathcal{R})$ n'est jamais une partition de l'ensemble des énoncés. En effet, soit la théorie est incohérente et $\mathcal{P} \cap \mathcal{R} \neq \varnothing$, soit elle est incomplète et $\mathcal{P} \cup \mathcal{R} \neq \mathcal{E}$,
- par ailleurs, à supposer que la théorie soit cohérente, il est impossible de la compléter afin d'obtenir une théorie qui reste énumérable, cohérente et qui soit complète,
- le résultat sur la cohérence est assez amusant : soit la théorie est cohérente et elle ne peut alors pas prouver sa propre cohérence, soit la théorie est incohérente et alors elle peut prouver sa cohérence (puisqu'une théorie incohérente contient une contradiction et à partir d'une telle contradiction, on peut prouver n'importe quel résultat).

Pour conclure, voici un petit exercice (dont je ne connais pas la réponse) : dans la théorie des ensembles de Zermelo-Fraenkel, qui est la théorie communément utilisée, rien n'interdit *a priori* de considérer l'ensemble :

$$\Omega = \{x \in A \mid x \notin x\}$$

dès que l'on s'est donné un ensemble A. Cette construction (ou tout autre construction faisant intervenir $x \notin x$) est-elle utilisée dans les mathématiques de « tous les jours » ?

Pour en savoir plus...

[B$_1$] Hendrik Peter Barendregt, *The lambda calculus, its syntax and semantics*, North-Holland, 1981.

[B$_2$] John Barwise (ed.), *Handbook of Mathematical Logic*, North-Holland, 1977.

[B$_3$] Alexandre Boisseau, *Lambda calcul*, Hubris (1998), no. 3, 7–12.

[B$_4$] Raphaél Bomboy, *L'axiome du choix*, Hubris (1997), no. 0, 2–7.

[B$_5$] Nicolas Bourbaki, *Éléments d'histoire des mathématiques*, Masson, 1974.

[CL] René Cori et Daniel Lascar, *Logique mathématique (tomes 1 et 2)*, Masson, 1994.

[D] Gilles Dowek, *La logique*, Domino, Flammarion, 1995.

[G] Martin Gardner, *La magie des paradoxes*, Bibliothèque pour la science, Belin, 1980.

[L] René Lalement, *Logique, réduction, résolution*, Masson, 1990.

[S$_1$] Raymond Smullyan, *Le livre qui rend fou*, Dunod, 1984.

[S$_2$] Raymond Smullyan, *Ça y est, je suis fou*, Dunod, 1993.

[S$_3$] Raymond Smullyan, *Les théorèmes d'incomplétude de Gödel*, Masson, 1993.

[7] Il n'est pas surprenant (du moins de nos jours) que l'arithmétique permette de coder de nombreux problèmes indécidables, on pourra consulter l'article de M. Davis dans [B$_2$] à ce sujet

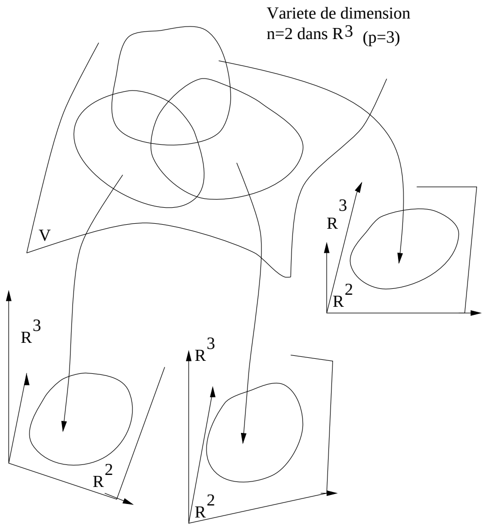
Courbure scalaire et variétés agrandissables

Hélène Davaux
davaux@darboux.math.univ-montp2.fr

Je souhaite donner une idée d'un problème que se posent les géomètres riemanniens en essayant de privilégier l'intuition quitte à perdre une part de la rigueur mathématique de l'exposé. Il s'agit de pouvoir décider si une variété peut ou non porter une métrique à courbure scalaire strictement positive.

Introduction à la géométrie riemannienne...

Les objets qui vont intéresser les géomètres riemanniens sont les *variétés riemanniennes*. Pour les lecteurs qui ne sont pas familiers des variétés différentielles, pensez à des surfaces de $\mathbf{R}^3$ (au sens commun du terme) et plus généralement, à des sous-ensembles de $\mathbf{R}^p$ qui ressemblent localement à $\mathbf{R}^n$ (avec des recollements adéquats de ses « $\mathbf{R}^n$ » locaux) : nous dirons que ce sont des (sous-)variétés de dimension n (dans $\mathbf{R}^p$). Les variétés de dimension 1 sont les courbes et celles de dimension 2 les surfaces (par exemple la sphère, le tore...). Ceci est illutré par la figure suivante :



Construction d'une variété par recollement

Maintenant que nous avons une idée de ce qu'est une variété, nous voulons la munir d'une structure qui permette de mesurer les longueurs des courbes comme nous avons pu le faire dans le cas des surfaces de $\mathbf{R}^3$ en intégrant la longueur du vecteur vitesse. Il faut donc un moyen de mesurer ce vecteur vitesse. Nous définissons tout d'abord l'*espace tangent* en v à la variété V, noté T_vV, comme l'espace vectoriel de tous les vecteurs vitesses des courbes incluses dans V passant par v. C'est bien un espace vectoriel. De plus, sa dimension est exactement n (l'espace tangent à une surface de $\mathbf{R}^3$ est un plan). Nous introduisons alors une *métrique* g sur une variété V, qui est la donnée en tout point v de V d'un produit scalaire g_v sur T_vV, ce produit scalaire dépend différentiablement du point. La longueur d'un chemin $\gamma : [0,1] \to V$ tracé sur V est alors donné par :

$$L(\gamma) = \int_0^1 \left[g_{\gamma(t)}(\gamma'(t), \gamma'(t))\right]^{1/2} \mathrm{d}t.$$

