

## L'équation de Catalan

M. Mignotte

---

Dans une Note extraite d'une lettre adressée à l'éditeur par Monsieur E. Catalan, répétiteur à l'École polytechnique de Paris, publiée dans le "*Journal für die reine und angewandte Mathematik*" en Allemagne en 1844, on peut lire :

*Je vous prie, Monsieur, de bien vouloir énoncer, dans votre recueil, le théorème suivant, que je crois vrai, bien que je n'aie pas encore réussi à le démontrer complètement : d'autres seront peut-être plus heureux : deux nombres entiers consécutifs, autres que 8 et 9, ne peuvent être des puissances exactes ; autrement dit : l'équation  $x^m - y^n = 1$ , dans laquelle les inconnues sont entières et positives, n'admet qu'une seule solution.*

Cette question a été résolue au début de cette année par Preda Mihăilescu, mathématicien d'origine roumaine : l'équation  $x^m - y^n = 1$ , dans laquelle les inconnues sont entières et positives,  $m$  et  $n \geq 2$ , n'admet qu'une seule solution, à savoir  $3^2 - 2^3 = 1$ .

Le but de cette présentation est de faire un historique rapide des travaux sur cette équation. La démonstration finale de Mihăilescu ayant été mise au point par Yuri Bilu [Bi], on la trouve sur sa page web<sup>1</sup>. Pour un historique complet jusqu'en 1992, voir le livre de Paulo Ribenboim [R].

Clairement, pour étudier le problème de Catalan, il suffit de considérer le cas où les exposants sont premiers :

---

<sup>1</sup> <http://www.math.u-bordeaux.fr/~yuri/publ/preprs/catal.ps>

$$x^p - y^q = 1, \text{ où } p \text{ et } q \text{ sont premiers, et } |x|, |y| > 1,$$

dans la suite les lettres  $p$  et  $q$  désigneront toujours des nombres premiers.

Le plan est le suivant :

- (1) Le cas  $pq$  pair
- (2) Le théorème de Cassels
- (3) Le théorème de Tijdeman
- (4) Les critères algébriques
- (5) Calculs
- (6) La conclusion de Mihăilescu

### 1. Le cas $pq$ pair

En 1738, Euler [E] a montré que la seule solution non triviale de l'équation  $x^2 - y^3 = 1$  est  $x = 3$  et  $y = 2$ , donc  $9 - 8 = 1$ . En 1850, V.A. Lebesgue [Le] a prouvé que l'équation  $x^p - y^2 = 1$  n'a pas de solutions entières avec  $y > 0$ . Mais ce n'est qu'en 1965 que l'équation  $x^2 - y^q = 1$  a été résolue par Ko Chao [K], qui montre que le seul cas où existe une solution non triviale est celui de l'équation d'Euler,  $q = 3$ .

Nous donnons la preuve du théorème de V.A. Lebesgue, c'est la seule preuve simple de toute cette histoire.

**Théorème (V.A. Lebesgue, 1850).** — *L'équation diophantienne*

$$x^p - y^2 = 1$$

*admet pour seule solution en nombres entiers  $y = 0$  et  $x = 1$ .*

**Démonstration.** — Supposons qu'il existe une solution avec  $y \neq 0$ . Du fait que la congruence  $x^p \equiv 2 \pmod{4}$  n'a pas de solution en nombres entiers, on voit aussitôt que  $y$  doit être pair tandis que  $x$  est impair. Dans l'anneau  $\mathbb{Z}[i]$  des entiers de Gauss, on a la factorisation

$$(1 + iy)(1 - iy) = x^p.$$

Comme  $y$  est pair, les facteurs  $1 \pm iy$  sont premiers entre eux. D'où l'existence d'entiers rationnels  $u$  et  $v$  tels que

$$1 + iy = i^r (u + iv)^p, \quad \text{avec } r \in \{0, 1, 2, 3\}.$$

Du fait que  $p$  est impair, on se ramène facilement au cas où  $r = 0$ , ce qu'on supposera. Alors,  $v$  est non nul puisque  $y$  n'est pas nul. En considérant la partie réelle dans l'égalité ci-dessus, on obtient la relation

$$u^p - \binom{p}{2} u^{p-2} v^2 + \dots + (-1)^{(p-1)/2} \binom{p}{p-1} u v^{p-1} = 1.$$

Donc  $u = \pm 1$ . Comme  $x = u^2 + v^2$  et que  $x$  est impair, on voit que  $v$  est pair et — en regardant modulo 4 — que  $u = 1$ . Ainsi,

$$\sum_{k=1}^{(p-1)/2} (-1)^k \binom{p}{2k} v^{2k} = 0.$$

Dans cette expression, pour  $1 < k \leq (p-1)/2$ , on peut écrire

$$\binom{p}{2k} v^{2k} = \frac{p(p-1)}{2} v^2 \times \binom{p-2}{2k-2} \frac{v^{2k-2}}{k(2k-1)},$$

et le second facteur est un nombre rationnel dont le numérateur est un nombre pair [en effet,  $2^{2k-2}$  divise  $v^{2k-2}$  mais ne divise pas le produit  $k(2k-1)$ ]. Ce qui montre que la relation ci-dessus est impossible si  $v$  n'est pas nul.  $\square$

Nous allons étudier rapidement l'équation

$$y^2 - 1 = x^p.$$

Démontrons d'abord que  $x$  est nécessairement pair. En effet, dans le cas contraire  $y+1$  et  $y-1$  sont premiers entre eux et on en déduit l'existence de deux entiers  $u$  et  $v$  tels que  $u^p - v^p = 2$ , ce qui est clairement impossible. Il existe donc des entiers  $u$  et  $v$  tels que

$$y \pm 1 = 2u^p, \quad y \mp 1 = 2^{p-1}v^p,$$

ce qui implique

$$u^p - 2^{p-2}v^p = \pm 1.$$

Admettons provisoirement que  $p$  divise  $y$ . Il en résulte facilement que

$$x + 1 = py_1^2, \quad \frac{x^p + 1}{x + 1} = py_2^2,$$

où  $y = py_1y_2$  est impair. Supposons d'abord  $p$  de la forme  $p = 8n + a$ ,  $a \in \{5, 7\}$ . De la relation  $x + 1 = py_1^2$ , il s'en suit que  $x \equiv a - 1 \pmod{8}$ . En écrivant la relation  $y^2 - 1 = x^p$  sous la forme

$$y^2 = (x^2 - 1 + 1)^{4n} x^a + 1,$$

on voit que  $y^2 \equiv x^a + 1 \pmod{x^2 - 1}$ . D'où le caractère quadratique (symbole de Jacobi)

$$\left( \frac{x^a + 1}{x - 1} \right) = \left( \frac{2}{x - 1} \right) = +1.$$

Mais ceci est impossible puisque  $x - 1 \equiv 3, 5 \pmod{8}$ .

Supposons maintenant,  $p = 8n + 3 = 24m + a$ ,  $a \in \{11, 19\}$ . Alors,  $x \equiv 2$

(mod 8). Et, cette fois,

$$y^2 = (x^3 - 1 + 1)^{8m} x^a + 1 \equiv x^a + 1 \pmod{x^3 - 1}.$$

Donc, 
$$\left(\frac{x^a + 1}{x^3 - 1}\right) = +1.$$

Dans le cas où  $a = 11$ , comme  $x^{11} - x^2 = x^2(x^9 - 1)$ , on a

$$+1 = \left(\frac{x^2 + 1}{x^3 - 1}\right) = \left(\frac{x^3 - 1}{x^2 + 1}\right) = \left(\frac{-x - 1}{x^2 + 1}\right) = \left(\frac{x^2 + 1}{x - 1}\right) = \left(\frac{2}{x + 1}\right) = -1.$$

Contradiction.

Si  $a = 19$ , alors

$$+1 = \left(\frac{x^{19} + 1}{x^3 - 1}\right) = \left(\frac{x + 1}{x^3 - 1}\right) = -\left(\frac{x^3 - 1}{x + 1}\right) = \left(\frac{2}{x + 1}\right) = -1.$$

De nouveau une contradiction. Nous avons partiellement démontré le résultat suivant, voir [N1] et [N2].

**Théorème (Nagell, 1921–1934).** — *Pour  $p > 3$ , si l'équation*

$$y^2 - 1 = x^p, \quad y > 0,$$

*possède une solution en nombres entiers alors  $y$  est pair,  $p$  divise  $x$  et  $p \equiv 1 \pmod{8}$ .*

Le fait que  $p$  divise  $x$  est un peu plus difficile à montrer. Nagell utilise un résultat de Størmer<sup>2</sup> sur l'équation de Pell–Fermat : *Si  $u_1$  et  $v_1$  désignent les solutions fondamentales de l'équation  $u^2 - Dv^2 = \pm 1$  alors parmi toutes les solutions  $v$  il n'y en aura aucune, ou bien une seule, à savoir  $v_1$ , jouissant de la propriété que chacun de ses diviseurs premiers divise  $D$ .* Il procède ainsi : si  $p$  ne divise pas  $y$  le Lemme ci-dessous implique  $x + 1 = x_1^2$  et alors

$$y^2 - x^p = y^2 - (x_1^2 - 1) \left( (x_1^2 - 1)^{\frac{p-1}{2}} \right)^2 = 1,$$

si bien que  $(x_1, (x_1^2 - 1)^{(p-1)/2})$  est une solution de l'équation de Pell–Fermat  $u^2 - (x_1^2 - 1)v^2 = 1$  pour laquelle  $(u_1, v_1) = (x_1, 1)$ , en contradiction avec le théorème de Størmer.

