Variations autour du théorème de récurrence de Poincaré

par

Étienne GHYS

1 Introduction

Henri Poincaré est le fondateur de la théorie des systèmes dynamiques[1]. Confronté à l'impossibilité de résoudre explicitement les équations différentielles gouvernant les trajectoires des planètes (dès qu'elles sont en nombre supérieur ou égal à trois), il développe un ambitieux programme qui cherche à décrire qualitativement le mouvement des corps célestes. Dans son fameux mémoire de 1890 *« Sur le problème des trois corps et les équations de la dynamique »*[2] [14], il démontre un théorème extrêmement surprenant. Nous en donnerons un énoncé précis plus loin mais il est préférable de citer directement l'analyse que H. Poincaré a faite de ses propres travaux [14] :

« Je n'ai pu résoudre rigoureusement et complètement le problème de la stabilité du système solaire, en entendant ce mot dans un sens strictement mathématique. L'emploi des invariants intégraux m'a cependant permis d'atteindre certains résultats partiels, s'appliquant surtout au problème dit restreint où les deux corps principaux circulent dans des orbites sans excentricité, pendant que le corps troublé a une masse négligeable. Dans ce cas, si on laisse de côté certaines trajectoires exceptionnelles, dont la réalisation est infiniment peu probable, on peut démontrer que **le système repassera une infinité de fois aussi près que l'on voudra de sa position initiale.** *C'est ce que j'ai appelé la stabilité à la Poisson ».*

Deux articles de vulgarisation publiés dans *Pour la Science* et *Science et Vie* décrivent ce théorème par un exemple où l'on *voit* une récurrence assez stupéfiante [3, 5]. Partant d'une reproduction d'une photographie de H. Poincaré, on lui applique une certaine transformation et on itère le procédé. Dès la troisième itération, il ne reste plus grand chose du visage du grand homme mais, de manière miraculeuse, après 241 itérations, Henri Poincaré est de retour sans qu'il ne lui manque un seul poil de barbe ! Nous avons reproduit le résultat à la fin de cet article.

Nous allons essayer d'expliquer ici pourquoi cet exemple, même s'il est frappant, n'illustre *en aucun cas* le théorème de Poincaré ! Ce phénomène est en fait le résultat d'une série de petits « miracles » de nature arithmétique que nous analyserons.

[1] Entre autres...

[2] Couronné par le prix de S.M. le roi Oscar II de Suède.

Nous espérons qu'au passage ceci permettra une meilleure compréhension du *vrai* théorème de Poincaré et de ses limitations. En passant, nous rencontrerons quelques questions ouvertes auxquelles certains lecteurs auront peut-être le plaisir de s'attaquer.

Ce chapitre est une version très légèrement modifiée d'un article paru dans le premier numéro du *Journal de Maths des élèves de l'ENS Lyon* (1994).

Remerciements. Je suis heureux de remercier Christophe Bavard, Patrick Iglesias, Bruno Sévennec et ma fille Élise pour leur aide précieuse dans la préparation de ce texte.

2 Le théorème de récurrence de Poincaré

Nous nous contenterons en fait d'un cas très particulier du théorème qui suffira à nos besoins. Soit C le carré $[0,1]\times[0,1]$ (qui sera bientôt l'écran d'un ordinateur...). En recollant les côtés opposés de C, on obtient un tore T. Autrement dit, T est obtenu à partir de C en identifiant pour chaque t de $[0,1]$, les points $(0,t)$ et $(1,t)$ ainsi que $(t,0)$ et $(t,1)$. On peut aussi considérer T comme le quotient du plan $\mathbf{R}^2$ par le réseau $\mathbf{Z}^2$ des points entiers, c'est-à-dire où l'on identifie les points (x,y) et (x_0,y_0) si leur différence est à coordonnées entières. On fait naturellement de T un espace métrique en définissant la distance entre deux points comme le minimum des distances entre les divers points de $\mathbf{R}^2$ qui les représentent.

Soit $F:\mathbf{R}^2\to\mathbf{R}^2$ un homéomorphisme qui respecte l'aire, c'est-à-dire tel que pour tout domaine $\Omega\subset\mathbf{R}^2$, l'aire de Ω est égale à celle de $F(\Omega)$. Si F est un difféomorphisme, cela revient bien sûr à dire que le déterminant de la matrice jacobienne de F est égal à ±1 en chaque point. On suppose de plus que F passe au quotient en un homéomorphisme de T. Autrement dit, F et son inverse envoient des points de $\mathbf{R}^2$ qui diffèrent entre eux d'un élément du réseau $\mathbf{Z}^2$ sur des points qui diffèrent également d'un élément de ce réseau. On obtient ainsi un homéomorphisme f du tore T qui respecte l'aire dans un sens à peu près évident. Si k est un entier positif, nous noterons f^k la composition $f\circ\cdots\circ f$ de k fois l'homéomorphisme f. Si a est un point de T, son *orbite* par f est la suite $(a_k)_{k\geqslant0}$ définie par $a_k=f^k(a)$. Étudier la dynamique de f, c'est décrire le comportement asymptotique de ces orbites lorsque le *temps* k tend vers l'infini. On dit qu'un point a est *récurrent* si c'est un point d'accumulation de son orbite.

