ÉQUIVALENCE ET CONJUGAISON : DEUX NOTIONS DE BASE EN MATHÉMATIQUES

Aziz El Kacimi
Université de Valenciennes
Cité des Géométries - Gare numérique de Jeumont

Conférence
UVHC, Valenciennes le 12 janvier 2012
LE TOUR DE FRANCE DES DÉCHIFFREURS

Les mathématiques sont un élément
de base de beaucoup de sciences.
Mais elles voguent aussi dans un univers
de beauté, de rêve, de musique... et nourrissent
ainsi le cœur de ceux qui les pratiquent !
Alors veillons à ce qu'on n'en fasse
pas un produit de supermarché !

(Mon prêche personnel !)

Les hommes ne savent faire que quelques opérations :

- *additionner,*
- *soustraire,*
- *multiplier,*
- *diviser.*

Le travail du mathématicien consiste essentiellement à transformer leurs problèmes en d'autres qui leur sont équivalents et qui peuvent être résolus juste par ces quatre opérations !

L'équivalence est donc une notion centrale en mathématiques !

1. L'équivalence

1.1. Préliminaires

Soit E un ensemble. On se donne une *relation binaire* $\mathcal{R}$ entre ses éléments. Lorsque x est en relation avec y on écrit : $x \mathcal{R} y$.
On dira que $\mathcal{R}$ est une relation d'*équivalence* si elle satisfait les conditions qui suivent :

- ***réflexivité* : $x \mathcal{R} x$;**
- ***symétrie* : $x \mathcal{R} y \Longrightarrow y \mathcal{R} x$;**
- ***transitivité* : $x \mathcal{R} y$ et $y \mathcal{R} z$ impliquent $x \mathcal{R} z$.**

La *classe d'équivalence* d'un élément $x \in E$ est l'ensemble $\overline{x}$ des éléments de E qui sont équivalents à x au sens de cette relation :

$$\overline{x} = \{y \in E : x \mathcal{R} y\}.$$

Si x et x' ne sont pas équivalents, leurs classes d'équivalence $\overline{x}$ et $\overline{x'}$ sont deux parties disjointes de l'ensemble E ; les classes d'équivalence forment une *partition* de E. Inversement, toute partition de E donne lieu à une relation d'équivalence. En effet, supposons E partionné en n parties (on a pris un nombre fini de parties pour simplifier) $E_1, \cdots, E_n$:

$$E = E_1 \cup \cdots \cup E_n \quad \textbf{et} \quad E_i \cap E_j = \emptyset \quad \textbf{pour} \quad i \neq j.$$

À cette partition on associe alors la relation $\mathcal{R}$:

$$x \,\mathcal{R}\, y \textbf{ si, et seulement si, il existe } i \in \{1, \cdots, n\} : x, y \in E_i.$$

Une vérification élémentaire montre que $\mathcal{R}$ ainsi définie est bien une relation d'équivalence.

De façon naturelle, se pose le problème de la *représentativité* d'une classe :

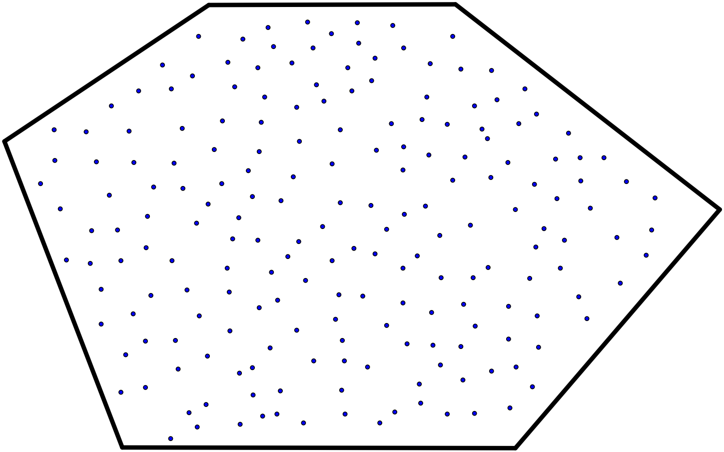
- **Admet-elle un *bon représentant*?**
- **Si oui, sur quels *critères* faut-il le choisir ?**
- **Comment l'*obtenir* à partir d'un élément quelconque ?**

Dans presque chaque situation il existe des critères permettant de montrer l'existence d'un bon représentant. On sait aussi comment, partant d'un élément quelconque ϕ dans une classe, en trouver un ψ qui soit "bon" ; on dit qu'on *conjugue* ϕ à ψ : les deux sont équivalents et gardent donc la *même propriété* voulue au départ !