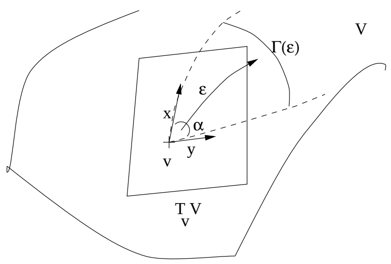
La distance entre deux points de la variété est défini par le minimum des longueurs des chemins reliants les deux points.

Nous voulons maintenant être capable de comprendre la stucture globale de la variété à partir de données infinitésimales. Comme dans le cas des courbes de $\mathbf{R}^2$ ou $\mathbf{R}^3$, nous introduisons la notion de courbure.

Rappelons que, pour une courbe C, donnée par $\gamma : I \to \mathbf{R}^2$, paramétrée par longueur d'arc, la *courbure* en $m = \gamma(t)$ de C est le scalaire $\|\gamma''(t)\|$. Nous pouvons aussi définir une *courbure algébrique*. Le théorème fondamental est qu'une courbe plane est déterminée à un déplacement près par sa courbure algébrique. En particulier, si la courbure est localement nulle, la courbe est localement une droite. Dans le cas des courbes de $\mathbf{R}^3$, il faut un autre paramètre pour définir complètement la courbe : la *torsion*.

Pour des variétés de dimension n quelconque, nous allons définir la *courbure sectionnelle*. Comme pour les courbes, elle permet de mesurer le défaut d'euclidienneté. Plus précisément, pour un petit arc de cercle $\Gamma(\varepsilon)$ obtenu sur V en portant la longueur ε sur les géodésiques (*i.e.* les chemins de longueurs critiques — pas forcément minimaux — par exemple les grands cercles pour la sphère) issu du secteur d'angle α déterminé par x et y, où x et y sont des vecteurs indépendants unitaires tangents à la variété en v (voir figure ci-après), nous pouvons donner un développement limité de la longueur de l'arc $\Gamma(\varepsilon)$:

$$L(\Gamma(\varepsilon)) = \alpha\varepsilon(1 - \varepsilon^2 \sec_v(x,y)/6 + o(\varepsilon^2))$$



Signification locale de la courbure sectionnelle

où $\sec_v$ désigne la courbure sectionnelle en v (nous disons sectionnelle car ici nous venons de nous intéresser au comportement local dans le plan (la section) engendrée par les vecteurs x et y). Remarquons que cette définition n'a pas de sens dans le cas des variétés de dimension 1 (*i.e.* pour les courbes).

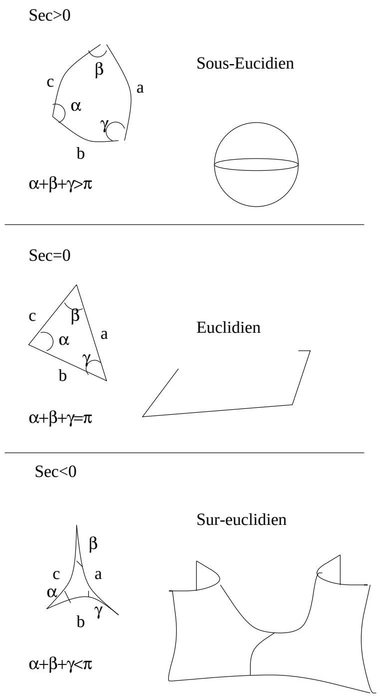
Par exemple, dans le plan $\mathbf{R}^2$, quelque soit le point où nous nous plaçons, nous avons $L(\Gamma(\varepsilon)) = \alpha\varepsilon$, d'où $\sec(x, y) = 0$: nous dirons que la courbure sectionnelle est constante, égale à 0. Pour la sphère unité S^2, quelque soit le point où nous nous plaçons, nous avons

$$L(\Gamma(\varepsilon)) = \alpha \sin \varepsilon = \alpha\varepsilon(1 - \varepsilon^2/6 + o(\varepsilon^2)),$$

donc la courbure sectionnelle est constante, égale à 1 ; pour celle de rayon r, la courbure sectionnelle est constante, égale à $1/r^2$.

Comme attendu, la courbure sectionnelle mesure exactement le défaut d'euclidienneté de (V, g) : cette variété est localement isomorphe à l'espace euclidien (nous dirons alors qu'elle est plate) si et seulement si sa courbure sectionnelle est nulle. Ainsi pour une sphère de grand rayon (par exemple la terre), la courbure sectionnelle tend vers zéro, « la sphère devient plate », ce qui est admis par tous les habitants de la planète (à part, peut être, les montagnards).

Le signe de cette courbure a même une interprétation géométrique en terme de triangles (voir figure ci-contre). En effet, selon le signe ($> 0, = 0, < 0$) de la courbure sectionnelle, la somme des angles intérieurs d'un triangle tracé sur la variété est supérieure, égale ou inférieure à π.