Le théorème suivant est une version du théorème de récurrence de Poincaré (1890) :

Théorème. *L'ensemble des points récurrents d'un homéomorphisme du tore qui respecte l'aire est dense dans le tore.*

Démonstration. Si n est un entier positif, nous conviendrons de dire qu'un point

a est $1/n$-récurrent s'il existe un entier k strictement positif tel que la distance (dans T) entre a et $f^k(a)$ est strictement inférieure à $1/n$. L'ensemble des points $1/n$-récurrents est un ouvert R_n de T et l'intersection de tous les R_n est l'ensemble des points récurrents de f. D'après le théorème de Baire, il suffit donc de montrer que chaque R_n est un ouvert dense. L'idée de la preuve est très simple. Soit Ω une boule ouverte de T de rayon inférieur à $1/(2n)$ et considérons la suite d'ouverts $f^k(\Omega)$ avec $k \geqslant 0$. Tous ont la même aire et la finitude de l'aire totale de T entraîne qu'ils ne peuvent être deux à deux disjoints. Il existe donc deux entiers k_1 et k_2 avec $0 \leqslant k_1 < k_2$ tels que $f^{k_1}(\Omega)$ et $f^{k_2}(\Omega)$ ne sont pas disjoints. Si on pose $k = k_2 - k_1$, on a donc $k > 0$ et $\Omega \cap f^k(\Omega)$ est non vide. Mais ceci signifie précisément que chacune de ces boules Ω contient au moins un point $1/n$-récurrent et donc que R_n est dense dans T. Ceci établit le théorème.

Quelques remarques s'imposent :

— Nous avons utilisé le théorème de Baire postérieur d'une dizaine d'années à celui de Poincaré ! Nous suggérons au lecteur de lire les articles de H. Poincaré pour y déceler les énoncés originaux du théorème [11, 12, 13, 14].

— Il serait facile de montrer que l'ensemble des points qui ne sont pas récurrents est de mesure de Lebesgue nulle (voir par exemple [9]). H. Poincaré n'avait pas à sa disposition la théorie générale de la mesure mais il avait les idées claires ! Il écrit dans [11] :

« On peut dire que les [trajectoires non récurrentes] sont l'exception et que les [trajectoires récurrentes] sont la règle au même titre que les nombres rationnels sont l'exception et les nombres incommensurables sont la règle. Je démontre en effet que la probabilité pour que les conditions initiales du mouvement soient celles qui correspondent à une solution instable [non récurrente], que cette probabilité, dis-je, est nulle. Ce mot n'a par lui même aucun sens : j'en donne dans mon Mémoire une définition précise. »

— Le fait que f soit un homéomorphisme du tore n'a bien entendu aucune importance. En général, on dispose d'un espace X qui peut être l'espace des phases d'un système mécanique et d'un homéomorphisme f de X qui envoie chaque position initiale sur la position une seconde plus tard par exemple. La mécanique classique nous enseigne que dans de nombreux cas X est une *variété symplectique* mais nous n'en retiendrons que le fait qu'il existe une notion de volume sur X et que f préserve ce volume (théorème de Liouville). Le théorème de Poincaré se généralise dans ce nouveau contexte pour peu que l'hypothèse cruciale (mais assez générale) soit vérifiée : la finitude du volume total de X. Pour en savoir plus, on consultera, par exemple, [1].

3 L'exemple de Pour la Science et Science et Vie

Soit Φ l'application linéaire de $\mathbf{R}^2$ de matrice :

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

C'est un difféomorphisme qui respecte l'aire puisque le déterminant de cette matrice est -1. D'autre part, le fait que les coefficients de Φ et de son inverse sont entiers montre que Φ envoie bijectivement le réseau des points entiers sur lui même. Ainsi, Φ définit par passage au quotient un difféomorphisme du tore T qui respecte l'aire, que nous noterons encore Φ, sans grand danger de confusion. Cet exemple est d'une grande importance dans la théorie des systèmes dynamiques, en dépit de la grande simplicité de sa définition. Dans un certain sens, c'est beaucoup plus qu'un exemple.

Théorème (Anosov 1967). *Soit Ψ un difféomorphisme de T proche de Φ (dans la topologie[3] C^1). Alors, il existe un homéomorphisme h du tore T tel que :*

$$\Psi = h \circ \Phi \circ h^{-1}.$$

On trouvera une démonstration dans [2]. Cela signifie que les difféomorphismes proches de Φ sont *les mêmes* que Φ, quitte à changer de coordonnées par un homéomorphisme. Si l'on comprend la structure de Φ, on comprend donc du même coup la structure d'un ouvert du groupe des difféomorphismes de T. C'est la fameuse *stabilité structurelle* qui a eu tant de développements ces 40 dernières années. Le lecteur aura d'ailleurs probablement deviné que le résultat est bien plus général que ce que nous avons énoncé ici ; en particulier il reste valable si l'on remplace Φ par une autre matrice 2×2, à coefficients entiers et de déterminant ± 1, pour peu qu'elle n'ait pas de valeur propre de module 1.

Appliquons le théorème de récurrence de Poincaré à Φ : presque tous les points de T sont récurrents. Dans les articles de *Pour la Science* et *Science et Vie*, on considère une reproduction du visage de Poincaré dans le carré $[0,1] \times [0,1]$ qui sert de base à la construction[4] du tore T puis on itère cette image par Φ.

Après 241 itérations, le miracle se produit : Poincaré est de retour ! Était-ce prévu par le théorème de récurrence ?

[3] Deux difféomorphismes f_1 et f_2 du tore sont C^1-proches s'ils proviennent de deux difféomorphismes F_1 et F_2 de $\mathbf{R}^2$ tels que $F_1 - F_2$ est petit ainsi que ses dérivées partielles du premier ordre.

[4] Dans l'exemple, l'origine des coordonnées est au centre de l'écran : le nez de Poincaré est un point fixe.