La démonstration de Ko Chao utilise ensuite un raisonnement très astucieux qui combine la loi de réciprocité quadratique et l'algorithme d'Euclide. Elle est présentée dans le livre de Mordell [Mo]. Chein [Ch] a ensuite donné une démonstration, un peu plus simple, mais tout aussi élémentaire et astucieuse qui est reproduite dans l'ouvrage de Ribenboim.

<sup>2</sup> *Nyt Tidsskrift for Matematik*, t. 19, Copenhague, 1908

En se permettant l'utilisation de formes linéaires de logarithmes on peut montrer que l'on a  $p < 200$  dans l'équation  $2^{p-1}u^p - v^p = \pm 1$  et conclure qu'il n'y a pas de solution en adaptant un théorème de Kummer sur le premier cas du théorème de Fermat. Bien sûr, maintenant le théorème de Ko Chao est un corollaire banal des extensions du théorème de Wiles ...

À partir de maintenant nous supposons toujours  $p$  et  $q$  impairs.

## 2. Le résultat de Cassels

Il s'agit du résultat suivant [C].

**Théorème (Cassels, 1960).** — *Si l'équation  $x^p - y^q = \varepsilon = \pm 1$  avec  $p, q \geq 3$ , et  $x, y > 1$ , possède une solution alors  $p$  divise  $y$  et  $q$  divise  $x$ .*

**Démonstration.** — Supposons  $q < p$ . Nous allons démontrer la « moitié facile » de ce théorème, à savoir que  $q$  divise  $x$ , ou, ce qui est équivalent, que  $q$  divise  $y + \varepsilon$ . On raisonne par l'absurde. Supposons que  $q$  ne divise pas  $y + \varepsilon$ . Alors, en raison de la factorisation

$$x^p = y^q + \varepsilon = (y + \varepsilon) \frac{y^q + \varepsilon}{y + \varepsilon},$$

le lemme ci-dessous implique l'existence d'un entier  $u > 1$  tel que  $y + \varepsilon = u^p$ .

Dans le cas où  $\varepsilon = 1$ , on a

$$x^p = y^q + 1 = (u^p - 1)^q + 1 < u^{pq},$$

et donc  $x \leq u^q - 1$ . Puisque  $p > q$ , on en déduit

$$x^p \leq (u^q - 1)^p < (u^p - 1)^q = y^q,$$

ce qui contredit la relation  $x^p - y^q = 1$ . Par contre, si  $\varepsilon = -1$ , on a

$$x^p = y^q - 1 = (u^p + 1)^q - 1 > u^{pq},$$

et donc  $x^p \geq (u^q + 1)^p - 1 > (u^p + 1)^q = y^q$ , ce qui contredit à nouveau  $x^p - y^q = \varepsilon$ .

Le lemme suivant, qui remonte à Euler, joue un rôle essentiel dans l'étude de l'équation de Catalan. Mais il lui est propre, car pour l'équation  $x^p - y^q = 2$  il n'existe pas une telle factorisation et on ne sait même pas s'il y a un nombre fini de solutions ou non.

**Lemme.** — Soient  $p$  un nombre premier impair et  $c$  un entier,  $|c| > 1$ . Alors

$$\text{pgcd} \left( \frac{c^p - 1}{c - 1}, c - 1 \right) = \begin{cases} 1, & \text{si } p \text{ ne divise pas } c-1, \\ p, & \text{sinon.} \end{cases}$$

De plus, lorsque ce pgcd est égal à  $p$ , on a

$$\frac{c^p - 1}{c - 1} \equiv p \pmod{p^2}.$$

Pour démontrer que  $p$  divise  $y$  le principe de l'argument de Cassels est le suivant : si  $p$  ne divise pas  $y$  alors on a  $x = z^q + \varepsilon$  pour un certain entier  $z$  (grâce au lemme ci-dessus). Puis Cassels fait une étude très fine du développement en série de  $x^{p/q} = (z^q + \varepsilon)^{p/q}$  qui doit donner une valeur très proche de l'entier  $y$  puisque  $|x^p - y^q| = 1$ . C'est un raisonnement typique d'approximation diophantienne qui conduit à un résultat de divisibilité.

En utilisant toujours le lemme ci-dessus, on obtient les factorisations suivantes qui sont indispensables dans tous les travaux algébriques qui suivront.

**Corollaire.** — Soient  $x$  et  $y$  des solutions de l'équation de Catalan

$$x^p - y^q = 1, \quad |x|, |y| > 1.$$

Il existe alors des entiers  $a, b, u$  et  $v$  tels que

$$x - 1 = p^{q-1}a^q, \quad y + 1 = q^{p-1}b^p \quad \text{et} \quad \frac{x^p - 1}{x - 1} = pu^q, \quad \frac{y^q + 1}{y + 1} = qv^p,$$

avec  $x = qbv$  et  $y = pau$ . De plus, on a

$$x \equiv -(p^{q-1} - 1) \pmod{q^2}, \quad \text{et} \quad y \equiv q^{p-1} - 1 \pmod{p^2}.$$

### 3. Le théorème de Tijdeman

Le résultat très fameux de Tijdeman [Ti] est le suivant.

**Théorème (Tijdeman, 1976).** — Pour l'équation de Catalan  $x^m - y^n = 1$ , avec  $x, y > 0$ , les exposants  $m$  et  $n$  sont bornés ainsi que les variables  $x$  et  $y$ ; de plus ces bornes sont effectivement calculables.

Contrairement à tous les résultats qui suivent, la preuve de Tijdeman n'utilise pas le théorème de Cassels. Tout au contraire, elle permet de redémontrer ce résultat, au moins pour  $p$  et  $q$  assez grands. Cependant, pour faciliter l'exposé nous nous limiterons à des exposants premiers et nous utiliserons alors le théorème de Cassels.

Les bornes « effectives » que l'on pouvait obtenir en 1976 ont été calculées par Michel Langevin [L] et leur ordre de grandeur était le suivant

$$\max\{m, n\} < 10^{106}, \quad \max\{x, y\} < \exp \exp \exp \exp 700.$$

La contribution fondamentale de Tijdeman est la majoration des exposants  $m$  et  $n$ ; la majoration de  $x$  et  $y$  résulte ensuite des travaux de Baker [B] sur les équations diophantiennes superelliptiques. Bien sûr, ces majorations de  $x$  et  $y$  ne sont jamais utilisées.

Dans ce paragraphe, pour simplifier, nous considérons l'équation de Catalan sous la forme

$$x^p - y^q = \varepsilon = \pm 1,$$

où  $p$  et  $q$  sont des nombres premiers impairs, avec  $p > q$ , et  $x$  et  $y$  des entiers  $> 1$ .

La preuve de Tijdeman utilise la méthode de Baker : des minoration de formes linéaires de logarithmes de nombres algébriques. Elle s'effectue en deux temps, une majoration de  $p$  en fonction de  $q$ , puis une majoration de  $q$  en fonction de  $p$ . La première étape utilise une forme en deux logarithmes tandis que la seconde fait intervenir trois logarithmes.

La relation  $y + \varepsilon = q^{p-1}b^p$ , conséquence du corollaire du théorème de Cassels, permet d'écrire

$$y + \varepsilon = s^p/q, \quad \text{avec } \log s > \frac{p}{q} \log q,$$

pour un certain entier positif  $s$ . Tijdeman considère la forme linéaire

$$\Lambda := p \log x - q \log(y + \varepsilon) = q \log q - p \log(s^q/x)$$

pour laquelle on montre facilement que

$$0 < |\Lambda| \leq 3q^2 s^{-p}, \quad \text{donc } \log |\Lambda| \leq - \left(1 - \frac{3q}{p}\right) \log s.$$

On suppose  $p \geq 100q$ . Ensuite, l'application d'une minoration générale d'une telle forme linéaire permet de majorer  $p$  en fonction de  $q$ . En appliquant par exemple le corollaire 2 de [LMN] on obtient

$$\log |\Lambda| \geq -24.4 \left( \max\{21, \log(p/\log q) + 1\} \right)^2 q \log q \log s.$$

En comparant ces deux estimations de  $|\Lambda|$  (remarquer que le terme  $\log s$  disparaît) on obtient

$$p \leq 25q \log q \left( \max\{21, \log(p/\log q) + 1\} \right)^2.$$

Notons au passage que ceci implique

$$p < 4q^2 \quad \text{pour } p > 100\,000.$$

Un travail plus sérieux, utilisant pleinement le théorème principal de [LMN], conduit à

$$p \leq 2.77q (\log(p/\log q) + 3.94)^2 \log p, \quad \text{pour } p \geq 503.$$

La formule  $x - \varepsilon = p^{q-1}a^p = r^q/p$  permet ensuite de montrer que la nouvelle forme linéaire

$$\Lambda' := q \log(y + \varepsilon) - p \log(x - \varepsilon) = p \log q - q \log p - pq \log(r/s)$$

est elle aussi « très petite ». Et une minoration de formes linéaires en trois logarithmes fournit une estimation de la forme

$$q \leq C \log^5 p,$$

pour une certaine constante  $C$  que l'on peut effectivement calculer. A partir de là il est clair que  $p$  et  $q$  sont bornés.

En utilisant le meilleur résultat actuel sur les formes en trois logarithmes [BBGMS], pour les exposants de l'équation initiale de Catalan  $x^m - y^n = 1$ , on peut obtenir une majoration de l'ordre suivant

$$\max\{m, n\} < 10^{17}.$$

#### 4. Les critères algébriques

Nous présentons la liste complète des différents critères connus sur l'équation de Catalan avant 2002. Le premier critère a été démontré par Inkeri [I1].