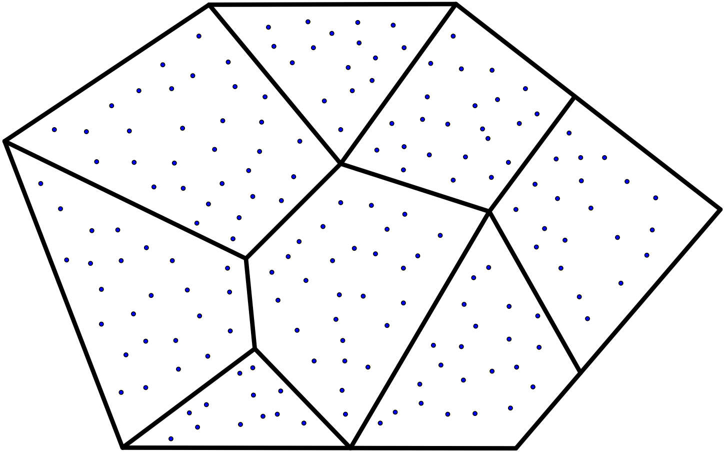
Nous allons voir comment les choses se passent selon le contexte et la nature des objets. Nous nous contenterons de traiter la question sur quelques exemples.

1.2. Un mauvais exemple

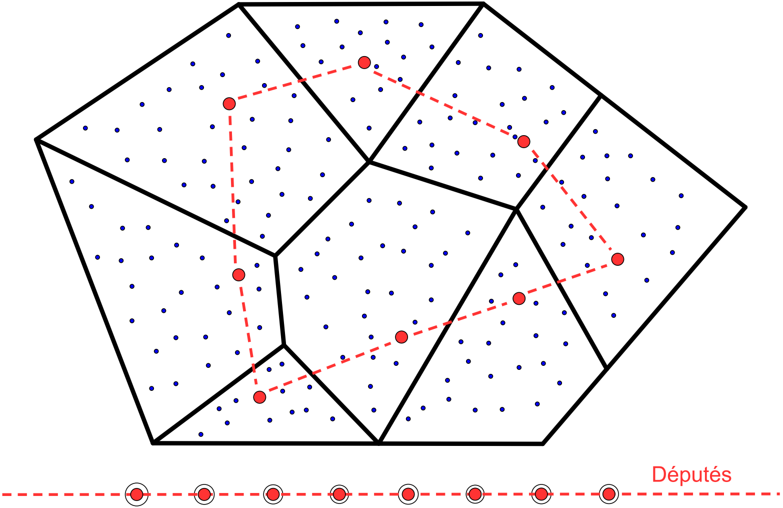
Un pays et ses habitants.



Ce même pays découpé en circonscriptions.



Chaque circonscription est représentée par un député.

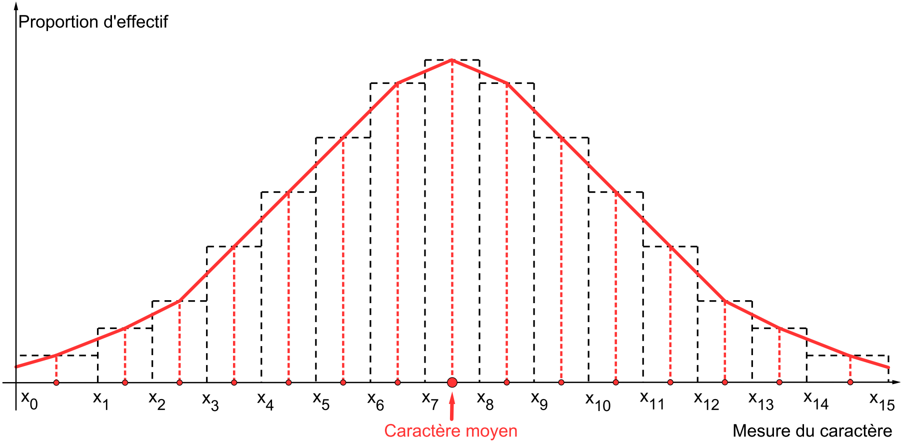


1.3. Exemple en statistiques

Problème assez courant en statistiques : on étudie un *caractère quantitatif* d'une *population*. Par exemple :

- **la *taille* des élèves d'un établissement scolaire,**
- **le *salaire* des employés d'une grande entreprise,**
- **la *répartition* de la population d'un pays suivant l'âge...**

Comme en général le nombre d'*individus* d'une population est assez grand, on fait des mesures sur un *échantillon* qu'on suppose assez *représentatif*. Mais la taille de l'échantillon peut aussi être assez grande et compliquer la tâche. On le partitionne alors en *classes*.


Proportion d'effectif
x_0
x_1
x_2
x_3
x_4
x_5
x_6
x_7
x_8
x_9
x_{10}
x_{11}
x_{12}
x_{13}
x_{14}
x_{15}
Caractère moyen
Mesure du caractère

1.4. Réduction d'une matrice

On se donne un espace vectoriel réel E de dimension n et une application $u : E \longrightarrow E$. On rappelle que u est dite ***linéaire*** si elle vérifie :

- $u(x+y) = u(x) + u(y)$ pour tous $x, y \in E$;
- $u(\lambda x) = \lambda u(x)$ pour tout $x \in E$ et tout $\lambda \in \mathbb{R}$.