4 Pourquoi l'exemple est-il surprenant ?

C'est bien sûr la rapidité du retour de H. Poincaré qui est étonnante. Le théorème de récurrence ne précise pas la valeur probable du temps de retour mais un argument heuristique simple permet de l'estimer. Si Ω est un ouvert non vide de T, nous avons vu que l'argument essentiel de la preuve est que les ouverts $\Phi^k(\Omega)$ ne peuvent tous être disjoints. En fait, on ne peut placer dans T qu'un nombre inférieur à $\text{aire}(T)/\text{aire}(\Omega)$ d'ouverts disjoints dont l'aire est égale à $\text{aire}(\Omega)$. On est donc en droit d'espérer que le temps de retour est de l'ordre de $\text{aire}(T)/\text{aire}(\Omega)$. C'est en fait un théorème, sous une hypothèse technique, dite d'ergodicité, qui est satisfaite dans notre cas[5] :

Théorème (Kač 1947). *Soit f un homéomorphisme du tore T préservant l'aire et ergodique. Soit Ω un ouvert non vide et pour chaque point a de Ω, notons $u(a)$ le plus petit entier non nul k tel que $f^k(a)$ appartienne à Ω. Alors la valeur moyenne de u sur Ω est donnée par :*

$$\frac{1}{\text{aire}(\Omega)} \int\int_{\Omega} u(a)\, da = \frac{\text{aire}(T)}{\text{aire}(\Omega)}.$$

Appliquons ce théorème au visage de H. Poincaré. Bien sûr, il a fallu discrétiser l'image et la remplacer par un nombre fini de points (les pixels) dont on considère les orbites. Supposons donc que l'on remplace le carré par l'ensemble fini à N^2 éléments formé des points $(i/N, j/N)$ avec $1 \leqslant i \leqslant N$ et $1 \leqslant j \leqslant N$. Chaque pixel correspond en fait à un petit carré qui recouvre une proportion de $1/N^2$ du grand carré $[0,1] \times [0,1]$. D'après le théorème précédent, nous pouvons donc espérer qu'un pixel retournera à sa place après un nombre d'itérations de l'ordre de N^2. Si, pour fixer les idées, nous prenons une valeur de N égale à 1000, le temps de retour d'un pixel sera voisin d'un million. Voilà qui est singulièrement plus grand que 241 !

Ce n'est pas tout ! Si chaque pixel revient après à peu près un million d'itérations, les temps de retour varient probablement d'un pixel à l'autre. Le temps de retour de l'image complète est donc le P.P.C.M d'un million d'entiers qui sont tous à peu près de l'ordre du million. L'image devrait donc mettre très, très longtemps avant de revenir... Pour illustrer ce phénomène, nous allons citer quelques résultats combinatoires concernant les permutations d'un ensemble fini E_M à M éléments (où nous penserons plus tard que $M = N^2$). Il y a bien sûr $M!$ permutations d'un tel ensemble et il est bien connu que chaque permutation σ est un produit de cycles disjoints. Si a est un point de E_M, la période de a sous l'action de σ est la longueur du cycle qui contient a. La période de σ, c'est-à-dire son ordre dans le groupe symétrique, est le P.P.C.M. des longueurs des cycles qui la composent. On peut chercher à estimer les moyennes arithmétiques de ces quantités sur l'ensemble des $M!$ permutations de

[5] On dit qu'un homéomorphisme du tore est ergodique si tout ensemble borélien invariant est de mesure de Lebesgue nulle ou a un complémentaire de mesure nulle. Le lecteur courageux pourra montrer seul que Φ est ergodique ainsi que le théorème (en cas de panne, il pourra consulter [2, 10]).

E_M. Voici les résultats que l'on pourra consulter dans [4] (où on trouvera également beaucoup de références et de compléments).

THÉORÈME. *Lorsque M tend vers l'infini :*

1. La valeur moyenne du logarithme de l'ordre d'une permutation d'un ensemble à M éléments est équivalente à $\frac{1}{2}\ln^2 M$.

2. La valeur moyenne de la longueur du plus grand cycle d'une permutation d'un ensemble à M éléments est équivalente à $0,62432965...M$.

3. La valeur moyenne du nombre de cycles d'une permutation d'un ensemble à M éléments est équivalente à $\ln M$.

Lorsque M est égal à un million, le théorème précédent donne une valeur tellement grande pour la moyenne de l'ordre d'une permutation qu'on perd l'espoir de voir revenir H. Poincaré !

Mais il y a pire ! Lorsqu'on discrétise un homéomorphisme f sur un ensemble fini E_M à M éléments, on obtient une application f_M de E_M dans lui-même qui n'a aucune raison d'être une bijection. Deux pixels a et b peuvent être différents mais avoir des images par f suffisamment proches pour être identifiées dans E_M. Ainsi, l'ordinateur itère en fait une application non nécessairement bijective d'un ensemble fini dans lui-même.

Introduisons quelques notions élémentaires relatives à la structure d'une application f d'un ensemble fini E dans E. Pour chaque entier positif k, soit $E(k)$ l'image $f^k(E)$. Ceci définit une suite décroissante de parties de E, donc stationnaire. Notons R l'intersection des $E(k)$; c'est une partie invariante par f et la restriction de f à R est une bijection. Nous dirons que R est la *partie récurrente* de E. Le complémentaire de R dans E est la *partie errante*. Un point a de E est dans la partie récurrente ou errante suivant que l'orbite $f^k(a)$ repasse ou non par le point a. Nous conviendrons aussi de définir le *degré de récurrence* de f comme le rapport entre le cardinal de la partie récurrente et celui de E. On trouvera aussi le théorème suivant dans [4].

THÉORÈME. *Lorsque M tend vers l'infini :*

1. La moyenne du degré de récurrence parmi les M^M applications d'un ensemble à M éléments dans lui même est équivalente à $\sqrt{\pi/(2M)}$.