**Théorème (Inkeri, 1964).** — *Soient  $p$  et  $q$  des nombres premiers impairs, avec  $p \equiv 3 \pmod{4}$ . Alors, si  $q$  ne divise pas le nombre de classes  $h(-p)$  du corps quadratique imaginaire  $\mathbb{Q}(\sqrt{-p})$ , et si l'équation  $x^p - y^q = 1$  admet une solution non triviale, on a la congruence*

$$p^{q-1} \equiv 1 \pmod{q^2}.$$

En passant, nous remarquons que, d'après la dernière assertion du corollaire du théorème de Cassels, la condition  $p^{q-1} \equiv 1 \pmod{q^2}$  équivaut à  $q^2 \mid x$ .

Le principe de la preuve d'Inkeri consiste à factoriser la relation

$$\frac{x^p - 1}{x - 1} = pu^p$$

dans le corps quadratique imaginaire  $\mathbb{Q}(\sqrt{-p})$  et bien sûr l'hypothèse  $q \nmid h(-p)$  est essentielle pour obtenir une factorisation utilisable. Ce n'est que 25 ans plus tard qu'Inkeri [I2] a obtenu un critère valable dans le cas  $p$  congru à 1 modulo 4 :

**Théorème (Inkeri, 1990).** — *Si l'équation de Catalan  $x^p - y^q = 1$  possède des solutions entières non triviales  $x, y$  et si, de plus, le nombre de classes  $H_p$  du corps cyclotomique  $\mathbb{Q}(e^{2i\pi/p})$  n'est pas divisible par  $p$ , alors on a la congruence*

$$p^{q-1} \equiv 1 \pmod{q^2}.$$

Pour la démonstration, on factorise cette fois l'expression  $(x^p - 1)/(x - 1) = pu^p$  dans le corps cyclotomique  $\mathbb{Q}(e^{2i\pi/p})$ . Mais ce critère a l'inconvénient de faire intervenir un corps de degré  $p - 1$  et en pratique on ne parvient pas à calculer  $H_p$  pour  $p \geq 71$ . Un premier progrès a été obtenu par Mignotte [M2] et ce résultat a été amélioré de façon importante par W. Schwarz [S].

**Théorème (W. Schwarz, 1995).** — *Soient  $p \neq q$  deux nombres premiers impairs. Soit  $\mathbb{K}^{(p)}$  le plus petit sous corps imaginaire du corps cyclotomique  $\mathbb{Q}(e^{2i\pi/p})$  et soit  $h^-(\mathbb{K}^{(p)})$  le nombre de classes relatif de  $\mathbb{K}^{(p)}$ . Alors l'équation de Catalan  $x^p - y^q = 1$  n'a pas de solution non triviale si*

$$q \nmid h^-(\mathbb{K}^{(p)}) \quad \text{et} \quad p^{q-1} \not\equiv 1 \pmod{q^2}.$$

Le corps  $\mathbb{K}^{(p)}$  est de degré deux pour  $p \equiv 3 \pmod{4}$  [on retrouve le premier critère d'Inkeri], de degré 4 pour  $p \equiv 5 \pmod{8}$ , ..., et plus généralement de degré  $D = 2^d$ , la plus grande puissance de deux qui divise  $p - 1$ . La plupart du temps ce degré est nettement plus petit que  $p - 1$ , premier progrès par rapport au second critère d'Inkeri [mais pas toujours, si  $p = 65537$  alors  $D = 65536$ ].

Mais l'intérêt pratique d'avoir remplacé un nombre de classes par le nombre de classes relatif est considérable, ce dernier se calcule de façon élémentaire [ce n'est pas toujours facile, pour  $p = 65537$  on a  $h^-(\mathbb{K}^{(p)}) > 10^{30\,000}$ ], voir à ce sujet le livre de Washington.

Tous ces ennuis avec les nombres de classes ont été résolus de manière magistrale par P. Mihăilescu [Mi].

**Théorème (Mihăilescu, 1999).** — Soient  $p$  et  $q$  deux nombres premiers impairs, alors si l'équation de Catalan  $x^p - y^q = 1$  possède une solution non triviale on a

$$p^{q-1} \equiv 1 \pmod{q^2} \quad \text{et} \quad q^{p-1} \equiv 1 \pmod{p^2}.$$

L'astuce de Mihăilescu consiste à faire intervenir un élément de Stickelberger au cours de la preuve du second critère d'Inkeri. La démonstration nécessite à peine plus d'une page, en voici une version abrégée. Une autre démonstration a été donnée par J.C. Puchta [P].

**Démonstration.** — Le corollaire au théorème de Cassels donne

$$\frac{x^p - 1}{x - 1} = pu^q.$$

Posons  $\zeta = e^{2i\pi/p}$ , alors  $X^{p-1} + \dots + X + 1 = \prod_{j=1}^{p-1} (X - \zeta^j)$  et donc  $p = \prod_{j=1}^{p-1} (1 - \zeta^j)$ , ainsi

$$(*) \quad \prod_{j=1}^{p-1} \frac{x - \zeta^j}{1 - \zeta^j} = u^q.$$

Puisque  $x \equiv 1 \pmod{p}$  les termes  $(x - \zeta^j)/(1 - \zeta^j)$  appartiennent à  $\mathbb{Z}[\zeta]$ , et il est facile de vérifier qu'ils sont deux à deux premiers entre eux. D'où une factorisation entre idéaux qui donne en particulier

$$\left( \frac{x - \zeta}{1 - \zeta} \right) = \mathfrak{a}^q.$$

Le groupe de Galois  $G$  du corps cyclotomique  $\mathbb{Q}(\zeta)$  est constitué par les isomorphismes  $\sigma_c : \zeta \mapsto \zeta^c$ ,  $c \in \{1, 2, \dots, p-1\}$ . D'après Stickelberger l'élément  $\theta = \sum_{c=1}^{p-1} c \sigma_{c-1} \in \mathbb{Z}[G]$  annule le groupe des classes d'idéaux de  $\mathbb{Q}(\zeta)$  ([W], Th. 6.10). Ceci permet d'écrire

$$(x - \zeta)^\theta = (1 - \zeta)^\theta \varepsilon \gamma^q, \quad \gamma \in \mathbb{Z}[\zeta],$$

où  $\varepsilon$  est une unité.

Si  $c' \in \{1, 2, \dots, p-1\}$  vérifie  $cc' \equiv 1 \pmod{p}$  et si on pose  $\lambda = (1 - \zeta)^\theta$  alors

$$\zeta^\theta = \prod_{c=1}^{p-1} (\zeta^{\sigma_{c'}})^c = \zeta^{\sum_{c=1}^{p-1} cc'} = \zeta^{p-1} = \zeta^{-1}$$

$$\text{et} \quad \lambda = \zeta^\theta (\zeta^{-1} - 1)^\theta = (-1)^{(p-1)/2} \zeta^{-1} \bar{\lambda},$$

où la barre désigne la conjugaison complexe. Il est clair que  $\zeta$  est une puissance  $q$ -ième dans  $\mathbb{Z}[\zeta]$  et on sait depuis Kummer que  $\varepsilon = \zeta^k \eta$ , où  $\eta$  est une unité réelle. Il existe donc  $\alpha \in \mathbb{Z}[\zeta]$  tel que

$$(1 - \zeta^{-1}x)^\theta = \eta\lambda\alpha^q.$$

Par conjugaison complexe,

$$(1 - \zeta x)^\theta = \eta\lambda\beta^q,$$

pour un certain  $\beta \in \mathbb{Z}[\zeta]$ , et on a

$$(1 - \zeta^{-1}x)^\theta - (1 - \zeta x)^\theta = \eta\lambda(\alpha^q - \beta^q).$$

Noter que

$$(1 - \zeta x)^\theta = \prod_{c=1}^{p-1} (1 - \zeta^c x)^c = 1 - x \sum_{c=1}^{p-1} c \zeta^c + x^2 \xi = 1 - x\mu + x^2 \xi, \quad \mu, \xi \in \mathbb{Z}[\zeta],$$

ce qui implique

$$\eta\lambda(\alpha^q - \beta^q) = x(\mu - \bar{\mu}) + x^2\omega, \quad \omega \in \mathbb{Z}[\zeta].$$

Soit  $\mathcal{Q}$  un idéal premier au-dessus de  $q$ . Il est facile de voir que

$$\alpha^q - \beta^q = (\alpha - \beta)^q + q(\alpha - \beta)\nu, \quad \nu \in \mathbb{Z}[\zeta],$$

ainsi  $\mathcal{Q}$  divise  $\alpha - \beta$ . Il en résulte que  $\mathcal{Q}^2$  divise  $\alpha^q - \beta^q$  et aussi  $x(\mu - \bar{\mu})$ . Mais

$$\mu - \bar{\mu} = \sum_{c=1}^{p-1} c(\zeta^c - \zeta^{-c}) = 2 \sum_{c=1}^{p-1} c' \zeta^c \not\equiv 0 \pmod{q}.$$

On peut donc supposer que  $\mathcal{Q}$  ne divise pas  $\mu - \bar{\mu}$ , donc  $\mathcal{Q}^2$  divise  $x$ . Mais  $q$  n'étant pas ramifié dans  $\mathbb{Q}(\zeta)$  ceci implique que  $q^2$  divise  $x$ . Donc  $p^{q-1} \equiv 1 \pmod{q^2}$ .  $\square$

Mais il reste encore quelques difficultés pour appliquer ce critère : le cas des doubles paires de Wieferich, c'est-à-dire des couples  $(p, q)$  tels qu'on ait simultanément  $p^{q-1} \equiv 1 \pmod{q^2}$  et  $q^{p-1} \equiv 1 \pmod{p^2}$ . Compte tenu des majorations du paragraphe précédent, il y en a trois pour  $\min\{p, q\} < 100\,000$ , qui sont  $(83, 4871)$ ,  $(193, 4877)$  et  $(2903, 18787)$ . Le cas des deux premières est facilement traité par le résultat très élémentaire suivant [M1] (qui utilise bien sûr les formules de Cassels).