Interprétation du signe de la courbure sectionnelle

... et à la courbure scalaire

En fait, nous allons nous intéresser à une courbure plus faible : la *courbure scalaire*. La signification infinitésimale de la courbure scalaire, notée $\mathrm{sc}_v(V, g)$, est révélée par la formule suivante reliant le volume (longueur en dimension 1, surface en dimension 2) des ε-boules de V (segments centré en dimension 1, disques en dimension 2) de centre v et de l'ε-boule euclidienne B_ε :

$$\mathrm{vol}B_v(V, \varepsilon) = (1 - \varepsilon^2\alpha_n \mathrm{sc}_v(V, g) + o(\varepsilon^2))\mathrm{vol}(B_\varepsilon)$$

où $\alpha_n = [6(n+2)]^{-1}$.

Ainsi, si la courbure scalaire en v est strictement positive, alors le volume des ε-boules de V en v est strictement inférieur au volume de la boule euclidienne de rayon ε, pour ε suffisamment petit. Inversement, si le volume des ε-boules de V en v est inférieur ou égal au volume de la boule euclidienne de rayon ε, pour ε suffisamment petit, alors la courbure scalaire est positive ou nulle en v. En d'autre terme, la positivité de la courbure scalaire montre que V est « sous-euclidienne » au niveau microscopique. En fait le signe de la courbure scalaire est le même que celui de la courbure sectionnelle. En effet, il existe un lien entre ces deux courbures donné par

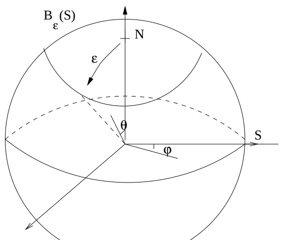
$$\mathrm{sc}_v = 2 \sum_{i<j} \sec_v(e_i, e_j)$$

où les vecteurs e_i forment une base orthonormée de l'espace tangent (T_vV, g_v).

Voyons ceci sur des exemples. En dimension 1, la courbure scalaire est toujours nulle. Pour la sphère unité S^2 muni de la métrique induite par son plongement dans $(\mathbf{R}^3, can)$, nous avons (voir figure cidessous) :

$$\begin{aligned} \mathrm{vol}B_v(V,\varepsilon) &= \int_{\theta=0}^{\varepsilon}\int_{\phi=0}^{2\pi}\sin\theta \mathrm{d}\theta\mathrm{d}\phi \\ &= 2\pi(1-\cos\varepsilon) \\ &= \pi\varepsilon^2(1-\varepsilon^2/12+o(\varepsilon^2)) \end{aligned}$$

d'où $\mathrm{sc}_v(S^2, can) = 2$.



Courbure scalaire de la sphère

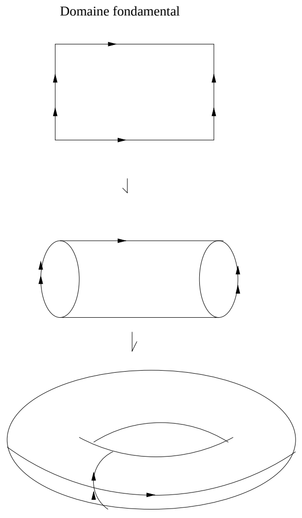
Plus généralement, $\mathrm{sc}_v(S^n) = n(n-1)$ et si nous considérons la sphère de rayon r, $\mathrm{sc}_v(S^n_r) = r^{-2}n(n-1)$. Une autre propriété intéressante est le fait que si nous multiplions la métrique par r^2, la courbure scalaire est divisée par r^2.

Nous avons maintenant une idée de la notion de courbure scalaire. Passons maintenant au problème annoncé dans l'introduction : quand pouvons-nous munir une variété riemanienne (V, g_0) d'une autre métrique g de courbure scalaire strictement positive ? Ce problème semble avoir des conséquences importantes en physique théorique, en particulier dans la théorie de la gravitation, mais je ne saurais en dire plus en raison de mon ignorance dans ce domaine (le lecteur m'en excusera).

Pourquoi la notion d'agrandissabilité ?

Introduction

La notion de variétés agrandissables a été introduite par M. Gromov et B. Lawson en 1980 pour montrer que le tore $T^n = \mathbf{R}^n/\mathbf{Z}^n$ de dimension n ne porte pas de métrique à courbure scalaire strictement positive. Lorsque nous considérons le tore T^n, nous pouvons le munir de la métrique plate induite par la métrique canonique de $\mathbf{R}^n$. Ainsi le tore porte une métrique à courbure scalaire nulle :



Le tore

Mais ceci ne règle pas le problème de l'existence de métrique à courbure scalaire strictement positive. Commençons par les petites dimensions.

Cas de la dimension 1

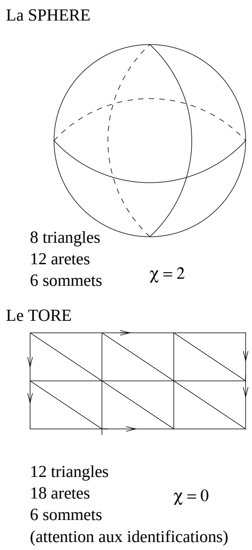
Le cas de la dimension 1 est clair puisque toute courbe, quelque soit la métrique, a une courbure scalaire nulle. Ceci montre en particulier la faiblesse de la courbure scalaire par rapport à la courbure sectionnelle (équivalente de la courbure classique des courbes). Cette courbure ne permet pas de retrouver la structure globale de la variété, comme nous pouvons le faire avec la courbure sectionnelle.