Si $e = (e_1, \cdots, e_n)$ est une base de E, tout vecteur $x \in E$ s'écrit de façon unique :

$$x = x_1 e_1 + \cdots + x_n e_n$$

où les $x_1, \cdots, x_n$ sont des nombres réels ; la connaissance de ces réels détermine complètement le vecteur x. On écrit :

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

Ainsi :

$$u(x) = u(x_1 e_1 + \cdots + x_n e_n) = x_1 u(e_1) + \cdots + x_n u(e_n).$$

Pour connaître u, il suffit donc de connaître les vecteurs :

$$u(e_1) = \begin{pmatrix} a_{11} \\ \vdots \\ a_{n1} \end{pmatrix}, \quad \cdots \quad u(e_j) = \begin{pmatrix} a_{1j} \\ \vdots \\ a_{nj} \end{pmatrix}, \quad \cdots \quad u(e_n) = \begin{pmatrix} a_{1\,n} \\ \vdots \\ a_{nn} \end{pmatrix}$$

et donc le tableau de nombres :

$$\mathcal{M}(u, e) = \begin{pmatrix} a_{11} & \cdots & a_{1j} & \cdots & a_{1n} \\ \vdots & & \vdots & & \vdots \\ a_{i1} & \cdots & a_{ij} & \cdots & a_{in} \\ \vdots & & \vdots & & \vdots \\ a_{n1} & \cdots & a_{nj} & \cdots & a_{nn} \end{pmatrix}$$

Ce tableau de nombres est ce qu'on appelle la *matrice* de u relativement à la base e. Si on change la base e en une autre base ε, la matrice de u change. On a alors un diagramme commutatif :

$$(*) \qquad \begin{array}{ccc} (E,e) & \xrightarrow{u} & (E,e) \\ id \downarrow & & \uparrow id \\ (E,\varepsilon) & \xrightarrow{u} & (E,\varepsilon) \end{array}$$

Comme ε est une base, pour tout $j \in \{1, \cdots, n\}$, le vecteur e_j s'écrit $e_j = p_{1j}\varepsilon_1 + \cdots + p_{nj}\varepsilon_n$. Ce qui nous fournit une matrice :

$$P = \begin{pmatrix} p_{11} & \cdots & p_{1j} & \cdots & p_{1n} \\ \vdots & & \vdots & & \vdots \\ p_{i1} & \cdots & p_{ij} & \cdots & p_{in} \\ \vdots & & \vdots & & \vdots \\ p_{n1} & \cdots & p_{nj} & \cdots & p_{nn} \end{pmatrix}$$

La matrice P est inversible et son inverse $P^{-1} = (p'_{ij})$ permet de passer de la base e à la base ε :

$$\varepsilon_j = p'_{1j} e_1 + \cdots + p'_{nj} e_n.$$

Le diagramme $(*)$ se traduit au niveau des matrices par la relation :

$$(**) \qquad \mathcal{M}(u, e) = P^{-1} \mathcal{M}(u, \varepsilon) P.$$

Deux matrices A et B représentant la même application linéaire $E \longrightarrow E$ sont liées par la relation $A = P^{-1}BP$; on dit qu'elles sont ***semblables*** ou ***conjuguées***. Ce qui amène naturellement la question suivante :

Existe-t-il une base ε de E dans laquelle la matrice A de u soit la plus simple possible ? Par exemple diagonale ?

Si une telle base $\varepsilon = (\varepsilon_1, \cdots, \varepsilon_n)$ existe, la matrice D de u par rapport à ε est de la forme :

$$D = \begin{pmatrix} \lambda_1 & 0 & \cdots & \cdots & 0 \\ 0 & \lambda_2 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & \lambda_{n-1} & 0 \\ 0 & \cdots & \cdots & 0 & \lambda_n \end{pmatrix}$$

Cela signifie que E se casse en n sous-espaces $E_1, \cdots, E_n$, chacun de dimesnion 1 :

$$E = E_1 \oplus \cdots \oplus E_n$$

tels que la restriction de l'application u à chaque E_i n'est rien d'autre que la multiplication par le scalaire λ_i. Ceci rend l'étude de u beaucoup plus simple : on revient aux quatre opérations élémentaires susmentionnées !

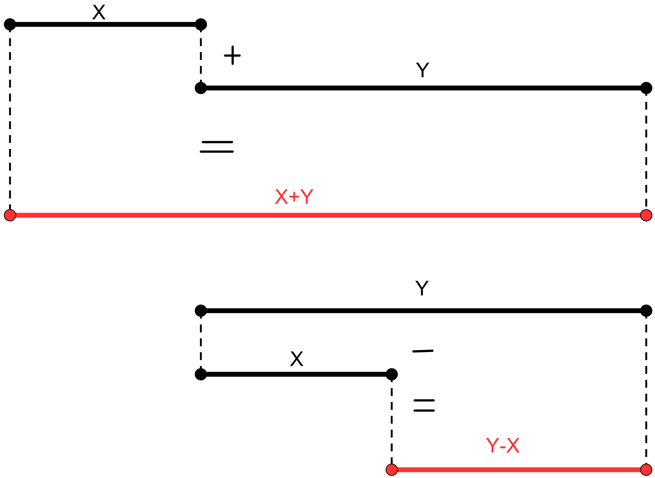
Chercher une matrice diagonale D semblable à A, c'est ***diagonaliser*** A. L'opération passe par le calcul des ***valeurs propres*** $\lambda_1, \cdots, \lambda_n$. Ce qui amène à la résolution d'une équation polynomiale de degré n ; on sait alors que, si n est assez grand, la partie est loin d'être gagnée ! L'existence des valeurs propres est une condition nécessaire (et non suffisante en général) pour pouvoir diagonaliser une matrice. Voici des exemples en dimension $n = 2$.