**Théorème (Mignotte, 1993).** — Soient  $p$  et  $q$  des nombres premiers impairs et soit  $\ell$  un nombre premier de la forme  $\ell = hpq + 1$ . Soit  $a'$  un entier vérifiant  $a'p \equiv 1 \pmod{\ell}$ . Alors, si on a simultanément

$$q^{hq} \not\equiv 1 \pmod{\ell}, \quad p^{hp} \not\equiv 1 \pmod{\ell},$$

et

$$\forall j \in \{0, 1, \dots, hp - 1\}, \quad \left( (1 + a'g^{jq})^p - 1 \right)^{hp} \not\equiv 1 \pmod{\ell},$$

l'équation de Catalan  $x^p - y^q = 1$  ne possède pas de solution non triviale.

Pour exclure les paires (83, 4871) et (193, 4877) on prend respectivement  $\ell = 16\,980\,307$  et  $\ell = 30\,120\,353$ . La paire (2903, 18787) résiste à ce critère, on peut cependant l'éliminer de façon laborieuse en travaillant dans le corps  $\mathbf{Q}(\sqrt{-2903})$ .

En 1999, Y. Bugeaud et G. Hanrot [BH], inspirés par les travaux de Y. Bilu et G. Hanrot sur les équations superelliptiques, ont obtenu un nouveau critère très original.

**Théorème (Bugeaud–Hanrot, 1999).** — Soient  $p > q$  deux nombres premiers impairs. Soit  $h_q^-$  le nombre de classes relatif du corps cyclotomique  $\mathbf{Q}(e^{2i\pi/q})$ . S'il existe des entiers  $x$  et  $y > 0$  tels que  $|x^p - y^q| = 1$ , alors  $p$  divise  $h_q^-$ .

Ce résultat permet d'éliminer les trois paires de Wieferich précédentes en une minute de calculs sur ordinateur. De plus il montre, sans faire appel aux formes linéaires de logarithmes, que si on fixe l'un des exposants alors l'autre ne peut prendre qu'un nombre fini de valeurs. La connaissance des premiers  $h(-p)$  (voir la table à la fin du livre de Washington) permet instantanément de montrer que si  $x^p - y^q = 1$  a une solution non triviale avec  $p$  et  $q$  impairs alors  $\min\{p, q\} \geq 41$ .

## 5. Calculs

Après plusieurs années de calculs avec une machine parallèle, le résultat suivant a été obtenu [MR].

**Théorème (Mignotte–Roy, 1998).** — Pour l'équation de Catalan  $x^p - y^q = \pm 1$  avec  $p$  et  $q$  premiers et  $p > q \geq 3$ , on a

$$q > 100\,000$$

et toujours  $p < 4q^2$ .

Aujourd'hui, grâce au critère de Mihăilescu ce calcul est considérablement simplifié et un jour de calcul suffit pour vérifier ce résultat. Mais, avant septembre 1999 ce n'était pas possible. On utilisait, pour chaque  $q$  fixé la borne sur  $p$  obtenue par les formes linéaires en deux logarithmes et pour chaque paire  $(q, p)$  le critère de W. Schwarz [et — si nécessaire — ce critère pour la paire  $(p, q)$ ]. Le critère de Mihăilescu a permis à Jon Graham (2000) de montrer que  $\min\{p, q\} > 3.4 \times 10^8$ , compte tenu des majorations des exposants il en résulte que si  $x^m - y^n = 1$  avec  $m, n$  impairs et  $xy \neq 0$  alors  $m$  et  $n$  sont nécessairement premiers.

En utilisant le nouveau résultat de Mihăilescu (2002) on peut encore économiser beaucoup de temps puisqu'il suffit maintenant de considérer le cas  $p \equiv 1 \pmod{q}$ . De plus, ce nouveau travail élimine aussi instantanément les trois paires de Wieferich  $(p, q)$  du paragraphe précédent du fait qu'aucune d'elles ne vérifie  $p \equiv 1 \pmod{q}$  ou  $q \equiv 1 \pmod{p}$ .

Notons aussi que le cas  $p \equiv 1 \pmod{q}$ , avec  $q$  impair et  $p > q$ , ne peut se produire puisqu'il impose  $p \geq 1 + 4q^2$  [en effet,  $1 + 2q^2$  est toujours divisible par trois], ce qui contredit le théorème ci-dessus. Cette remarque joue un rôle important dans la dernière partie : la conclusion de Mihăilescu (2002) suppose  $p > q$  et  $p \not\equiv 1 \pmod{q}$ . C'est pour cette raison, et seulement pour elle, que les formes linéaires de logarithmes servent dans la preuve complète. [Le critère de Bugeaud-Hanrot ne peut être appliqué, les valeurs de  $h_q^-$  étant beaucoup trop grandes.]

## 6. La conclusion de Mihăilescu

Dans cette dernière section on supposera toujours

$$p > q \geq 5 \quad \text{et} \quad p \not\equiv 1 \pmod{q^2}$$

ce qui est possible d'après les calculs indiqués au paragraphe précédent.

Nous rappelons qu'une preuve a été rédigée par Y. Bilu et qu'elle figure sur sa page web. Nous ne donnerons donc que très peu de détails.

Soit  $\zeta$  une racine primitive  $p$ -ième de l'unité. La première originalité de Mihăilescu est de travailler dans le corps réel  $\mathbb{Q}(\zeta + \zeta^{-1})$ , le sous corps réel maximal de  $\mathbb{Q}(\zeta)$ , alors que tous les autres critères [à l'exception bien sûr du critère sur les congruences modulo  $\ell$ ] utilisaient le corps  $\mathbb{Q}(\zeta)$  tout entier ou un de ses sous-corps complexes. Posons

$$G = \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}), \quad K = \mathbb{Q}(\zeta + \zeta^{-1}), \quad G^+ = \text{Gal}(K/\mathbb{Q}), \quad R = \mathbb{F}_q[G^+].$$

Il étudie ensuite certains  $R$ -modules et l'action d'éléments bien choisis de l'anneau  $R$ . En particulier, le  $R$ -module  $E$  des unités positives de  $K$  joue un rôle important, ainsi que  $C$ , celui des unités cyclotomiques de  $K$ . Un résultat essentiel dans la preuve est le théorème suivant [Th], voir aussi [W], seconde édition, Th. 15.2.

**Théorème (Thaine, 1988).** — Soit  $H$  le groupe des classes d'idéaux du corps  $K$  et soit  $\tilde{\Theta} \in \mathbb{Z}[G]$  qui annule la  $q$ -partie<sup>3</sup> du groupe  $E/C$ . Alors  $\Theta$  annule aussi la  $q$ -partie de  $H$ .

On reprend la décomposition (\*) considérée plus haut, cette fois en regroupant les éléments conjugués (sur  $\mathbb{C}$ ) et on fait agir des  $\Theta \in \mathbb{F}_q[G^+]$  convenables. Mais les détails sont trop délicats pour être expliqués plus avant dans ce survol.

Maurice Mignotte

Université Louis Pasteur, Strasbourg  
mignotte@math.u-strasbg.fr

### Références

- [B] A. Baker .— Bounds for the solutions of the hyperelliptic equation, *Proc. Camb. Phil. Soc.*, **65**, 1969, p. 439–444.
- [Bi] Y. Bilu .— Catalan's conjecture (after Mihailescu), manuscrit, 2002.
- [BBGMS] C.D. Bennett, J. Blass, A.M.W. Glass, D.B. Meronk, R.P. Steiner .— Linear forms in the logarithms of three positive rational numbers, *J. Th. Nombres Bordeaux*, **9**, 1997, p. 97–136.
- [BH] Y. Bugeaud, G. Hanrot .— Un nouveau critère pour l'équation de Catalan, *Mathematika*, **47**, 2000, p. 63–73.
- [C] J.W.S. Cassels .— On the equation  $a^x - b^y = 1$ , II, *Proc. Cambridge Society* **56**, 1960, p. 97–103.
- [Ca] E. Catalan .— Note extraite d'une lettre adressée à l'éditeur, *J. für reine und ang. Math.*, **27**, 1844, p. 192.
- [Ch] E.Z. Chein A note on the equation  $x^2 = y^q + 1$ , *Proceedings of the Amer. Math. Soc.*, 1976, p. 83–84.
- [E] L. Euler .— Theorematum quorundam arithmetorum demonstrationes, *Comm. Acad. Sci. Petrop.*, **10**, 1738, p. 125–146. ( *Opera Omnia*, Ser. I, Vol. II, *Commentationes Arithmeticae I*, p. 38–58, B.G. Teubner, Basel, 1915).
- [I1] K. Inkeri .— On Catalan's problem, *Acta Arith.* **9**, 1964, p. 285–290.
- [I2] K. Inkeri .— On Catalan's conjecture, *J. Number Th.* **34**, 1990, p. 142–152.
- [K] Ko Chao .— On the diophantine equation  $x^2 = y^n + 1$ ,  $xy \neq 0$ , *Sci. Sinica*, **14**, 1965, p. 457–460.
- [L] M. Langevin .— Quelques applications de nouveaux résultats de van der Poorten, *Sém. Delange-Pisot-Poitou*, 1977/78, Paris, Exp. 4, 7 pages.
- [LMN] M. Laurent, M. Mignotte, Y. Nesterenko .— Formes linéaires en deux logarithmes et déterminants d'interpolation, *J. Numb. Th.*, **55**, 1995, p. 285–321.
- [Le] V.A. Lebesgue .— Sur l'impossibilité en nombres entiers de l'équation  $x^m = y^2 + 1$ , *Nouv. Ann. Math.*, **9**, 1850, p. 178–181.

<sup>3</sup> C'est-à-dire le  $q$ -sous-groupe de Sylow de ce groupe.