Cas de la dimension 2

Le cas de la dimension 2 est déjà plus intéressant et non trivial. Il nécessite un théorème fondamental pour les surfaces : le théorème de Gauss-Bonnet. Nous devons d'abord définir la *caractéristique d'Euler* d'une surface V, noté $\chi(V)$. A partir d'une triangulation de la variété V, nous aurons $\chi(V) =$ (nombre de triangles) - (nombre d'arètes) + (nombre de sommets). Ainsi, $\chi(S^2) = 2$, $\chi(T^2) = 0$ (voir figure ciaprès). Le lecteur pourra vérifier sur ces exemples que la caractéristique d'Euler ne dépend pas de la triangulation choisie.

Le *théorème de Gauss-Bonnet* lie la caractéristique d'Euler et la courbure scalaire par la formule

$$\int_V \mathrm{sc}_v(V,g)\mathrm{d}v = 4\pi\chi(V)$$



Caractéristique d'Euler

Ainsi dans le cas du tore, quelque soit la métrique, $\int_V \mathrm{sc}_v(T^2, g)\mathrm{d}v = 0$. Par des raisonnements classiques sur le signe de l'intégrande, nous pouvons montrer que $\mathrm{sc}_v(T^2, g) \equiv 0$ ou bien prend nécessairement les deux signes.

Cas général ?

En dimension supérieure, le problème a été résolu partiellement d'abord en employant la régularité d'hypersurfaces minimales par R. Schoen et S.T. Yau en 1979 pour les dimensions inférieures ou égales à 7.

En fait, le problème de savoir si une variété possède une métrique à courbure scalaire strictement positive est très difficile. En 1963, A. Lichnerowicz trouve une obstruction à l'existence de métrique à courbure scalaire strictement positive : un certain invariant numérique doit être nul.

Mais pour le tore cet invariant est nul, donc ceci ne permet pas d'exclure le fait que le tore puisse porter une métrique à courbure scalaire strictement positive. Il faut attendre 1980 et l'article de M. Gromov et B. Lawson pour montrer, pour toutes les dimensions n, que le tore ne peut avoir une métrique à courbure scalaire strictement positive. En adaptant astucieusement les méthodes de Lichnerowiscz, ils montrent que des variétés, dites agrandissables, ne peuvent porter de métrique à courbure scalaire strictement positive (ce sera le cas des tores). Ceci permet en particulier de montrer qu'une variété compacte sans bord (V, g_0) de courbure sectionnelle négative ou nulle ne peut porter de métrique g à courbure scalaire positive ou nulle.

Quelques définitions

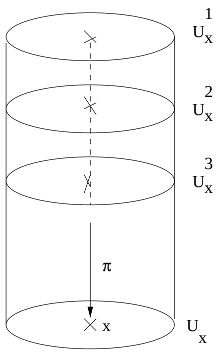
Pour pouvoir donner la définition « exacte » des variétés agrandissables, nous devons introduire des termes mathématiques inconnus des non-initiés, par exemple : orientable, revêtement (riemannien), degré. Nous laissons à l'intuition la notion d'orientabilité.

Voyons donc ce qu'est le degré d'une application et un revêtement d'une variété.

Soit une application $f : V^n \to S^n$, le *degré* de cette application est l'entier $n_y = \sum_{y=f(x)} \varepsilon(x)$ où $\varepsilon(x) = 1$ si $\mathrm{d}f_x : T_xV \to T_yS^n$ est de déterminant positif, -1 sinon. Remarquons que n_y ne dépend pas de y (n_y est localement constante et continue) et que s'il existe y n'ayant pas d'antécédant alors degré$f = 0$.

Un *revêtement fini* de cardinal p de V est une variété $\tilde{V}$ muni d'une projection $\pi : \tilde{V} \to V$ telle que, quelque soit x dans V, il existe U_x un voisinage de x dans V tel que $\pi^{-1}(U_x) = \coprod_{i=1}^{p} U_x^i$ où $\pi : U_x^i \to U_x$ est un homéomorphisme (voir figure ci-dessous). Nous dirons que ce revêtement est *riemannien* si nous pouvons munir $\tilde{V}$ d'une métrique compatible avec celle de V par la projection π.

Par exemple, $S^1 \to S^1 : z \mapsto z^2$ est un revêtement fini de cardinal 2, comme chacun peut s'en persuader.



Revêtement fini à 3 feuilles

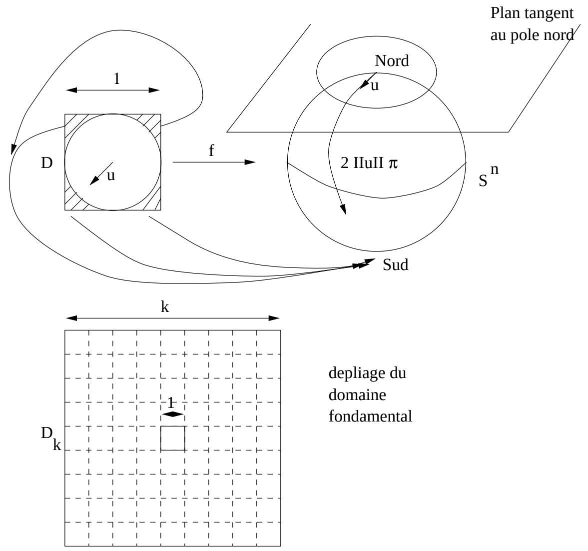
Voilà maintenant la définition à laquelle nous voulions parvenir. Nous dirons qu'une variété V compacte riemannienne orientable de dimension n est *agrandissable* si, quel que soit $\varepsilon > 0$, il existe un revêtement riemannien fini $\tilde{V}_\varepsilon$ et une application $f : \tilde{V}_\varepsilon \to S^n$ de degré non nul et ε-contractante (i.e. $\forall v \in V_\varepsilon,\ \forall x \in T_vV_\varepsilon,\ \|\mathrm{d}f_v(x)\| \leq \varepsilon\|x\|$).