$$A_1 = \begin{pmatrix} 1 & 2 \\ 3 & 2 \end{pmatrix} \qquad A_2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad A_3 = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}.$$

La matrice A_1 est semblable à $\begin{pmatrix} -1 & 0 \\ 0 & 4 \end{pmatrix}$; A_2 a deux valeurs propres égales à 1 mais n'est pas diagonalisable. Quant à A_3, excepté pour $\theta \in \pi\mathbb{Z}$, elle n'a aucune valeur propre réelle.

1.5. Multiplier

L'addition et la soustraction de deux nombres réels (positifs) X et Y se réalisent physiquement comme suit :



Mais qu'en est-il du produit XY ?
Faut-il une machine qui transforme
la multiplication en addition ?

Oui ! et elle existe fort heureusement ! C'est la fonction
Logarithme **:** $X \in \mathbb{R}_+^* \longmapsto \ln(X) \in \mathbb{R}$.
Elle possède la propriété fondamentale :

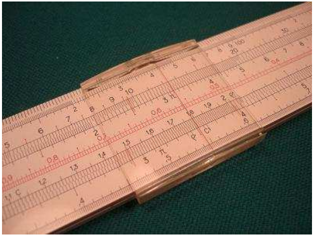
$$\ln(XY) = \ln(X) + \ln(Y).$$

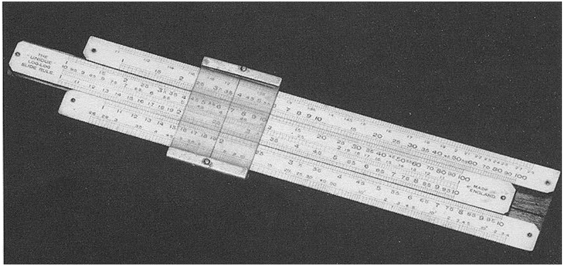
Elle est bijective et son inverse, la fonction ***exponentielle***
$X \in \mathbb{R} \longmapsto e^X \in \mathbb{R}_+^*$ **vérifie :**

$$e^{X+Y} = e^X \cdot e^Y.$$

C'est donc gagné : Le Logarithme amène X **et** Y **vers** $\mathbb{R}$**, on effectue physiquement l'addition de** $A = \ln(X)$ **et** $B = \ln(Y)$ **et l'Exponentielle ramène** $A + B$ **en** XY **dans** $\mathbb{R}_+^*$ **!**

$$\left(\mathbb{R} \text{ muni de l'addition}\right) \simeq \left(\mathbb{R}_+^* \text{ muni de la multiplication}\right)$$