2. Le nombre moyen de cycles de la restriction à la partie récurrente est équivalent à $\ln M$.

En d'autres termes, une application *aléatoire* d'un ensemble à un million d'éléments a en moyenne une partie récurrente contenant à peine plus d'un millier d'éléments répartis en une dizaine de cycles. La grande majorité des points ne reviennent jamais à leur place lorsqu'on itère l'application. Encore une raison de plus pour ne pas croire au retour du visage de H. Poincaré...

5 Pourquoi l'exemple est très particulier

PREMIER MIRACLE. *L'ensemble fini E_{N^2} formé des N^2 points $(i/N, j/N)$ avec $1 \leqslant i \leqslant N$ et $1 \leqslant j \leqslant N$ sur lequel on discrétise est un ensemble invariant par la transformation Φ.*

C'est clair car l'application linéaire Φ préserve le réseau $\mathbf{Z}^2$ ainsi que tous les réseaux $\frac{1}{N}\mathbf{Z}^2$. La discrétisation de Φ est donc une bijection de E_{N^2} et nous avons déjà signalé que c'est une propriété très particulière. Si l'on conjugue Φ par un homéomorphisme du tore à peu près quelconque, le nouvel homéomorphisme ainsi obtenu ne préserve plus l'ensemble E_{N^2} et la discrétisation n'est plus une bijection.

DEUXIÈME MIRACLE. *La permutation induite par Φ sur l'ensemble E_{N^2} n'est pas du tout quelconque et son ordre est beaucoup plus petit que l'ordre auquel on pourrait s'attendre (à peu près 10^{41} pour $N^2 = 10^6$).*

Avant de justifier cette assertion, introduisons une notation. Si $\mathcal{A}$ est un anneau commutatif unitaire, nous noterons $\mathrm{GL}(2, \mathcal{A})$ le groupe des matrices 2×2 à coefficients dans $\mathcal{A}$ et de déterminant inversible. Ce groupe agit naturellement par applications « linéaires » sur $\mathcal{A} \times \mathcal{A}$. On peut en particulier considérer $\mathrm{GL}(2, \mathbf{Z})$ et $\mathrm{GL}(2, \mathbf{Z}/N\mathbf{Z})$. La réduction modulo N donne un homomorphisme

$$\rho_N : \mathrm{GL}(2, \mathbf{Z}) \to \mathrm{GL}(2, \mathbf{Z}/N\mathbf{Z}).$$

L'ensemble E_{N^2} de discrétisation peut bien sûr être identifié à $\mathbf{Z}/N\mathbf{Z} \times \mathbf{Z}/N\mathbf{Z}$ et l'action de Φ sur cet ensemble est simplement celle de l'élément $\rho_N(\Phi)$ sur $\mathbf{Z}/N\mathbf{Z} \times \mathbf{Z}/N\mathbf{Z}$ (nous identifions le difféomorphisme Φ et la matrice 2×2 qui le définit). L'ordre de la restriction de Φ à E_{N^2} est donc l'ordre de l'élément $\rho_N(\Phi)$ dans le groupe fini $\mathrm{GL}(2, \mathbf{Z}/N\mathbf{Z})$. On obtient donc une estimation, grossière mais efficace, de cet ordre : il est majoré par le cardinal de ce groupe fini qui est évidemment inférieur à N^4. Nous n'avons toujours pas compris pourquoi 241 est si petit mais nous avons maintenant une borne supérieure de l'ordre de 10^{12} qui est plus « raisonnable » que 10^{41}.

TROISIÈME MIRACLE. *L'ordre des éléments de $\mathrm{GL}(2, \mathbf{Z}/N\mathbf{Z})$ est en fait beaucoup plus petit que la borne précédente N^4.*

Pour simplifier, nous travaillerons en fait dans le sous-groupe $\mathrm{SL}(2, \mathbf{Z}/N\mathbf{Z})$ des matrices de déterminant 1. Remarquons que la matrice Φ n'est pas dans ce sous-groupe mais que son carré est bien sûr de déterminant 1. Le théorème suivant est dû à Dyson et Falk [6].

THÉORÈME. *L'ordre d'un élément de $\mathrm{SL}(2, \mathbf{Z}/N\mathbf{Z})$ est inférieur ou égal à $3N$.*

La preuve qui suit est peut-être un peu technique mais le lecteur effrayé pourra tout simplement l'ignorer sans que cela nuise à la compréhension de la suite.

DÉMONSTRATION. Soit A un élément du groupe $\mathrm{SL}(2, \mathbf{Z}/N\mathbf{Z})$. Nous allons distinguer plusieurs cas.

Premier cas. Supposons d'abord que N soit un nombre premier (que nous noterons bien sûr p). Les deux valeurs propres de A sont donc ou bien dans $\mathbf{Z}/p\mathbf{Z} = \mathbf{F}_p$ ou dans un corps[6] $\mathbf{F}_{p^2}$ qui est une extension quadratique de $\mathbf{F}_p$.

1. Supposons que A soit diagonalisable sur le corps fini $\mathbf{F}_p$ à p éléments. Puisque les deux valeurs propres de A sont inverses, l'ordre de l'élément A dans $\mathrm{SL}(2, \mathbf{F}_p)$ est alors égal à l'ordre de l'une des valeurs propres dans le groupe multiplicatif des éléments non nuls de $\mathbf{F}_p$. C'est un diviseur de $p-1$ et donc inférieur à $3p$.