Il est important de noter que cette propriété de la variété ne dépend pas de la métrique qu'elle porte.

Retour au cas du tore

Nous allons maintenant montrer que le tore est une variété agrandissable, ce qui permettra d'affirmer que pour toute dimension n, ce tore ne peut porter de métrique à courbure scalaire strictement positive.

Soit le tore $T^n = \mathbf{R}^n/\mathbf{Z}^n$. Considérons un domaine fondamental D de T^n, par exemple le pavé $[-1/2, 1/2]^n$ et construisons une application $f : D \to S^n$ α-contractante de degré 1 en « enveloppant » la sphère par le domaine D :



Construction

Considérons ensuite un revêtement fini de T^n de la forme $\tilde{T}^n_k = \mathbf{R}^n/(k\mathbf{Z})^n$ de cardinal k^n. Un domaine fondamental D_k de $\tilde{T}^n_k$ est par exemple $[-k/2, k/2]^n$. En fait D_k peut être vu comme l'image de D par une homothétie de rapport k. Ainsi l'application $\phi_k : D_k \to S^n$ définie par $\phi_k(x) = f(x/k)$ est α/k-contractante de degré 1. Nous venons de montrer que le tore est agrandissable.

Conclusion

M. Gromov a donné dans un article récent une nouvelle interprétation de la notion d'agrandissabilité. Il associe à chaque variété riemanienne un réel positif, éventuellement infini, appelé K-Aire. Une variété agrandissable a, dans ce cas, une K-Aire infinie. De plus, le fait d'être de K-Aire infinie est indépendant de la métrique initiale portée par la variété. Le théorème, disant que les variétés agrandissables ne peuvent porter de métrique à courbure scalaire strictement positive, a ainsi une expression plus quantitative :

$$\mathrm{sc}(V, g) > \varepsilon^2 \Rightarrow K\text{-Aire}(V, g) \leq k_n/\varepsilon^2$$

où k_n est une constante qui ne dépend que de la dimension de la variété V.

Il s'agit maintenant d'étudier ce nouvel objet.

Pour en savoir plus...

[B_1] Marcel Berger, *Rencontre avec un géomètre*, Gazette des mathématiciens **76** (1998), 25–45.

[B_2] Marcel Berger, *Rencontre avec un géomètre*, Gazette des mathématiciens **77** (1998), 29–53.

[BB] Lionel Bérard-Bergery, *La coubure scalaire des variétés riemanniennes*, Séminaire Bourbaki, 32ème année, 1979–1980, exposé 556.

[dC_1] Manfredo P. do Carmo, *Differential Geometry of Curves and Surfaces*, Prentice Hall, 1976.

[dC_2] Manfredo P. do Carmo, *Riemannian Geometry*, Birkhaüser, 1992.

[GHL] Sylvestre Gallot, Dominique Hulin, et Jacques Lafontaine, *Riemannian Geometry*, Springer-Verlag, 1987.

[GL] Mickael Gromov et H. Blaine Lawson, Jr., *Spin and Scalar Curvature in Presence of a Fundamuntal Group*, Annals of Mathematics **111** (1980), 209–230.

[LM] H. Blaine Lawson, Jr. et Marie-Louise Michelson, *Spin Geometry*, Princeton University Press, 1989.

Petits problèmes

Nous proposons ici quelques problèmes, dont l'énoncé est généralement assez simple, mais dont nous n'avons pas de solution satisfaisante. Vous pouvez ainsi apporter votre contribution à Hubris en nous envoyant la réponse à certains de ces problèmes, ou en proposant de nouveaux problèmes. **N.M.**

Solution de **Les bagues de Suleima**
(Problème posé dans le numéro 2 d'Hubris)

Le fiancé de Suleima, orfèvre arithméticien, prépare dans son atelier une bague pour sa bien-aimée. Il a en effet promis, comme preuve de son amour, de lui offrir chaque mois une bague en or différente, incrustée d'émeraudes, de saphirs ou de rubis. Chaque bague a dix pierres précieuse, régulièrement réparties, et se distingue des autres uniquement par l'ordonnancement des pierres qu'elle comporte. Pendant combien de temps Suleima pourra-t-elle être rassurée sur l'amour que lui voue son futur mari ?

Nous allons voir que se problème est un cas particulier d'un problème plus général, à savoir le dénombrement des mots circulaires, et peut se résoudre en faisant appel à la fonction de Möbius. Ce problème de combinatoire sur les mots circulaires est traité dans [B] et c'est sa présentation que nous allons suivre. Pour ce qui concerne la fonction de Möbius, on pourra également se reporter à [NQ].