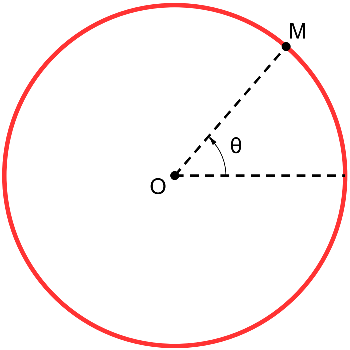




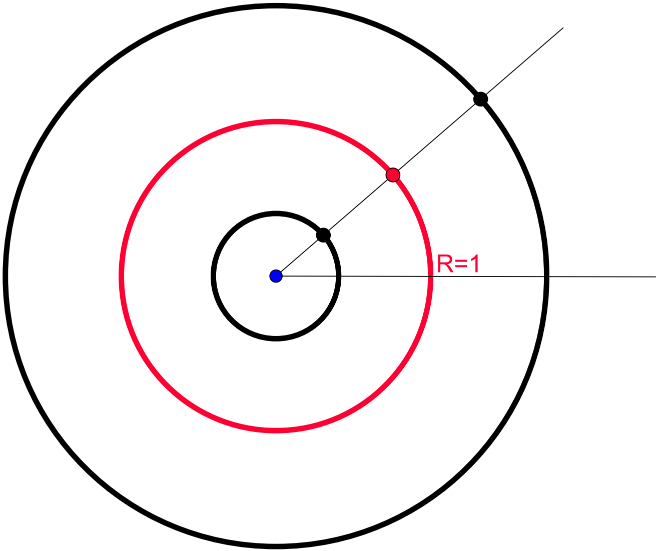
Règles à calcul

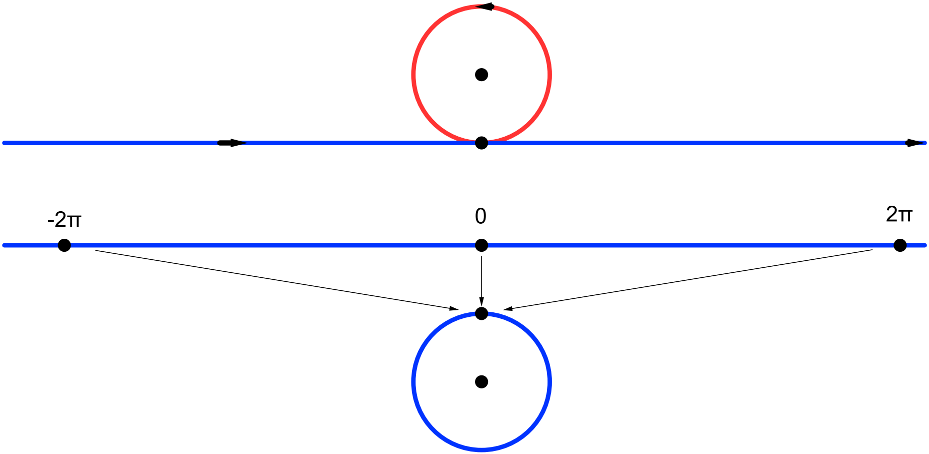
2. Un célèbre problème de conjugaison

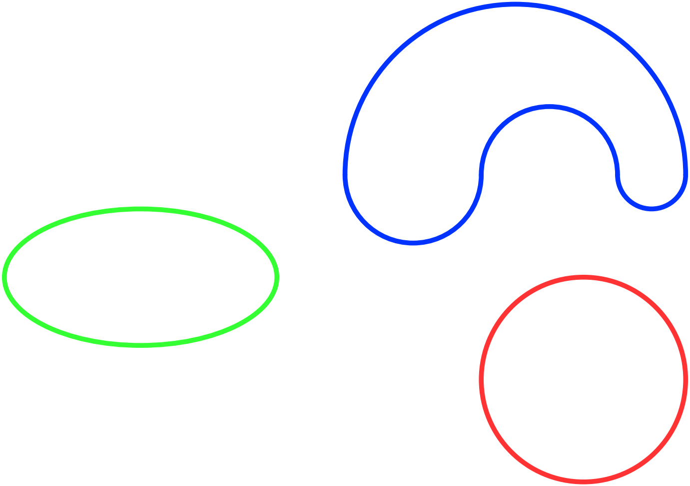
2.1. Le cercle



Le cercle de centre O et de rayon R est
l'ensemble des points du plan qui sont
à une distance R du point O


R=1


-2π
0
2π



Comment faire de l'analyse sur le cercle $\mathbb{S}^1$?

On a vu (sur un dessin précédent) que le cercle s'obtient à partir de $\mathbb{R}$ en identifiant un point x et tous ses translatés $x + 2k\pi$ où k est un entier relatif. C'est donc le quotient :

$$\mathbb{S}^1 = \mathbb{R}/2\pi\mathbb{Z}.$$

Une fonction sur le cercle $f : \mathbb{S}^1 \longrightarrow \mathbb{C}$ est donc représentée par une fonction $\widetilde{f} : \mathbb{R} \longrightarrow \mathbb{C}$ qui vérifie $\widetilde{f}(x + 2\pi) = f(x)$ pour tout $x \in \mathbb{R}$ *i.e.* une fonction d'une variable réelle et *périodique* de période 2π.

La régularité de f sera celle de $\widetilde{f}$:

- **f est continue $\Longleftrightarrow$ $\widetilde{f}$ l'est ;**
- **f est dérivable $\Longleftrightarrow$ $\widetilde{f}$ l'est ;**
- **f est de classe C^∞ $\Longleftrightarrow$ $\widetilde{f}$ l'est.**

. . .

Dorénavant on confondra f et $\widetilde{f}$ et on notera simplement f !

Comment reconnaître les fonctions C^∞ sur $\mathbb{S}^1$?

- **Les premiers exemples d'abord :** $\chi_n : x \in \mathbb{R} \longmapsto e^{inx}$ **avec** $n \in \mathbb{Z}$.
- **Les combinaisons linéaires finies** $S_n(x) = \sum_{n=-N}^{N} f_n e^{inx}$.
- **Les séries** $f(x) = \sum_{n \in \mathbb{Z}} f_n e^{inx}$ **quand elles convergent.**
- **Si cette série converge uniformément, la fonction** f **est continue.**
- **Si on dérive formellement, on obtient la série** $\sum_{n \in \mathbb{Z}} in f_n e^{inx}$.
- **Si cette série converge uniformément, la fonction** f **est de classe** C^1.

Plus les *coefficients de Fourier* f_n sont à décroissance rapide, plus la fonction f a tendance à être *régulière*. En fait, on a la :

Proposition

Toute fonction sur $\mathbb{S}^1$ s'écrit $f(x) = \sum_{n\in\mathbb{Z}} f_n e^{inx}$.