- [M1] M. Mignotte .— Un critère élémentaire pour l'équation de Catalan, *C.R. Math. Rep. Acad. Sci. Canada*, **15**, n<sup>o</sup> 5, 1993, p. 199–200.
- [M2] M. Mignotte .— A criterion on Catalan's equation, *J. Numb. Th.*, **52**, 1995, p. 280–283.
- [MR] M. Mignotte, Y. Roy .— Minorations pour l'équation de Catalan, *C. R. Acad. Sci. Paris*, **324**, 1997, p. 377–380.
- [Mi] P. Mihăilescu .— A class number free criterion for Catalan's conjecture, *J. Number Th.*, à paraître.
- [Mo] L.J. Mordell .— *Diophantine Equations*, Acad. Press, Londres, 1969.
- [N1] T. Nagell .— Sur l'impossibilité de l'équation indéterminée  $z^p + 1 = y^2$ , *Nordsk. Mat. Forenings Skr. (1)*, 1921, No. 4, 10 pages.
- [N2] T. Nagell .— Sur une équation diophantienne à deux indéterminées, *Det Kong. Norske Vidensk. Selskab Forhandlinger, Trondhejm*, No. 38, 1934, p. 136–139.
- [P] J.C. Puchta .— On a criterion for Catalan's conjecture, *Ramanujan J.*, **5**, 2001, p. 405–407.
- [R] P. Ribenboim .— *Catalan's Conjecture*, Acad. Press, Boston, 1994.
- [S] W. Schwarz .— A note on Catalan's equation, A note on Catalan's equation, *Acta Arith.*, **72**, 1995, p. 277–279.
- [Th] F. Thaine .— On the ideal class groups of the real abelian number fields, *Annals of Math.*, **128**, 1988, p. 1–18.
- [Ti] R. Tijdeman .— On the equation of Catalan, *Acta Arith.*, **29**, 1976, p. 197–209.
- [W] L.C. Washington .— *Introduction to cyclotomic fields*, Springer-Verlag, New York, 1982.
- [Ri] P. Ribenboim.— Consecutive powers; *Expositiones Mathematicae*, **2**, 1984, p. 193–221.
- [Sch] R. Schoof.— Communication personnelle, janvier 1992.
- [St1] C. Størmer.— Quelques théorèmes sur l'équation de Pell  $x^2 - Dy^2 = \pm 1$  et leurs applications; *Christiania. Videnskabens Selskabs Skifter, Math. Nat. Kl.*, n<sup>o</sup> 2, 1897, 48 pages.
- [St2] C. Størmer.— Solution d'un problème curieux qu'on rencontre dans la théorie élémentaire des logarithmes; *Nyt Tidsskrift für Math.*, (Copenhague) B, **19**, 1908, p. 1–7.
- [Ti] R. Tijdeman.— On the equation of Catalan; *Acta Arith.*, **29**, 1976, p. 197–209.
- [Wal] M. Waldschmidt.— Minorations de combinaisons linéaires de logarithmes de nombres algébriques, manuscrit, juillet 1982.

# Mathématiques et reconnaissance des formes

O. Catoni

---

La reconnaissance des formes, nous reviendrons sur la signification donnée ici à ce terme, représente un enjeu important de la recherche en informatique. Notre propos sera ici d'expliquer pourquoi de nombreux mathématiciens ont contribué à faire progresser ce domaine de recherche depuis maintenant plus de vingt ans. Nous souhaiterions aussi convaincre le lecteur du fait qu'il s'agit d'un problème complexe et difficile, dans lequel les avancées ont été au fil des ans modestes et progressives, au prix d'élaborations théoriques importantes. Nous sommes convaincus qu'il continuera d'en être ainsi : nous ne pensons pas qu'il existe de recette miracle ni non plus de difficulté rédhibitoire, mais que des progrès continueront à voir le jour, et qu'ils seront le fruit des efforts conjugués d'une communauté de chercheurs qui ne cesse de croître et qui enjambe les clivages traditionnels entre disciplines.

En un mot la reconnaissance des formes consiste à repérer dans des signaux compliqués (signal de parole ou images numérisées, mais aussi texte en langue naturel ou séquence d'ADN ...) la présence de certaines structures (ou objets, ou formes ...) et à les classer en un nombre restreint de classes pertinentes pour l'application envisagée, le tout de façon automatique, à l'aide d'un ordinateur. Cette définition peut paraître floue ; la discipline tire en fait sa cohérence de l'existence de difficultés techniques communes aux différents cas de figure possibles.

Indiquons tout d'abord par quelques exemples dans quels contextes pratiques on fait appel à la reconnaissance des formes. Il s'agit en général de reproduire de façon automatique des tâches d'interprétation et de discrimination réalisées par le cerveau humain avec une certaine facilité, mais par des voies difficiles à élucider. Quelques illustrations en vrac dans le domaine de l'imagerie : interpréter des images médicales et les classer en fonction des pathologies dont elles témoignent, interpréter automatiquement des images satellites (y reconnaître les différents types de sols, les réseaux routiers et fluviaux, les différents types de bâtiments ...), traduire un texte manuscrit en caractères d'imprimerie, interpréter des images vidéo prises par une caméra embarquée sur un objet en mouvement (par exemple une voiture : reconnaître les limites de la route, les autres véhicules, les piétons, les panneaux de signalisation, les obstacles éventuels ...), localiser les individus sur des photos de groupe (par exemple pour effectuer des tâches de vidéo-surveillance, évaluer le nombre de personnes présentes lors d'une manifestation publique, etc.).

D'autres domaines d'application : la reconnaissance de la parole (mono ou multilocuteur, continue ou discontinue), la classification automatique de textes (par exemple classer les dépêches d'une agence de presse en fonction du thème traité), l'analyse de séquences d'ADN (détecter automatiquement l'emplacement des gènes, rapprocher les séquences similaires dans des espèces différentes, ...). Il convient maintenant de mettre en lumière les points communs de ces applications à première vue disparates.

Essayons pour cela de recenser quelques difficultés qui fondent l'unité de la discipline. Une première difficulté vient du flou habituel avec lequel la tâche est définie : en fait il s'agit dans les exemples cités de l'automatisation d'une tâche effectuée par un être humain, si bien que le résultat souhaité est le plus souvent défini par l'exemple. C'est ce que l'on appelle une situation d'apprentissage *supervisée*. Développons le premier exemple cité, celui de l'interprétation d'images médicales, par exemple des radiographies : il est possible de demander à un radiologue de circonscrire et de nommer des structures pathologiques sur un ensemble de radiographies, mais il est en général impossible de résumer l'expertise fournie par le radiologue pour poser son diagnostic en une série de critères simples et quantifiés susceptibles de permettre à un ordinateur d'effectuer la même analyse. De plus deux radiologues différents ne poseront pas forcément toujours le même diagnostic ... cette marge d'incertitude ou d'erreur donne au problème une dimension statistique, sur laquelle nous reviendrons par la suite.

Une autre difficulté générique est celle de la localisation de la structure à reconnaître : pour reprendre notre exemple, il ne s'agit pas uniquement de dire si une zone donnée d'une radiographie correspond à une structure pathologique, mais aussi de délimiter cette zone. Le sous-problème consistant à délimiter la zone correspondant à la structure recherchée s'appelle *segmentation*. La segmentation est un problème fondamental de la reconnaissance des formes, qui conditionne tout le reste de la marche à suivre et n'est à ce jour que très mal résolu. Plus précisément, la difficulté du problème de segmentation associée à une tâche de reconnaissance donnée conditionne en grande partie sa difficulté. Par exemple, il est beaucoup plus facile de reconnaître un objet sur un fond uni que sur un fond texturé qui rend problématique la détermination de son contour extérieur (ceci est d'ailleurs aussi valable pour la vision humaine). De même la parole continue est beaucoup plus difficile à interpréter que des mots prononcés isolément dans une ambiance sonore présentant un faible bruit de fond. En fait, dans les situations, souvent en partie artificielles, où la segmentation est facile à effectuer, on peut appliquer des méthodes *globales* de classification qui deviennent complètement inopérantes quand la segmentation doit avoir lieu en même temps que la reconnaissance. D'une façon schématique, on peut dire que les problèmes

de reconnaissance pour lesquels on possède actuellement des méthodes efficaces sont des situations dans lesquelles les zones d'intérêt sont faciles à segmenter.

Le problème de la segmentation s'apparente à une question à laquelle les mathématiciens ont beaucoup réfléchi depuis que les mathématiques existent – celui du *passage du local au global*, car c'est bien de cela qu'il s'agit : en l'absence de moyens de détection évidents des contours de l'objet à reconnaître, la présence de cet objet doit être déduite d'une accumulation d'indices locaux. Plusieurs outils sont alors à forger : il faut tout d'abord définir des indices locaux qui permettent d'accumuler le maximum d'information possible sur les objets à reconnaître sous la forme la plus condensée possible, et ce à différentes échelles de localisation. Souvent, ces indices locaux sont le produit de développements récents de l'analyse harmonique, en particulier les différentes déclinaisons possibles de la décomposition d'un signal ou d'une image en une superposition d'ondelettes. La théorie de l'approximation permet d'évaluer combien de coefficients sont nécessaires pour représenter avec un certain degré d'approximation les fonctions typiques de certains espaces fonctionnels (c'est-à-dire pour mailler par un réseau d'un certain pas dans la norme considérée la boule unité de cet espace). Les théorèmes d'approximation utilisent parfois la théorie du codage, ainsi que des arguments probabilistes, jetant ainsi un pont entre analyse fonctionnelle, théorie de l'information et probabilités. Des techniques d'EDP interviennent aussi pour définir des déformations des images qui permettent de les simplifier tout en préservant un certain nombre d'invariants et constituent ainsi l'une des approches possibles de la représentation multiéchelles des signaux à analyser. Une fois le système de représentation des indices locaux choisi, il convient de gérer d'une manière ou d'une autre l'accumulation de ces indices. La description et la sélection des arrangements d'indices locaux retenus pour la reconnaissance se heurte à des problèmes de complexité algorithmique, qui appellent là encore une approche statistique reposant sur une modélisation probabiliste, souvent inspirée par les modèles inventés par les physiciens de la mécanique statistique (champs de Markov, lois de Gibbs . . .), mais puisant aussi dans une tradition plus proprement statisticienne (modèles d'arbres de décision, modèles linéaires et « boosting »). En termes plus concrets, il est impossible d'examiner tous les indices locaux pouvant dénoter la présence d'un objet, et encore moins toutes les combinaisons de ces indices. Il faut faire un choix, dans un contexte trop complexe pour qu'une modélisation exhaustive des cas de figure pertinents soit possible, ou pour que l'intuition puisse être un guide suffisant. On se tourne alors vers des méthodes *statistiques* de choix de modèles et de détecteurs, liées à la *théorie de l'information*.