Les mots circulaires

Désignons par A l'ensemble à trois éléments :

$$A = \{\texttt{emeraude}, \texttt{rubis}, \texttt{saphir}\}.$$

Une bague est déterminée par la donnée d'une application :

$$b : \{1, \ldots, 10\} \to A$$

qui indique la suite des pierres qui la composent. Deux telles applications définissent la même bague dès qu'il existe un entier p tel que pour tout i entre 1 et 10, on ait :

$$b'(i) = b(i + p)$$

(en comptant modulo 10). On définit ainsi une relation d'équivalence sur sur l'ensemble des applications de $\{1, \ldots, 10\}$ dans A et le nombre de bagues différentes que l'on peut construire est égal au nombre de classes d'équivalence de l'ensemble quotient.

Afin de généraliser ceci, nous allons définir la notion de mot circulaire de longueur n (on avait ici $n = 10$) sur un alphabet fini A que l'on supposera de cardinal m :

- un mot de longueur n sur A est un élément w de A^n qui peut également être vu comme une application :

$$w : \mathbf{Z}/n\mathbf{Z} \to A,$$

- deux mots de longueur n sur A, w et w', sont dits équivalents si et seulement si il existe $p \in \mathbf{Z}/n\mathbf{Z}$ tel que quel que soit $i \in \mathbf{Z}/n\mathbf{Z}$ on ait :

$$w'(i) = w(i + p)$$

  et on note alors $w \circlearrowleft w'$,
- l'ensemble quotient $A^n/\circlearrowleft$ est appelé ensemble des mots circulaires.

On aura également besoin de la notion de période primitive d'un mot. Un mot w de longueur n sur A induit une application :

$$\begin{array}{ccc} \mathbf{Z} & \to & A \\ i & \mapsto & w(\bar{i}) \end{array}$$

(où $\bar{i}$ désigne la classe de i modulo n). L'ensemble des périodes de cette application est un idéal de $\mathbf{Z}$, non vide (il contient n). Il est par conséquent de la forme $p\mathbf{Z}$ où $p \in \mathbf{N}$ est non nul. p est appelé période primitive de w. Remarquons qu'un tel p est nécessairement un diviseur de n.

Pour p compris entre 1 et n et divisant n, on note $M(p)$ l'ensemble des mots circulaires dont un représentant est de période primitive p, on a alors trivialement :

$$\mathrm{card}(A/\circlearrowleft) = \sum_{\substack{1 \leq p \leq n \\ p \mid n}} \mathrm{card}(M(p))$$

(puisque tout mot possède une période primitive).

Intervention de la fonction de Möbius

Pour $k \in \mathbf{N}$ non nul, notons :

$$k = p_1 \ldots p_r$$

une décomposition de k en facteurs premiers. On convient de poser :

- $\mu(k) = 0$ si deux des p_i sont égaux (*i.e.* k contient un facteur carré),
- $\mu(k) = (-1)^r$ sinon.

La fonction μ ainsi définie est appelée fonction de Möbius. On va utiliser le résultat suivant (dit formule d'inversion de Möbius) :

Théorème. — *Soient* f *et* g *deux applications de* $\mathbf{N}^*$ *dans* $\mathbf{Z}$ *telles que, quel que soit* $n \in \mathbf{N}^*$, *on ait :*

$$f(n) = \sum_{d|n} g(d)$$

alors pour tout* $n \in \mathbf{N}^*$ *on a :

$$g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right).$$

Appliquons ceci avec les fonctions :

$$\begin{array}{rccl} g\colon & \mathbf{N}^* & \to & \mathbf{Z} \\ & n & \mapsto & \operatorname{card}(A^n) = m^n \\ f\colon & \mathbf{N}^* & \to & \mathbf{Z} \\ & p & \mapsto & p \cdot \operatorname{card}(M(p)). \end{array}$$

Comme chaque classe d'équivalence dans $M(p)$ est de cardinal p, on a bien :

$$g(n) = \sum_{\substack{1 \le p \le n \\ d|n}} f(n)$$

et appliquant la formule d'inversion de Möbius, il vient :

$$\begin{aligned} f(p) = p \cdot \operatorname{card}(M(p)) &= \textstyle\sum_{\substack{1 \le q \le p \\ q|p}} \mu\left(\frac{p}{q}\right) g(q) \\ &= \textstyle\sum_{\substack{1 \le q \le p \\ q|p}} \mu\left(\frac{p}{q}\right) m^q \end{aligned}$$

ce qui donne finalement :

$$\begin{aligned} \operatorname{card}(A/\circlearrowleft) &= \sum_{\substack{1 \le p \le n \\ p|n}} M(p) \\ &= \sum_{\substack{1 \le p \le n \\ p|n}} \frac{f(p)}{p} \\ &= \sum_{\substack{1 \le p \le n \\ p|n}} \frac{1}{p} \sum_{\substack{1 \le q \le p \\ q|p}} \mu\left(\frac{p}{q}\right) m^q. \end{aligned}$$

Terminons avec une petite application numérique : il y a exactement quatre nombres p entre 1 et 10 divisant 10, il s'agit de :

- $p = 1$: la contribution de ce terme est $\mu(1)m^1 = m = 3$,
- $p = 2$: la contribution de ce terme est :

$$\frac{1}{2}(\mu(2)m + \mu(1)m^2) = \frac{3^2 - 3}{2} = 3,$$

- $p = 5$: la contribution de ce terme est :

$$\frac{1}{5}(\mu(5)m + \mu(1)m^5) = \frac{3^5 - 3}{5} = 48,$$

- $p = 10$: la contribution de ce terme est :

$$\begin{aligned} &\frac{1}{10}(\mu(10)m + \mu(5)m^2 + \mu(2)m^5 + \mu(1)m^{10}) \\ &= \frac{3 - 3^2 - 3^5 + 3^{10}}{10} = 5880 \end{aligned}$$

ce qui donne finalement 5934 bagues différentes, soit un peu moins de 500 années d'amour pour Suleima.