Elle est de classe C^∞

si, et seulement si,

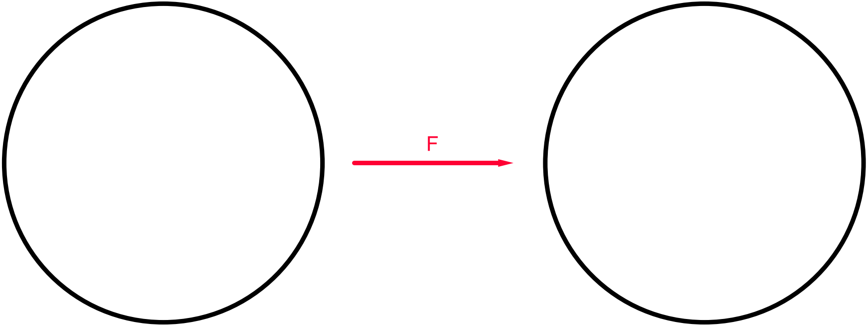
pour tout $r \in \mathbb{N}$, la série $\sum_{r\in\mathbb{Z}} |n|^r |f_n|$ converge.

Les fonctions de classe C^∞ sur le cercle $\mathbb{S}^1$ à valeurs réelles ou complexes forment des espaces vectoriels qui seront notés :

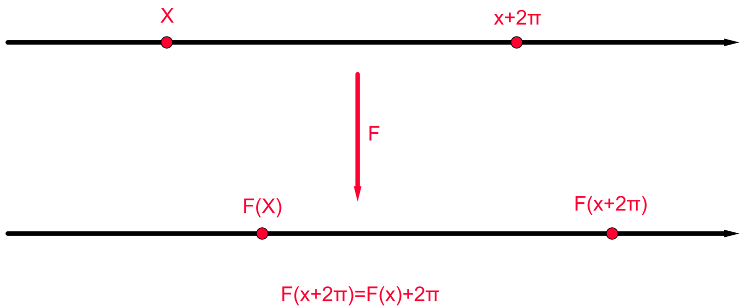
$$C^\infty(\mathbb{S}^1, \mathbb{R}) \qquad \text{et} \qquad C^\infty(\mathbb{S}^1, \mathbb{C}).$$

2.2. Homéomorphismes et difféomorphismes

Un *homéomorphisme* du cercle est une bijection $F : \mathbb{S}^1 \longrightarrow \mathbb{S}^1$ telle que F et F^{-1} soient continues.



Un homéomorphisme du cercle est induit par un homéomorphisme de la droite $F : \mathbb{R} \longrightarrow \mathbb{R}$ tel que $F(x + 2\pi) = F(x) + 2\pi$.



Un homéomorphisme $F : \mathbb{S}^1 \longrightarrow \mathbb{S}^1$ est un *difféomorphisme* si en plus F et F^{-1} sont de classe C^∞. C'est équivalent à dire que l'homéomorphisme de la droite $F : \mathbb{R} \longrightarrow \mathbb{R}$ qui induit F est aussi un difféomorphisme, c'est-à-dire qu'il est de classe C^∞ ainsi que son inverse F^{-1}.

Les homéomorphismes du cercle forment un groupe noté $\mathbf{Homéo}(\mathbb{S}^1)$; les difféomorphismes en forment un sous-groupe noté $\mathbf{Diff}(\mathbb{S}^1)$:

$$\mathbf{Diff}(\mathbb{S}^1) \subset \mathbf{Homéo}(\mathbb{S}^1).$$

Désormais, on ne considérera que les homéomorphismes et les différomorphismes qui préservent l'orientation du cercle (qu'on suppose donnée). Les groupes correspondants seront notés respectivement $\mathbf{Homéo}_+(\mathbb{S}^1)$ et $\mathbf{Diff}_+(\mathbb{S}^1)$ et on a bien sûr :

$$\mathbf{Diff}_+(\mathbb{S}^1) \subset \mathbf{Homéo}_+(\mathbb{S}^1).$$

2.3. Orbites

Soit $F : \mathbb{S}^1 \longrightarrow \mathbb{S}^1$ un homéomorphisme du cercle (préservant l'orientation). Pour tout $n \in \mathbb{Z}$, on pose :

$$F^n = \begin{cases} \text{identité} & \text{si } n = 0 \\ F \circ \cdots \circ F & n \text{ fois si } n > 0 \\ F^{-1} \circ \cdots \circ F^{-1} & |n| \text{ fois si } n < 0 \end{cases}$$

L'***orbite*** d'un point $x \in \mathbb{S}^1$: $\mathcal{O}_x = \{F^n(x) : n \in \mathbb{Z}\}$.

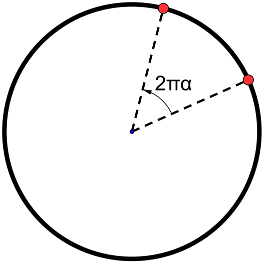
L'étude de la structure des orbites de l'homéomorphisme F est centrale dans la compréhension du ***système dynamique*** $(\mathbb{S}^1, F)$.

Une orbite peut être :

- ***périodique***, c'est-à-dire $\mathcal{O}_x = \{x, F(x), \cdots, F^p(x) = x\}$;
- ***dense*** dans le cercle : elle rencontre tout arc ouvert ;
- ou plus ***compliquée***.