Sous l'impulsion de Vladimir Vapnik est ainsi née une discipline nouvelle : la *théorie statistique de l'apprentissage*, proche des statistiques et

de la théorie de l'information (au sens de Shannon, Kolmogorov et de leurs continuateurs), développée non seulement par des mathématiciens, mais aussi par des informaticiens du *machine learning*. Son but est encore une fois de lutter contre la *malédiction de la dimension* en arbitrant entre différents modèles de façon adaptative (au vu des données disponibles) à l'aide d'inégalités non asymptotiques indépendantes de la dimension (c'est-à-dire dont la qualité d'approximation ne dépend pas de la dimension de l'espace ambiant de la représentation, qui est le plus souvent très grande). Ces inégalités peuvent être obtenues de diverses manières, et entretiennent des liens profonds avec la théorie de la concentration de la mesure et l'analyse convexe.

La reconnaissance des formes sollicite ainsi des contributions venant de nombreux domaines des mathématiques, et en particulier de nombreux domaines de l'analyse. Elle pose des problèmes de modélisation d'un genre nouveau, dans lesquels le modèle est choisi en fonction des besoins du processus d'apprentissage et de reconnaissance et ne prétend pas rendre compte de façon exhaustive ou exacte de la structure des signaux analysés, ce qui serait dans la plupart des cas impossible. Au fur et à mesure des avancées (ou plutôt des piétinements!) de la recherche, on s'est ainsi aperçu que les liens entre les problèmes de synthèse (d'images, de paroles, etc.) et les problèmes de reconnaissance étaient beaucoup plus ténus que prévu, et même souvent inexistantes (sauf dans quelques cas particuliers, comme celui de la synthèse de textures). Pour illustrer cet apparent paradoxe nous prendrons l'exemple des photos numériques de visages : la production d'images de synthèse réalistes et la détection de visages sur des photographies numériques sont deux domaines de recherche bien avancés, cependant les solutions retenues pour effectuer ces deux tâches n'ont absolument rien à voir. Cette absence complète de réciprocité entre reconnaissance et synthèse se comprend mieux lorsque l'on songe qu'il s'agit dans un cas de reproduire *un unique* visage et dans l'autre de les caractériser *tous*. Le fait qu'il existe maintenant des outils mathématiques quantitatifs permettant d'appréhender cette distinction et de fonder en quelque sorte une *science de la variabilité des apparences* nous paraît – au delà des enjeux technologiques de la reconnaissance des formes – posséder un certain intérêt conceptuel.

Enfin, en guise de post-scriptum, j'aimerais demander par avance au lecteur averti d'excuser les omissions, les erreurs, les imprécisions et les généralisations hâtives qu'il ne manquera pas d'avoir relevées dans ces quelques lignes, où je sens bien que j'ai dû, à des fins de vulgarisation, simplifier et déformer mon sujet dans le but de le réduire à un faible nombre d'idées directrices, dont le choix, forcément tendancieux et contestable, ne reflète que ma sensibilité personnelle et les imperfections de mon jugement. J'ai aussi préféré ne mentionner que quelques noms d'une célébrité quasi-impersonnelle, plutôt que de commettre des

injustices et de froisser des susceptibilités en tentant vainement de citer tous ceux qui auraient mérité de l'être (au nombre desquels je n'ai pas la prétention de me compter).

*Olivier Catoni*

CNRS - Université Paris VI  
Laboratoire de Probabilités et Modèles Aléatoires

## Géométrie non commutative d'après Alain Connes : la notion de triplet spectral

G. Skandalis

---

*L'Académie Royale des Sciences de Suède, réunie en assemblée générale le 24 janvier 2001, a décidé de décerner le Prix Crafoord pour l'année 2001, dans le domaine des mathématiques, à Alain Connes, professeur à l'IHÉS et au Collège de France, Paris, pour ses travaux importants dans le domaine de la théorie des algèbres d'opérateurs et pour avoir été l'un des fondateurs de la géométrie non-commutative.*

*Le mathématicien français Alain Connes a ouvert de nouvelles voies dans la théorie des algèbres d'opérateurs et est l'un des fondateurs de la géométrie non-commutative. Cette dernière est un domaine entièrement nouveau des mathématiques à la création duquel Alain Connes a apporté une contribution décisive.*

*Pour l'illustrer nous avons reçu le texte suivant, écrit par Georges Skandalis. Il est à noter aussi qu'Alain Connes a été l'un des conférenciers de l'Université de tous les Savoirs, et que son texte est disponible dans le volume consacré aux Mathématiques publié aux Éditions Odile Jacob.*

★ ★ ★

Qu'est-ce que la géométrie non commutative selon Alain Connes ? D'abord, des exemples issus de la géométrie, de l'analyse harmonique, de la physique, voire de la théorie des nombres... La motivation est avant tout physique : on veut allier la relativité – donc la géométrie riemannienne – à la physique quantique, donc non commutative.

Je présente ici quelques aspects de la théorie. L'exposé qui suit se veut non technique. S'il m'arrive d'employer quelques « gros mots » par ci par

là, c'est en espérant qu'ils aideront ceux qui connaissent ce jargon, mais qu'ils ne seront pas un obstacle pour les autres.

Un bon analogue non commutatif de la notion d'espace (localement) compact est fourni par la théorie des  $C^*$ -algèbres.

Rappelons qu'une  $C^*$ -algèbre est une algèbre de Banach complexe  $A$  munie d'une *involution*  $a \mapsto a^*$  (antilinéaire et qui vérifie  $(ab)^* = b^*a^*$  pour  $a, b \in A$ ) et telle que, pour tout  $a \in A$ , on ait  $\|a^*a\| = \|a\|^2$ .

Les  $C^*$ -algèbres commutatives sont exactement les algèbres de Banach des fonctions continues (nulles à l'infini) sur un espace (localement) compact. On peut donc considérer les  $C^*$ -algèbres non commutatives comme des «espaces (localement) compacts non commutatifs».

Le but de la géométrie non commutative selon Connes est d'essayer d'appliquer certains outils de la géométrie à certaines  $C^*$ -algèbres non commutatives naturelles, qui peuvent être considérées comme des «variétés différentielles non commutatives». Certains outils passent sans problème au cadre non commutatif : la théorie des fibrés vectoriels, donne celle des modules projectifs, qui sont classifiés par la  $K$ -théorie. La cohomologie de de Rham passe plus difficilement ; son analogue non commutatif, la *cohomologie cyclique* de Connes, a été un des premiers succès de la géométrie non commutative. Ensuite, peu à peu Connes a pu construire dans cette cohomologie cyclique les analogues du cycle fondamental, des formes différentielles, des connexions, ainsi que plusieurs autres objets courants de la géométrie.

On dispose dans notre étude de plusieurs exemples naturels, sur lesquels on voudrait pouvoir appliquer des idées géométriques :

– *Le dual d'un groupe de type fini.* Soit  $\Gamma$  un groupe. Il lui est naturellement associé l'algèbre  $\mathbf{C}\Gamma$  : le  $\mathbf{C}$ -espace vectoriel admettant une base  $(u_g)_{g \in \Gamma}$ , muni du produit défini par  $u_g u_h = u_{gh}$  (pour  $g, h \in \Gamma$ ). Son adhérence  $C_r^*(\Gamma)$  dans la représentation régulière dans l'espace hilbertien  $\ell^2(\Gamma)$  est une  $C^*$ -algèbre appelée  *$C^*$ -algèbre réduite de  $\Gamma$* . Signalons que, suivant les propriétés étudiées, on peut être amené à considérer une autre  $C^*$ -algèbre complétion de  $\mathbf{C}\Gamma$  : la  $C^*$ -algèbre maximale,  $C^*$ -algèbre enveloppante de l'algèbre  $\mathbf{C}\Gamma$ . Lorsque  $\Gamma$  est commutatif, l'algèbre  $C_r^*(\Gamma)$  est l'algèbre des fonctions continues sur le groupe (compact)  $\widehat{\Gamma}$  dual de Pontrjagyn de  $\Gamma$ . Si  $\Gamma$  est de plus de type fini,  $\widehat{\Gamma}$  est une variété (un tore). Lorsque  $\Gamma$  n'est plus commutatif mais reste de type fini, il est naturel de considérer la  $C^*$ -algèbre  $C_r^*(\Gamma)$  comme une variété non commutative.

– *Les produits croisés.* Lorsque le groupe  $\Gamma$  opère par automorphismes sur une algèbre  $A$ , on forme ce produit croisé  $A \rtimes \Gamma$  : c'est l'algèbre engendrée par  $A$  et  $\mathbf{C}\Gamma$  avec la règle de commutation  $u_g a = (g.a)u_g$  pour  $a \in A$ ,  $g \in \Gamma$ , où l'on a noté  $a \mapsto g.a$  l'action de  $g$  dans  $A$ .