Références

[B] Claude Berge, *Principes de combinatoire*, Dunod, 1968.

[NQ] Patrice Naudin and Claude Quitté, *Algorithmique algébrique*, Masson, 1992.

G.d.R., A.B., N.M.

Les couvertures

On se donne un certain nombre de couvertures carrées. La surface totale des couvertures vaut 4. Montrer que les couvertures peuvent recouvrir le carré unité. **N.M.**

Problème d'informatique

Soit $G = (V, E)$ un graphe connexe fini non orienté, et tel que E ne contienne pas de boucle d'un état sur lui-même. Sur chaque sommet de ce graphe, on dispose un certain nombre de jetons (et on nomme « configuration » du graphe une disposition de ces jetons).

Une « partie » est une suite de configurations, partant d'une configuration initiale, et telle que le passage d'une configuration à la suivante est régi par le principe suivant : *si un sommet possède* p *voisins et* $k \ge p$ *jetons, il distribue un jeton à chacun de ses voisins*. Il est clair qu'une partie peut être finie (intuitivement, s'il n'y a pas beaucoup de jetons) ou infinie (intuitivement, s'il y a beaucoup de jetons).

Le nombre total de jetons est donc constant sur une partie. Notons le j.

Notons également $n = |V|$ et $m = |E|$.

Montrer que si une partie est infinie, alors toutes les parties commençant par la même configuration initiale sont infinies.

Montrer qu'une partie est infinie si, et seulement si, elle fait intervenir tous les sommets.

Montrer les équivalence suivantes :

$j > 2m - n$	$\Leftrightarrow$	toutes les parties sont infinies, quelle que soit la configuration initiale
$j < m$	$\Leftrightarrow$	toutes les parties sont finies, quelle que soit la configuration initiale.

N.M.

Livres

Model theory and algebraic geometry,
An introduction to E. Hrushovski's proof
of the geometric Mordell–Lang conjecture,
E. Bouscaren editor, Springer Verlag,
LNM 1696 (1998)

Rappelons l'objet d'étude de la géométrie algébrique : on se donne un corps (algébriquement clos) k, une famille de polynômes $(P_i)_{i\in I}$ à n indéterminées et on s'intéresse à l'ensemble de ses zéros,

$$\{\,(x_1,\ldots,x_n)\in k^n\;:\;\forall i\in I\ P_i(x_1,\ldots,x_n)=0\,\}.$$

C'est ce que l'on appelle une *variété affine.*

La théorie des modèles formalise cette notion de variété affine (j'entends déjà les mauvaises langues : « comme si la géométrie algébrique avait besoin de cette bourbakisation supplémentaire ! »), que l'on pourra ensuite généraliser, par exemple en remplaçant les corps par des corps différentiels ou des corps réels.

On part d'une « théorie », par exemple la « théorie des corps algébriquement clos de caractéristique 17 » (vous pouvez mettre votre nombre premier préféré à la place de 17, c'est pareil), définie comme l'ensemble des propriétés vérifiées par ces corps et exprimées à l'aide de quantificateurs ($\exists$, $\forall$), d'opérations logiques (et, ou, non), des opérations des corps ($+$, $-$, $\times$) des constantes de ces corps (0 et 1) et de la relation d'égalité. On peut montrer que cette théorie est *complète*, *i.e.*, toute assertion est soit vraie pour tous les corps algébriquement clos de caractéristique 17, soit fausse pour tous.

On peut alors s'intéresser aux *ensembles définissables*, *i.e.*, aux formules $F(x_1,\ldots,x_n)$ en n variables que l'on peut écrire dans la théorie et, pour tout corps k algébriquement clos de caractéristique 17, l'ensemble

$$\{\,(x_1,\ldots,x_n)\in k^n\;:\;F(x_1,\ldots,x_n)\,\}.$$

Les ensembles définissables sont un peu plus généraux que les variétés affines : il s'agit des combinaisons booléennes (union, intersection, complémentaire) de variétés affines. On peut montrer que la théorie des corps algébriquement clos de caractéristique 17 possède l'*élimination des quantificateurs*, *i.e.*, toute formule (dépendant de variables $x_1,\ldots,x_n$) est equivalente à une formule sans quantificateurs. Traduite en termes géométriques, cette assertion n'est autre que le théorème de Chevalley : la projection d'une combinaison booléenne de variétés affines est encore une combinaison booléenne de variétés affines.

On peut continuer cette « bourbakisation » de la géométrie algébrique en donnant des définitions « logiques » des idéaux, de la dimension, etc. — je ne détruis pas le suspense et laisse le lecteur découvrir cela par lui-même.

L'intérêt de cette démarche est double :

- d'une part, appliquer les méthodes de la géométrie algébrique dans d'autres contextes, comme les corps différentiables ou les corps réels ;
- d'autre part, appliquer les méthodes de la logique à la géométrie algébrique, qui permettent de démontrer des résultats qui résistent aux géomètres.

V.Z.