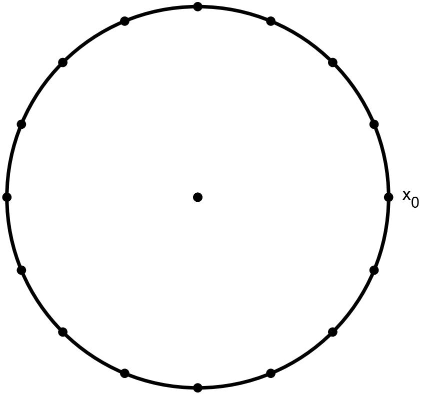
L'exemple le plus simple dans $\mathit{Diff}_+(\mathbb{S}^1)$ *!*

Une rotation

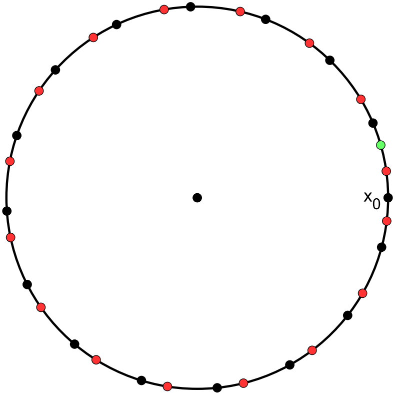


induite par une translation de la droite réelle.

Ses orbites



Orbite par une
rotation rationnelle



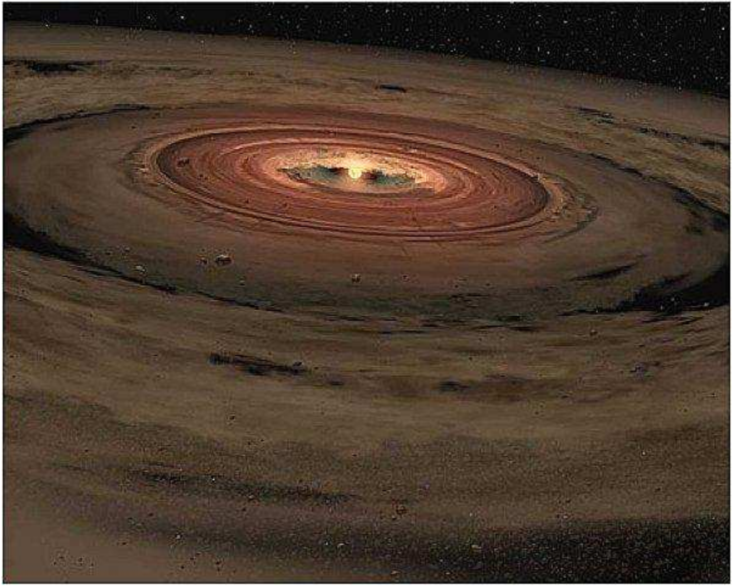
Orbite par une
rotation irrationnelle

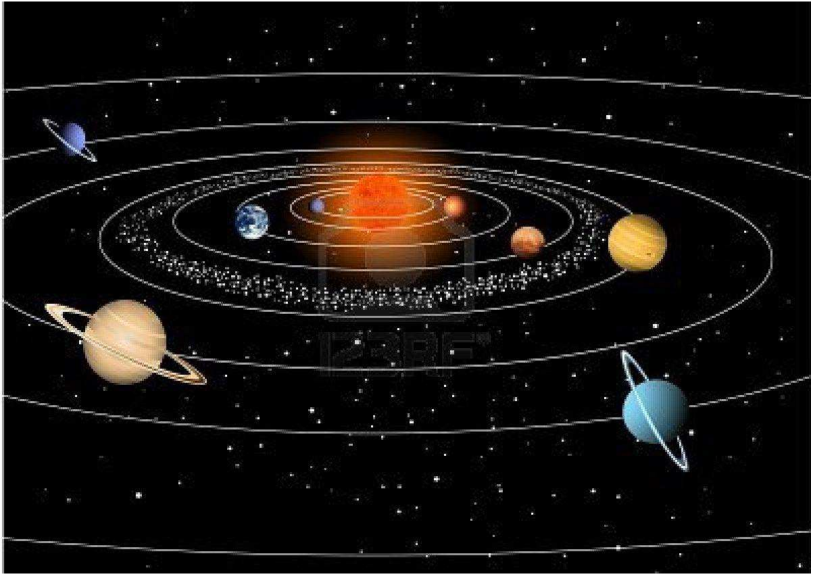
Mais pourquoi le cercle ?

Beaucoup de phénomènes apparaissant dans le monde où nous vivons sont *périodiques*. Les trajectoires des éléments qui y interviennent sont cycliques et sont des *courbes fermées*, et en particulier des *cercles*.

Les exemples abondent :

- **La terre fait le tour sur elle-même en *24 heures* et**
- **autour du soleil en *365 jours et 6 heures* à peu près.**
- **Il y a *un milliard d'années*, j'étais probablement dans cette salle, devant vous et en train de vous servir la même salade !**




123RF

2.4. Formulation du problème

Question

Soit F un élément de Diff$_+(\mathbb{S}^1)$. Dans quelle mesure est-il équivalent à un élément de Diff$_+(\mathbb{S}^1)$ mais beaucoup plus simple, par exemple une rotation ?