Dans les exemples qui nous intéressent, l'algèbre  $A$  est l'algèbre des fonctions continues sur une variété  $V$  et l'action du groupe  $\Gamma$  (de type fini) sur  $A$  provient d'une action par difféomorphismes sur  $V$ .

L'exemple le plus simple, pour lequel de très nombreux calculs ont été effectués est celui du «tore non commutatif» :

Notons  $\mathbf{U} = \{z \in \mathbf{C}; |z| = 1\}$ ; le groupe  $\Gamma = \mathbf{Z}$  opère sur  $\mathbf{U}$  par une rotation irrationnelle :  $n.z = e^{2i\pi n\theta}z$ , où  $\theta \in \mathbf{R} \setminus \mathbf{Q}$ . Notons alors  $u = u_1$  et  $v : z \mapsto z$ ,  $v \in A = C(\mathbf{U})$ .

Le produit croisé  $A \rtimes \mathbf{Z}$  est la  $C^*$ -algèbre universelle engendrée par deux opérateurs unitaires  $u, v$  tels que  $uv = e^{2i\pi\theta}vu$ .

Cette algèbre s'appelle le tore non commutatif, puisque son analogue commutatif, obtenu pour  $\theta = 0$ , est la  $C^*$ -algèbre universelle engendrée par deux opérateurs unitaires qui commutent, c'est-à-dire  $C^*(\mathbf{Z}^2) = C(\widehat{\mathbf{Z}^2}) = C(\mathbf{T}^2)$ .

Une variante très importante du produit croisé est :

– *La  $C^*$ -algèbre d'un feuilletage.* C'est l'exemple de base, qui guide les travaux dans le domaine depuis une vingtaine d'années : celui de la «variété non commutative»  $V/F$ , espace des feuilles d'un feuilletage  $F$  sur une variété  $V$ . En se plaçant sur une transversale (ouverte)  $M$ , on est amené à considérer le produit croisé de l'algèbre  $C_0(M)$  des fonctions continues nulles à l'infini sur  $M$  par un (pseudo)-groupe de difféomorphismes.

Pour pouvoir adapter les outils de la géométrie dans le cadre non commutatif, on cherche à exprimer les divers outils de la géométrie d'une variété  $V$  à l'aide d'une algèbre de fonctions sur  $V$ , sans utiliser la commutativité de cette algèbre.

Prenant modèle sur l'exemple des opérateurs de type signature ou Dirac sur une variété riemannienne, Alain Connes a proposé comme objet de départ d'«une géométrie non commutative» un triplet  $(H, A, D)$  où  $H$  est un espace de Hilbert,  $A$  est une sous-algèbre de l'algèbre  $\mathcal{L}(H)$  des opérateurs continus sur  $H$ , et  $D$  est un opérateur autoadjoint non borné à résolvante compacte, agissant sur  $H$ . Un tel triplet  $(H, A, D)$  est appelé un *triplet spectral*. Le tout est maintenant de mettre sur notre triplet spectral suffisamment de conditions pour pouvoir faire des calculs, tout en incluant suffisamment d'exemples. Ces conditions varient d'un exemple à l'autre. Cela montre en fait la richesse de la théorie.

## La géométrie non commutative dans le cas commutatif

Soit  $V$  une variété riemannienne compacte. Notons  $C(V)$  l'algèbre des fonctions continues sur  $V$ .

Soit  $D$  un «bon» opérateur différentiel elliptique d'ordre 1. Pour fixer

les idées, on va supposer que  $D$  est l'opérateur de signature  $D = d + d^*$ . On va considérer  $D$  comme opérateur autoadjoint non borné, à résolvante compacte, agissant sur l'espace de Hilbert  $H$  des formes différentielles de carré intégrable.

Considérons l'algèbre  $C(V)$  comme agissant par multiplication sur  $H$ . Remarquons tout de suite que, pour  $f \in C(V)$ , l'opérateur

$$[D, f] = Df - fD$$

est borné si et seulement si  $f$  est lipschitzienne.

De plus,  $\|[D, f]\|$  est égal à la constante de Lipschitz de  $f$ .

En effet, si  $f$  est de classe  $C^1$ ,  $[D, f]$  est l'opérateur de multiplication de Clifford par  $df$ .

À cet endroit, on peut noter que notre donnée nous a permis de retrouver complètement la métrique sur  $V$ , donc la structure riemannienne. En effet, la distance entre deux points vaut

$$d(a, b) = \sup\{|f(a) - f(b)|, f \in C(X); \|[D, f]\| \leq 1\}.$$

On retrouve aussi facilement la structure  $C^\infty$  de  $V$ , puisqu'une fonction  $f \in C(V)$  est de classe  $C^\infty$  si et seulement si elle est dans le domaine  $C^\infty$  de la dérivation  $\delta : f \mapsto [|D|, f]$ , c'est à dire, pour tout  $n$ , dans le domaine de la composée  $n$ -ième  $\delta^{\circ n}$  de  $\delta$  avec elle même. Ici  $|D|$  désigne le module de  $D$ , c'est à dire l'opérateur positif tel que  $|D|^2 = D^*D = D^2$ . En effet,  $|D|$  est un opérateur pseudodifférentiel dont le symbole principal est scalaire (en un vecteur cotangent  $\xi$  c'est la multiplication par  $\|\xi\|$ ). Le commutateur de  $|D|$  avec un opérateur pseudodifférentiel d'ordre 0 est pseudodifférentiel d'ordre 0, et est donc borné.

Remarquons que notre triplet spectral nous a permis de retrouver une algèbre d'opérateurs pseudodifférentiels d'ordre 0! Notons que les opérateurs obtenus ainsi à partir de  $C^\infty(V)$  par commutateur avec  $|D|$  ont un symbole principal scalaire (ils sont même scalaires dans le cas plat). Si on veut obtenir des opérateurs pseudodifférentiels d'ordre 0 opérant sur le fibré des formes, il suffit de considérer la plus petite sous algèbre d'opérateurs sur  $H$  contenant  $C^\infty(V)$ , les commutateurs  $[D, f]$  pour  $f \in C^\infty(V)$  et stable par commutateur avec  $|D|$ . Notons-la  $\mathcal{P}_0$ . On retrouve aussitôt les opérateurs pseudodifférentiels d'ordre  $m$  (complexe) : ce sont les opérateurs de la forme  $P(D^2 + 1)^{m/2}$ , où  $P \in \mathcal{P}_0$ .

Nous allons à présent rappeler un outil très puissant et que nous n'aurons aucun mal à définir juste en termes de notre triplet spectral : *le résidu non commutatif, ou résidu de Wodzicki*.

Le résidu d'un opérateur pseudodifférentiel  $P$  est donné par une « formule locale » :

$$\text{res } P = (2\pi)^{-\dim V} \int_V s_P$$

où  $s_P$  est une densité sur  $V$  qui se calcule à l'aide du symbole (total) de  $P$  : pour  $x \in V$ ,  $s_P(x)$  est la moyenne sur la sphère de l'espace cotangent en  $x$  du symbole d'ordre  $-\dim(V)$  de  $P$  (dans n'importe quelle carte de  $V$ ). Ce résidu admet de très nombreuses interprétations. Pour nous, la plus pratique à utiliser est la suivante : notons  $\text{Tr}$  la trace définie sur l'idéal des opérateurs à trace sur  $H$ . La fonction

$$z \mapsto \text{Tr}(P(D^2 + 1)^{-z/2})$$

définie pour  $\Re(z)$  assez grande ( $\Re(z) > \dim(V) + m$  où  $m$  est – la partie réelle de – l'ordre de  $P$ ), admet un prolongement méromorphe sur tout  $\mathbf{C}$ , avec des pôles simples. Alors  $\text{res}(P)$  est le résidu en 0 de cette fonction. En particulier, le résidu de Wodzicki s'interprète uniquement en termes de notre triplet spectral. De plus, ce résidu est une trace : si  $P, Q$  sont des opérateurs pseudodifférentiels, on a  $\text{res } PQ = \text{res } QP$ . C'est d'ailleurs l'unique trace sur l'algèbre des opérateurs pseudodifférentiels sur  $V$ .

À l'aide du résidu de Wodzicki, on peut à présent retrouver le cycle fondamental sur  $V$ , c'est-à-dire l'intégrale sur  $V$  des formes différentielles de plus haut degré. On supposera que la dimension  $n$  de  $V$  est un multiple de 4. Dans ce cas, le fibré des formes différentielles est somme directe orthogonale de deux sous fibrés  $E_+ \oplus E_-$  (les espaces propres de l'opérateur  $*$  de Hodge) et l'opérateur de signature est impair pour cette décomposition (il envoie les sections de  $E_+$  dans celles de  $E_-$  et inversement). On notera  $\varepsilon$  l'opérateur de graduation défini par  $\varepsilon(\xi_+ + \xi_-) = \xi_+ - \xi_-$ , où  $\xi_{\pm}$  est une section de  $E_{\pm}$ . Si  $f_0, f_1, \dots, f_n \in C^\infty(V)$ , on a

$$\int_V f_0 df_1 \dots df_n = \pi^n \text{res}(\varepsilon f_0 [D, f_1] \dots [D, f_n] (D^2 + 1)^{-n/2})$$

où  $\varepsilon$  est l'opérateur de graduation.

L'opérateur  $\varepsilon f_0 [D, f_1] \dots [D, f_n] (D^2 + 1)^{-n/2}$  apparaissant dans cette formule est d'ordre  $-n$ . Le résidu de Wodzicki de ces opérateurs peut être aussi interprété comme une *trace de Dixmier* qui est une trace positive définie sur un idéal légèrement plus gros que l'idéal des opérateurs à trace.