2. Supposons maintenant que les valeurs propres de A soient non pas dans $\mathbf{F}_p$ mais dans $\mathbf{F}_{p^2}$. Les deux valeurs propres λ_1 et λ_2 de A sont alors échangées par l'automorphisme de Frobenius :

$$x \in \mathbf{F}_{p^2} \mapsto x^p \in \mathbf{F}_{p^2}.$$

On a donc $\lambda_2 = \lambda_1^p$ et $\lambda_1^{(p+1)} = 1$, puisque le déterminant de A est égal à 1. Il en résulte que l'ordre de A est un diviseur de $p+1$, donc en particulier inférieur à $3p$.

3. Si la matrice A n'est ni diagonalisable dans $\mathbf{F}_p$, ni dans $\mathbf{F}_{p^2}$, c'est que les deux valeurs propres de A sont égales et valent donc ± 1.

— Si la matrice A est unipotente, c'est-à-dire si ses deux valeurs propres sont égales à 1, alors elle est conjuguée à une matrice de la forme :

$$\begin{pmatrix} 1 & v \\ 0 & 1 \end{pmatrix}$$

avec v dans $\mathbf{F}_p$. L'ordre d'une telle matrice est évidemment 1 ou p et donc inférieur à $3p$.

— Si les deux valeurs propres de A sont égales à -1, alors $-A$ est unipotente et l'ordre de A est donc un diviseur de $2p$, donc inférieur à $3p$.

Deuxième cas. On suppose maintenant que N est une puissance p^n d'un nombre premier et nous allons démontrer le théorème par récurrence sur n. Le cas $n = 1$ vient d'être établi ci-dessus et nous supposons donc le théorème démontré jusqu'à n. Par réduction modulo p^n, on a un homomorphisme :

$$\rho : \mathrm{SL}(2, \mathbf{Z}/p^{n+1}\mathbf{Z}) \to \mathrm{SL}(2, \mathbf{Z}/p^n\mathbf{Z}).$$

Nous savons, par récurrence, que l'ordre d'un élément de $\mathrm{SL}(2, \mathbf{Z}/p^n\mathbf{Z})$ est inférieur à $3p^n$ et il suffit donc de montrer que l'ordre d'un élément du noyau de ρ est 1 ou p. Mais ceci est élémentaire car ce noyau est constitué de matrices de la forme : $\mathrm{Id} + p^n B$ de sorte que leur puissance p-ième est l'identité dans $\mathrm{SL}(2, \mathbf{Z}/p^{n+1}\mathbf{Z})$.

Troisième cas. Il reste à montrer que si le théorème est vrai pour les entiers $p_1^{n_1}, \ldots, p_\ell^{n_\ell}$ premiers entre eux, alors il est également vrai pour le produit $N =$

[6] En cas de problème, voir [15].

$p_1^{n_1} \cdots p_l^{n_\ell}$. En considérant les réductions modulo $p_1^{n_1}, \ldots, p_\ell^{n_\ell}$, on définit un homomorphisme de $\mathrm{SL}(2, \mathbf{Z}/N\mathbf{Z})$ sur le produit des $\mathrm{SL}(2, \mathbf{Z}/p_i^{n_i}\mathbf{Z})$ et le *lemme chinois* garantit qu'il s'agit d'un isomorphisme. L'ordre d'un élément de $\mathrm{SL}(2, \mathbf{Z}/N\mathbf{Z})$ est donc le P.P.C.M. des ordres des diverses composantes de son image dans les $\mathrm{SL}(2, \mathbf{Z}/p_i^{n_i}\mathbf{Z})$. Le deuxième cas nous a en fait montré que l'ordre d'un élément de $\mathrm{SL}(2, \mathbf{Z}/p^n\mathbf{Z})$ est de l'une des formes suivantes :

1. αp^β où α divise $p-1$ et $0 \leqslant \beta \leqslant n-1$;
2. αp^β où α divise $p+1$ et $0 \leqslant \beta \leqslant n-1$;
3. p^β où $\beta \leqslant n$;
4. $2p^\beta$ où $\beta \leqslant n$.

Si p est un nombre impair, $p+1$ est pair ! Si $p \neq 2$ cet ordre est donc inférieur ou égal à p^n ou est le double d'un entier inférieur ou égal à p^n. Il en résulte facilement que si N est impair, c'est-à-dire si les p_i sont tous différents de 2, le P.P.C.M. des divers ordres modulo les $p_i^{n_i}$ est inférieur ou égal à $2N$. Si $N = 2^n$, l'ordre est inférieur ou égal à $3 \cdot 2^{n-1}$, c'est-à-dire à $3N/2$.

Dans le cas général, N est le produit d'une puissance de 2 et d'un nombre impair de sorte que l'ordre modulo N est majoré par $((3/2) \times 2)N = 3N$ et le théorème est démontré.

Remarquons que la borne obtenue est optimale. On peut trouver par exemple un élément de $\mathrm{SL}(2, \mathbf{Z}/10\mathbf{Z})$ qui est d'ordre 3 modulo 2 et d'ordre $10 = 2 \times 5$ modulo 5 et donc d'ordre $30 = 3 \times 10$ modulo 10.

Remarque. Fixons une matrice A de $\mathrm{SL}(2, \mathbf{Z})$ et un nombre premier p. Il n'est pas difficile de s'assurer qu'il existe deux entiers α et β tels que, pour tout n *assez grand*, l'ordre de la projection de A dans $\mathrm{SL}(2, \mathbf{Z}/p^n\mathbf{Z})$ est exactement $\alpha \cdot p^{n-\beta}$. Ainsi, lorsque n tend vers l'infini, l'ordre de A modulo p^n est comparable à p^n. Pour la « majorité » des entiers N (non nécessairement puissances d'un nombre premier), on peut donc penser que l'ordre de A modulo N a le même ordre de grandeur que N. Nous laissons au lecteur le soin de donner un sens à cette assertion puis de la démontrer si elle s'avère exacte ! Quoi qu'il en soit, si $N = 1000$, nous avons maintenant une borne supérieure de 3000 pour l'ordre d'un élément de $\mathrm{SL}(2, \mathbf{Z}/N\mathbf{Z})$ et nous avons vu que dans de nombreux cas, cette borne est encore trop grande, de sorte que notre 241 devient enfin raisonnable !