Morse Theory,
J. Milnor,
Princeton University Press, (1963)

Ce livre a pour but d'exposer une démonstration du théorème de périodicité de Bott dans les cas réel et complexe qui s'énonce ainsi :

Théorème. — ***Les classes d'homotopie stables des groupes classiques*** $\mathrm{U}(n)$ ***et*** $\mathrm{O}(n)$ ***sont périodiques, de période*** 2 ***dans le cas complexe,*** 8 ***dans le cas réel.***

Pour démontrer ce théorème de nature algébrique, il est surprenant de passer par des méthodes de géométrie différentielle, en particulier la théorie de Morse. Elle permet, connaissant une fonction sur une variété, de construire un complexe cellulaire de même type d'homotopie que la variété. Ceci est l'objet du premier chapitre. Pour poursuivre, l'auteur a besoin de résultats en géométrie riemannienne. Il développe ainsi la théorie des connexions, des géodésiques, etc. (il en donne d'ailleur un exposé clair). L'étape suivante consiste à étudier l'espace des chemins sur une variété riemannienne et en particulier la fonctionnelle énergie (qui sera la fonction de Morse utilisée), à ce propos il introduit les champs de Jacobi. Il peut ensuite utiliser (après quelques transformations techniques) le théorème de Morse démontré dans la première partie pour donner un complexe cellulaire de même type d'homotopie que l'espace des chemins (qui est une « variété » de dimension infinie). Il ne reste plus qu'à appliquer ceci au cas des variétés $\mathrm{U}(n)$ et $\mathrm{O}(n)$ pour conclure. Il faut alors faire une digression sur les espaces symétriques puis retrousser ses manches pour se lancer dans la démonstration de la périodicité de Bott unitaire puis réel (les problèmes allant croissants).

Cette démonstration de la périodicité de Bott est une des premières. Les personnes étudiants la K-théorie ne pouront l'éviter même s'il existe d'autre démonstration. **H.D.**

Une histoire des mathématiques,
A. Dahan-Dalmedico et J. Peiffer,
Seuil, « Points science », 1986

La vision que l'on a des mathématiques dans l'enseignement supérieur est un peu comparable à la vision que l'on aurait du monde en feuilletant un atlas : les territoires sont très détaillés, leurs frontières et leur relations très nettes, et on pourrait d'ailleurs croire (à tort sans doute) que ce caractère rigide et fixe favorise leur apprentissage. Pourtant, on sait bien, au moins inconsciemment, que les mathématiques n'ont pas toujours eu le visage qu'elle présentent aujourd'hui (et qu'elle ne le garderont probablement pas indéfiniment) mais on ne se rend pas toujours compte à quel point leur histoire est composée d'impasses, de doutes, de problèmes *a priori* insolubles surgissant au détour d'un chemin où on ne les attendait pas. Ce livre retrace la naissance et le développement de l'activité mathématique à travers différents thèmes. On peut citer par exemple les mathématiques grecques (souvent les plus connues, sans doute parce qu'elles présentent une forme et un modèle de raisonnement encore proche de ceux employés aujourd'hui), le développement de l'algèbre, entravé par des détails *a priori* sans importance et pourtant capitaux : la moindre opération arithmétique devient extrêmement compliqué hors d'un système de notations appropriées (essayez par exemple de réaliser une multiplication en utilisant des chiffres romains !) et privés de la notion de variable pour représenter les inconnues, les énoncés et les solutions des problèmes s'enlisent inexorablement dans des explications alambiquées. L'introduction d'éléments « imaginaires » par rapport à la « réalité » que les mathématiques étaient censées décrire (par exemple les nombres complexes ou les points à l'infini de la géométrie projective) ont aussi été l'occasion de débats, parfois virulents. Bref, les mathématiques ne sont pas seulement une science en développement : elles possèdent également une histoire intrinsèquement mêlée à celle des hommes. De plus, certaines discussions parfois virulentes, que l'on peut entendre aujourd'hui à propos des mathématiques (sur les forum de discussion par exemple) prennent à la lecture de ce livre un petit air de déjà vu plutôt amusant. **A.B.**

Principles of Program Analysis,
F. Nielson, H.R. Nielson et C. Hankin,
Springer, 1998

Ce livre est bien sûr un livre d'informatique puisqu'il traite de programmes, mais c'est pourtant également un livre mathématique, et ce à plus d'un titre. Tout d'abord dans la nature du sujet traité : le mathématicien étudie un certain domaine au moyen de la démarche mathématique. Ce domaine peut aussi bien être celui des objets géométriques, ou celui des structures algébriques, ou bien les mathématiques elles-même, si le mathématicien en question est un logicien, ou n'importe quel autre domaine, du moment que la modélisation et les techniques employées sont de nature mathématique. Ce n'est pas autre chose qui est fait ici, les objets étudiés sont simplement des programmes et on veut montrer que certains de ces programmes satisfont certaines propriétés, du genre :

- « ce programme ne produira pas d'erreurs durant son exécution »,
- « si on a calculé la valeur de telle expression à tel point du programme, il est inutile de la recalculer à tel autre »,
- *etc.*

La manière de répondre (au moins partiellement) à ces questions revêt elle-aussi un caractère mathématique : il s'agit d'attacher à ces programmes des objets de nature mathématique (graphes, ensembles de contraintes, fonctions, types,. . .), de calculer si ces objets possèdent certaines propriétés et d'en déduire des résultats sur le programme de départ. Comme les propriétés intéressantes sur les programmes sont en général indécidables, il faut souvent de contenter de résultat approchés : une théorie permettant de réaliser de telles approximations est ainsi décrite, elle-aussi de manière mathématique. Signalons finalement que les auteurs ne se contentent pas de décrire des « recettes » : ils expliquent également comment les différentes approches sont reliées entre-elles.

A.B.