### Les axiomes d'une géométrie non commutative

La discussion du cas commutatif nous amène à préciser les conditions que l'on va mettre sur notre triplet spectral.

a) L'ensemble des  $f \in A$  tels que  $[D, f]$  soit borné est dense dans  $A$ . Comme la résolvante de  $D$  est compacte, cette condition est une version non bornée, due à Baaj-Julg de la théorie de Kasparov. On dit que le triplet  $(H, A, D)$  est *module de Fredholm non borné*.

Un tel module définit un *indice analytique* qui est un morphisme de la  $K$ -théorie de  $A$  vers  $\mathbf{Z}$ . Un des problèmes naturels est alors de calculer cet homomorphisme.

b) La résolvante de  $D$  est dans une classe de Schatten  $C^p$ , *i.e.*  $(D^2 + 1)^{-p/2}$  est un opérateur à trace. On dit que le triplet  $(H, A, D)$  est *p-sommable*. Dans ce cas la *dimension* de  $(H, A, D)$  est égale à  $\inf\{p; (D^2 + 1)^{-1/2} \in C_p\}$ . Une condition beaucoup plus faible est de dire que  $\exp(-sD^2)$  est à trace pour  $s > 0$ . Dans ce cas on dit que  $(H, A, D)$  est  *$\theta$ -sommable*.

On peut dans ces deux cas écrire une *formule d'indice* : on peut à l'aide de la trace des opérateurs écrire un cocycle cyclique sur l'algèbre  $\{a \in A; [D, a] \text{ est borné}\}$  qui va jouer le rôle de la classe d'indice dans la formule d'Atiyah-Singer.

- c) On peut faire des hypothèses plus contraignantes, en supposant que
- $(H, A, D)$  est *p-sommable* ;
  - les éléments  $C^\infty$  pour la dérivation  $\delta : f \mapsto [[D], f]$  forment une sous-algèbre  $\mathcal{A}$  dense dans  $A$  ;
  - pour  $P$  dans la plus petite sous-algèbre de  $\mathcal{L}(H)$  contenant  $\mathcal{A}$ , les commutateurs  $[D, f]$  pour  $f \in \mathcal{A}$  et stable par  $\delta$ , la fonction  $z \mapsto \text{Tr}(P(D^2 + 1)^{-z/2})$  définie pour  $\Re(z)$  assez grande, admet un prolongement méromorphe sur tout  $\mathbf{C}$ , avec des pôles simples.

Dans ce cas, on pourra écrire une formule de l'indice en termes de résidus de prolongements méromorphes de fonctions de la forme

$$z \mapsto \text{Tr}(P(D^2 + 1)^{-z/2}) ;$$

comme cette formule est uniquement basée sur des résidus, elle est plus «robuste» : elle ne change pas quand on modifie  $D$  par un opérateur de rang fini. Dans le cas d'un opérateur (pseudo-)différentiel  $D$  sur une variété, cette formule ne dépend que du symbole total de  $D$ . Pour cela on dit que cette formule d'indice est *locale*.

d) Dans certains cas, on pourra exprimer le fait que l'opérateur  $D$  est *différentiel d'ordre 1*. Cela s'exprimera en disant que  $[D, f]$  est *local*. En géométrie «commutative», cette localité s'exprime en disant que  $[D, f]$  commute aux multiplications par les fonctions ; mais évidemment, dans le cadre non commutatif, ce n'est pas la bonne définition : les éléments de  $\mathcal{A}$  elle même doivent être locaux. Inspiré par la théorie de Tomita, Connes propose un analogue non commutatif à la localité : on suppose donné un opérateur antilinéaire  $J : H \rightarrow H$  tel que  $J^2 = \pm \text{id}$  et  $JAJ^{-1}$  et  $\mathcal{A}$  commutent. On dit alors que  $T \in \mathcal{L}(H)$  est local si  $T$  commute à  $JAJ^{-1}$ . Dans le cas commutatif où  $H$  est l'espace des sections  $L^2$

d'un fibré  $S$  sur une variété  $V$ ,  $J$  est juste une structure réelle sur  $S$  et  $JAJ^{-1} = A$ .

*Nous terminons en discutant trois exemples non commutatifs.*

1. Le cas d'un groupe  $\Gamma$  de type fini.

On peut prendre  $H = \ell^2(\Gamma)$  dans lequel  $A = C_r^*(\Gamma)$  opère par translations; l'opérateur  $|D|$  est l'opérateur  $\xi \mapsto \ell\xi$ , où  $\ell : \Gamma \rightarrow \mathbf{R}_+$  est une fonction longueur, *i.e.* satisfait  $\ell(gh) \leq \ell(g) + \ell(h)$ .

Remarquons que  $u_g^{-1}|D|u_g - |D|$  est un opérateur de multiplication continu et sa norme est égale à  $\ell(g)$ ; donc

$$[|D|, u_g] = u_g \left( u_g^{-1}|D|u_g - |D| \right)$$

est aussi continu. Notons que  $(H, A, |D|)$  est  $p$ -sommable si et seulement si le groupe  $\Gamma$  est à croissance polynomiale (pour la longueur  $\ell$ ), ce qui implique que  $\Gamma$  est presque nilpotent. Par contre, lorsque  $\ell$  est la longueur des mots, ce module est toujours  $\theta$ -sommable.

On n'a construit que le module  $|D|$  de  $D$ . Celui-ci donne des informations métriques, mais il manque la *phase* de  $D$  qui est la seule qui compte pour l'indice. Celle-ci pourra être construite dans certains cas. Par exemple cette construction peut se faire si le groupe  $\Gamma$  opère sur un arbre, ou sur un immeuble de Bruhat-Tits.

2. L'opérateur de signature transverse sur un feuilletage.

C'est un cas étudié par Connes en collaboration avec Moscovici dans toute une série d'articles. On va en fait se placer dans le cas légèrement plus simple d'un groupe dénombrable  $\Gamma$  de difféomorphismes d'une variété  $M$  de classe  $C^\infty$  de dimension  $n$ . Si l'on veut construire un opérateur de signature dans ce cadre, le premier problème que l'on rencontre est que, dans le cas général, il n'y a pas de métrique sur  $M$  invariante par  $\Gamma$ , donc on ne peut pas construire un opérateur différentiel elliptique dont le symbole principal soit invariant par  $\Gamma$ . Pour cela, Connes et Moscovici se placent dans l'espace  $P$  des métriques sur  $M$ , c'est-à-dire l'ensemble des repères du fibré tangent, quotienté par l'action de  $O(n)$ . On construit alors un opérateur pseudodifférentiel  $D$  *hypoelliptique* qui est «presque invariant» par *tous les difféomorphismes* de  $M$ .

Cet opérateur se décrit en écrivant une formule  $D|D| = Q$ ,

$$Q = d_V^* d_V - d_V d_V^* + d_t + d_t^*$$

où  $d_V$  est un opérateur de différentiation «vertical» *i.e.* le long de la fibre de la fibration  $P \rightarrow M$  et  $d_t$  est un opérateur de différentiation «transverse» à cette fibration.

On peut démontrer que le triplet  $(H, A, D)$  ainsi obtenu satisfait toutes les conditions c) ci-dessus. On peut donc donner une formule locale de l'indice. Pour faciliter le calcul de ce cocycle, Connes et Moscovici introduisent de plus une algèbre de Hopf  $\mathcal{H}_n$  non commutative et non cocommutative de « champs de vecteurs transverses » sur  $\mathbf{R}^n$  qui joue le rôle de « groupe quantique de symétries » de la situation. Signalons qu'une algèbre de Hopf analogue est aussi utilisée par Connes et Kreimer afin d'organiser les calculs dans la théorie de la renormalisation.

### 3. Le cas du tore non commutatif.

Dans ce cas, tous les calculs sont complètement explicites : l'espace de Hilbert que l'on va prendre s'écrit

$$H = \ell^2(\mathbf{Z}^2) \oplus \ell^2(\mathbf{Z}^2).$$

L'algèbre  $A$  engendrée par des opérateurs unitaires  $u, v$  tels que  $vu = e^{2i\pi\theta}uv$  opère sur chacune des composantes  $\ell^2(\mathbf{Z}^2)$  par les mêmes formules :

$$u(E_{n,m}) = E_{n+1,m} \text{ et } v(E_{n,m}) = e^{2ni\pi\theta} E_{n,m+1},$$

où l'on a noté  $(E_{n,m})_{n,m \in \mathbf{Z}}$  la base hilbertienne canonique de  $\ell^2(\mathbf{Z}^2)$ . L'opérateur  $D$  s'écrit :

$$D = \begin{pmatrix} 0 & \partial^* \\ \partial & 0 \end{pmatrix}$$

où  $\partial$  est l'opérateur donné par  $\partial(E_{n,m}) = (n + im)E_{n,m}$ .

On dispose aussi ici de l'opérateur antilinéaire  $J$  qui opère sur chaque composante  $\ell^2(\mathbf{Z}^2)$  par la formule  $JE_{n,m} = e^{2nm i \pi \theta} E_{-n,-m}$ . L'opérateur  $D$  est alors différentiel au sens de la condition d) ci-dessus.

Cet exemple a donné lieu à des calculs très jolis, et a servi de laboratoire pour de nombreux outils de la théorie. Certains d'entre eux se sont révélés assez fins pour avoir un comportement dépendant des propriétés diophantiennes du nombre irrationnel  $\theta$ .

De nombreux autres exemples naturels ont été – et sont étudiés. On n'est certainement qu'au début de l'histoire...

*George Skandalis*

Université Paris VII

Institut de Mathématiques de Jussieu