Quatrième miracle. *Il existe une suite d'entiers $(\varphi_k)_{k \geqslant 0}$, tendant vers l'infini (exponentiellement) lorsque k tend vers l'infini, telle que si on discrétise l'écran en $\varphi_k \times \varphi_k$ points, alors le retour de H. Poincaré se produit* **exactement** *après $2k$ itérations...*

Bien sûr, choisir la discrétisation en fonction du temps de retour désiré est un peu une tricherie. Mais ceci montre encore mieux le caractère illusoire de ces récurrences. La qualité de ces discrétisations est excellente puisque nous verrons qu'on a, par exemple, pour un retour après 30, 34, 40, 106, 238, 240, 242 ou 246 itérations :

$\varphi_{15} = 1364$

$\varphi_{17} = 3571$

$\varphi_{20} = 15127$

$\varphi_{53} = 119218851371$

$\varphi_{119} = 74050703664649512645635 99$

$\varphi_{120} = 53583592549909666408718 40$

$\varphi_{121} = 19386725908489881939795601$

$\varphi_{123} = 50755107359004694554823204.$

Ainsi, en utilisant une (bonne) image constituée de 3571×3571 pixels, Poincaré revient après seulement 34 itérations ! Mais qui aurait l'idée d'utiliser précisément 3571 pixels[7] !

En revanche, si on choisit un entier n qui n'est pas de la forme φ_k, nous savons que le retour sera certes rapide (inférieur à $3n$) mais peut-être pas aussi rapide.

Pour justifier ces assertions, on introduit deux suites de Fibonacci a_k et b_k définies par :

$$a_0 = 0 \quad a_1 = 1 \quad a_{k+2} = a_{k+1} + a_k$$
$$b_0 = 2 \quad b_1 = 1 \quad b_{k+2} = b_{k+1} + b_k$$

pour $k \geqslant 0$, et on définit la suite φ_k par :

$$\varphi_{2k} = a_{2k} \qquad \varphi_{2k+1} = b_{2k+1}.$$

Bien sûr, φ_k tend vers l'infini exponentiellement lorsque k tend vers l'infini.

THÉORÈME. *La puissance $2k$-ième de la matrice Φ est congrue à l'identité modulo φ_k.*

DÉMONSTRATION. D'après le théorème de Hamilton- Cayley (dans le cas des matrices 2×2 !), on a :

$$\Phi^2 = \Phi + \mathrm{Id}.$$

Il en résulte que :

$$\Phi^{-2} = -\Phi^{-1} + \mathrm{Id}.$$

Par conséquent, pour tout entier k, on a :

$$\Phi^{k+2} = \Phi^{k+1} + \Phi^k$$

$$\Phi^{-(k+2)} = -\Phi^{-(k+1)} + \Phi^{-k}.$$

[7] Exercice : quand revient Poincaré avec une image 3570×3570 ? avec 3572×3572 ?

Pour chaque k, posons :

$$A_k = \Phi^k - (-1)^k \Phi^{-k} \qquad B_k = \Phi^k + (-1)^k \Phi^{-k}.$$

On a donc, pour tout entier k :

$$A_{k+2} = A_{k+1} + A_k \qquad B_{k+2} = B_{k+1} + B_k.$$

Par ailleurs, on calcule facilement :

$$A_0 = 0 \qquad A_1 = \Phi + \Phi^{-1}$$

$$B_0 = 2 \cdot \mathrm{Id} \qquad B_1 = \Phi - \Phi^{-1} = \mathrm{Id}.$$

On obtient donc par récurrence l'expression suivante pour A_k et B_k :

$$A_k = a_k \cdot (\Phi + \Phi^{-1}) \qquad B_k = b_k \cdot \mathrm{Id}.$$

Finalement :

$$\Phi^{4k} - \mathrm{Id} = (\Phi^{2k} - \Phi^{-2k})\Phi^{2k} = a_{2k} \cdot (\Phi + \Phi^{-1})\Phi^{2k}$$

$$\Phi^{4k+2} - \mathrm{Id} = (\Phi^{2k+1} - \Phi^{-2k-1})\Phi^{2k+1} = b_{2k+1} \cdot \Phi^{2k+1}.$$

Nous avons bien montré que $\Phi^{2k} - \mathrm{Id}$ est divisible par φ_k.

Remarque. Les puissances impaires de Φ ne présentent pas ce phénomène de haute récurrence que nous avons rencontré pour les puissances paires. La matrice Φ, étant de déterminant -1, renverse l'orientation[8]. Il est donc nécessaire d'élever Φ à une puissance paire pour obtenir un retour orienté ! Plus précisément, si la matrice entière Φ^{2k+1} est égale à Id modulo un certain entier l, en comparant les déterminants, on obtient que l est égal à ± 1 ou ± 2. C'est pour cette raison que nous pensons que la récurrence présentée dans *Pour la Science* et *Science et Vie* ne se produit pas après 241 itérations et qu'il y a probablement eu une erreur d'une unité dans le décompte des itérations (la première figure étant l'itération d'ordre 0). *La récurrence se produit certainement à la 240ème itération !*

Il reste à comprendre la valeur 240 même s'il est maintenant clair que cette valeur est nécessairement artificielle. Une explication possible vient de la constatation suivante. Lorsqu'on décompose les entiers φ_k en facteurs premiers (grâce à Maple), on remarque que les nombres premiers qui interviennent sont presque tous extrêmement grands, avec l'exception notable de φ_{120}. En reprenant les quelques exemples choisis plus haut, on a par exemple :

$\varphi_{53} = 119218851371$

$\varphi_{119} = 29 \times 239 \times 10711 \times 3571 \times 27932732439809$

[8]Sur la photographie initiale, on peut voir l'oreille gauche du Maître alors que sur sa transformée par Φ, c'est une oreille droite que l'on distingue, même si elle est déformée.

$\varphi_{120} = 2^5 \times 3^2 \times 5 \times 7 \times 11 \times 23 \times 31 \times 41 \times 61 \times 241 \times 2161 \times 2521 \times 20641$

$\varphi_{121} = 199 \times 97420733208491869044199$

$\varphi_{123} = 2^2 \times 4767481 \times 370248451 \times 7188487771.$

Les constructeurs d'ordinateurs ont naturellement tendance à choisir les tailles de leurs écrans parmi les entiers qui sont des produits de petits entiers tels que 2, 3 ou 5 et il semble que ce soit finalement cette propriété de φ_{120} qui est à l'origine du retour après 240 itérations... Ce n'est d'ailleurs pas une surprise. En effet, le polynôme $X^{2k} - 1$ est le produit des polynômes cyclotomiques indexés par les diviseurs de $2k$ de sorte que si $2k$ a beaucoup de diviseurs (comme 120), alors $A^{2k} - \mathrm{Id}$ a également beaucoup de diviseurs.

En résumé, le retour après 241 itérations se passe en fait après 240 itérations et la raison de ce retour n'a pas grand-chose à voir avec le théorème de récurrence mais plutôt avec le fait que 120 est un entier qui a beaucoup de diviseurs !

Nous pouvons même essayer de deviner le nombre n de pixels utilisés dans les articles de *Pour la Science* et *Science et Vie*. Il s'agit d'un diviseur de φ_{120} qui n'est probablement divisible que par $2, 3$ et 5. S'agit-il de 160, 480 ou de 1440 ?

Exercice 1 : Si l'on examine avec attention la reproduction jointe à la fin de ce chapitre, on constate un phénomène bizarre : après 48 itérations on voit apparaître 5 visages de H. Poincaré décalés les uns par rapport aux autres. Nous laissons au lecteur le plaisir de trouver l'explication. Nous nous contenterons de remarquer que :

$$240 = 5 \times 48.$$

$$\varphi_{24} = 46368 = 2^5 \times 3^2 \times 7 \times 23$$

(ainsi 5 divise φ_{120} mais pas φ_{24}). Le discriminant du polynôme $X^2 - X - 1$ est 5 de sorte que la réduction modulo 5 de Φ a une valeur propre double (et 5 est le seul nombre premier ayant cette propriété).

Exercice 2 : Comment pourrait-on fabriquer une image de Poincaré qui soit telle qu'après 241 itérations, le visage de Newton apparaisse ! ?

6 Une question

L'espace de tous les homéomorphismes du tore qui respectent l'aire peut être muni (par exemple) de la topologie de la convergence uniforme. Nous dirons qu'une propriété d'un homéomorphisme est générique si l'ensemble des homéomorphismes qui la satisfont est un ensemble résiduel au sens de Baire (i.e. une intersection dénombrable d'ouverts denses). Le problème que nous voudrions soumettre au lecteur est celui de savoir dans quelle mesure un ordinateur est capable de rendre compte de la dynamique générique d'un homéomorphisme. Précisons la question. Si N est

un entier positif, on note toujours E_{N^2} l'ensemble des points du tore de coordonnées $(i/N, j/N)$ avec $1 \leqslant i \leqslant N$ et $1 \leqslant j \leqslant N$. Soit f un homéomorphisme du tore qui préserve l'aire. Soit : $f_N : E_{N^2} \to E_{N^2}$ la discrétisation d'ordre N, c'est-à-dire l'application qui envoie un point de E_{N^2} sur le point de E_{N^2} le plus proche de son image par f (génériquement unique). Soit $r_N(f)$ le degré de récurrence de f_N.

PROBLÈME. *Est-il possible de décrire le comportement asymptotique de la suite $r_N(f)$ lorsque N tend vers l'infini pour un homéomorphisme générique du tore qui respecte l'aire ?*

Bien sûr, la discrétisation d'un homéomorphisme générique n'est pas une application quelconque d'un ensemble fini à N^2 éléments dans lui même : la continuité de f force une espèce de continuité faible pour f_N sur l'ensemble fini E_{N^2}. Il n'est donc pas clair que l'estimation du degré de récurrence que nous avons décrite plus haut, en $\sqrt{\pi/2}/N$, soit valable pour $r_N(f)$. Si cette estimation (ou une autre un peu moins bonne) était tout de même valable pour un homéomorphisme générique, on pourrait se poser des questions sur l'usage de l'informatique dans la théorie des systèmes dynamiques...

On trouvera dans [7] une discussion intéressante de ce genre de questions pour des systèmes dynamique *non inversibles* (ainsi qu'une bibliographie complémentaire). La taille des cycles des discrétisations des difféomorphismes génériques du cercle est discutée dans [8].

7 Le mélange

Pour terminer cet article, nous voudrions citer un résultat qui porte le coup de grâce à l'espoir de déceler une récurrence dans les figures (voir [10] pour plus d'informations). Alors que presque tous les points sont récurrents, les figures ont par contre une tendance à se mélanger :

THÉORÈME. *Soient Ω_1 et Ω_2 deux ensembles boréliens du tore T. Alors l'aire de l'intersection $\Phi^k(\Omega_1) \cap \Omega_2$ tend vers le produit des aires de Ω_1 et de Ω_2 lorsque l'entier k tend vers l'infini.*

DÉMONSTRATION. Soient u_1 et u_2 les fonctions indicatrices de Ω_1 et Ω_2 respectivement. Il s'agit de montrer que :

$$\lim_{k\to+\infty} \iint_T u_1 \circ f^{-k}(x,y) \cdot u_2(x,y)\, dxdy = \left(\iint_T u_1(x,y)\, dxdy\right) \left(\iint_T u_2(x,y)\, dxdy\right).$$

A fortiori, il suffit de le démontrer pour tous les couples (u_1, u_2) de fonctions de carré intégrable sur T. En développant u_1 et u_2 en séries de Fourier, on se ramène au cas où u_1 et u_2 sont de la forme :

$$u_1(x,y) = \exp 2i\pi(m_1 x + n_1 y) \qquad u_2(x,y) = \exp 2i\pi(m_2 x + n_2 y)$$

où x et y désignent des éléments de $\mathbf{R}/\mathbf{Z}$ et où m_1, m_2, n_1, n_2 sont des entiers. Lorsque l'on évalue $u_1 \circ \Phi^{-k}$, on trouve :

$$u_1 \circ \Phi^{-1}(x, y) = \exp 2i\pi(m(k)x + n(k)y)$$

avec :

$$\begin{pmatrix} m(k) \\ n(k) \end{pmatrix} = {}^t\Phi^{-k} \begin{pmatrix} m_1 \\ n_1 \end{pmatrix}.$$

Si (m_1, n_1) ou (m_2, n_2) est égal à $(0, 0)$, alors le produit des intégrales de $u_1 \circ \Phi^{-k}$ et de u_2 est bien sûr constant et la convergence de ce produit n'est pas trop difficile...

Si (m_1, n_1) et (m_2, n_2) sont différents de $(0, 0)$, on vérifie facilement que, pour k assez grand, $(m(k), n(k)) \neq (m_2, n_2)$ de sorte que $u_1 \circ \Phi^{-k}$ et u_2 sont orthogonaux pour le produit hermitien de l'espace de Hilbert des fonctions de carré intégrable sur T et, bien entendu, chacune de ces deux fonctions est d'intégrale nulle. Ici encore, la convergence est facile... Ceci établit le théorème.

Le théorème signifie que si l'on itère un petit domaine Ω_1 par Φ, il va s'éparpiller dans tout le tore d'une manière uniforme : asymptotiquement, la proportion de $\Phi^k(\Omega_1)$ dans Ω_2 est la même que celle de Ω_1 dans T. Tout se brouille et s'estompe...

« Avec le temps...

Avec le temps, va, tout s'en va

On oublie le visage et l'on oublie la voix

Le cœur quand ça bat plus, c'est pas la peine d'aller

Chercher plus loin, faut laisser faire et c'est très bien

Avec le temps...

Avec le temps, va, tout s'en va

L'autre qu'on adorait, qu'on cherchait sous la pluie

L'autre qu'on devinait au détour d'un regard

Entre les mots, entre les lignes et sous le fard

D'un serment maquillé qui s'en va faire sa nuit

Avec le temps tout s'évanouit. »

Léo Ferré

Références

[1] Arnold, V. : *Méthodes mathématiques de la mécanique classique.* Mir, Moscou, 1976.

[2] Arnold, V. : *Chapitres supplémentaires de la théorie des équations différentielles ordinaires.* Mir, Moscou, 1980.

[3] Berger, M. : Maths 89 : l'école française 3 ème du monde. *Science et Vie*, mars 1989, 274-283.

[4] Bollobás, B. : *Random Graphs.* Academic Press, London, 1985.

[5] Crutchfield, J., Farmer, D. & Packard, N., Shaw, R. : Le chaos. *Pour la Science*, février 1987, 26-50.

[6] Dyson F., Falk, H : Period of a discrete cat mapping. *Amer. Math. Monthly* 99 (1992), no. 7, 603–614.

[7] Lanford, O. : Informal remarks on the orbit structure of discrete approximations to chaotic maps. *Experiment. Math.* 7 (1998), no. 4, 317–324.

[8] Miernowski, T. : Discrétisations des homéomorphismes du cercle, à paraître dans *Ergod. Th. & Dynam. Sys.*

[9] Oxtoby, J.-C. : *Measure and Category.* Graduate Texts in Mathematics 2, Springer Verlag, New York, Heidelberg, Berlin, 1971.

[10] Petersen, K. : *Ergodic theory.* Cambridge University Press, Cambridge, 1983.

[11] Poincaré, H. : Sur le problème des trois corps et les équations de la dynamique. *Acta Math.* 13 (1890), 1-270.

[12] Poincaré, H. : Sur le problème des trois corps. *Bulletin Astronomique* 8 (1891), 12-24.

[13] Poincaré, H. : *Les méthodes nouvelles de la mécanique céleste,* tome 3. Gauthier-Villars, Paris, 1899.

[14] Poincaré, H. : Analyse des travaux scientifiques, *Œuvres* de Henri Poincaré, tome 7, Gauthier-Villars, Paris, 1952.

[15] Serre, J.-P. : *Cours d'arithmétique.* PUF, Paris, 1970.

Étienne Ghys

Unité de Mathématiques Pures et Appliquées

de l'École normale supérieure de Lyon

U.M.R. 5669 du CNRS

46, Allée d'Italie

69364 Lyon Cedex 07- France

ghys@umpa.ens-lyon.fr

---

22 septembre 2005