Cela signifie : ***peut-on reparamétrer le cercle $\mathbb{S}^1$ de façon à ce que F "soit une rotation" ?***

En termes plus précis : ***existe-t-il un élément $H \in$ Diff$_+(\mathbb{S}^1)$ et une rotation R_α (d'angle $2\pi\alpha$) tels que le diagramme qui suit soit commutatif ?***

$$\begin{array}{ccc} \mathbb{S}^1 & \xrightarrow{F} & \mathbb{S}^1 \\ H \downarrow & & \uparrow H \\ \mathbb{S}^1 & \xrightarrow{R_\alpha} & \mathbb{S}^1 \end{array}$$

Nous avons donc à résoudre l'équation, hautement *non linéaire* :

$$(ENL) \qquad H \circ F = R_\alpha \circ H \qquad \textbf{ou} \qquad R_\alpha = H \circ F \circ H^{-1}.$$

Il y a deux inconnues : la rotation R_α et le difféomorphisme H.

Ce problème a été initié au début du 20ème siècle par *Poincaré*.

Depuis lors, des mathématiciens de taille ont contribué à sa résolution. De façon directe :

Denjoy, Arnold, Moser, Herman, Yoccoz,...

De façon indirecte :

Kolmogorov, Nash, Hamilton,...

2.5. Résolution du problème

Nous ne donnerons évidemment que les grandes étapes et juste dans le cas où il y avait le plus de difficultés.

Nous verrons toujours un élément F de Homéo$_+(\mathbb{S}^1)$ ou Diff$_+(\mathbb{S}^1)$ comme un homéomorphisme ou difféomorphisme $\mathbb{R} \longrightarrow \mathbb{R}$ vérifiant $F(x+2\pi) = F(x) + 2\pi$.

Y a-t-il un candidat R_α ?

***Poincaré* avait démontré le :**

Théorème

*Pour tout $x \in \mathbb{R}$ la limite $\lim\limits_{n\to+\infty} \left\{ \dfrac{F^n(x) - x}{2\pi n} \right\}$ existe et définit un élément dans $\mathbb{Z}/2\pi\mathbb{Z}$ indépendant de x. On le note $\rho(F)$ et on l'appelle **nombre de rotation** de F.*

On pose alors $\alpha = \rho(F)$ et on note R_α la rotation induite par la translation $x \in \mathbb{R} \longmapsto x + 2\pi\alpha$.

Un calcul simple montre que α est rationnel si, et seulement si, F a un point périodique, c'est-à-dire il existe $x \in \mathbb{R}$ et un entier $p >$ tels que $F^p(x) = x$. On a toujours $\rho(R_{2\pi\theta}) = \theta$.

Désormais, F est un difféomorphisme et son nombre de rotation α est irrationnel.

La première frappe au problème de la *conjugaison* de F à R_α a été portée par *Denjoy* vers les années 30 :

Théorème

*Soit $F \in Diff_+(\mathbb{S}^1)$ ayant un nombre de rotation $\alpha = \rho(F)$ irrationnel. Alors F est **topologiquement conjugué** à la rotation R_α i.e. il existe $H \in Homéo_+(\mathbb{S}^1)$ tel que $R_\alpha = H \circ F \circ H^{-1}$.*

C'est un travail d'artiste de l'analyse fine et *Denjoy* était sans doute le meilleur de cette spécialité !

Restait toutefois une question cruciale qui a traversé le siècle dernier :

Peut-on lisser H en un difféomorphisme ?

C'est-à-dire :

Existe-t-il $H \in \mathrm{Diff}_+(\mathbb{S}^1)$ tel que $R_\alpha = H \circ F \circ H^{-1}$?

Ce sont *Arnold* et *Moser* qui apportèrent les premières réponses au début des années 60.

Avant de continuer à conter l'histoire, faisons la remarque qui suit (valable pour n'importe quel $\alpha = \rho(F)$ rationnel ou pas) : on peut toujours écrire $F(x) = x + f(x)$ où $f : \mathbb{R} \longrightarrow \mathbb{R}$ est une fonction C^∞, 2π-périodique et qui induit donc une fonction $\mathbb{S}^1 \xrightarrow{f} \mathbb{R}$ de classe C^∞. En particulier, si F et G sont deux éléments de $\mathrm{Diff}_+(\mathbb{S}^1)$, $F - G$ est un élément de $C^\infty(\mathbb{S}^1, \mathbb{R})$.

La linéarisation de l'équation (ENL) amène à l'équation suivante :

$$h(x) - h(x + 2\pi\alpha) = f(x)$$

pour tout x **où** $f(x) = F(x) - x$ **et** $h(x) = H(x) - x$.
Si on intègre les deux membres de cette équation sur l'intervalle $[0, 2\pi]$, **on obtient :**

$$\int_0^{2\pi} f(x)dx = \int_0^{2\pi} h(x)dx - \int_0^{2\pi} h(x + 2\pi\alpha)dx = 0.$$

La condition $I(f) = \int_0^{2\pi} f(x)dx = 0$ **est donc nécessaire pour que l'équation** $h(x) - h(x + 2\pi\alpha) = f(x)$ **admette une solution.**

En fait, lorsque la fonction $F - R_\alpha$ **et toutes ses dérivées successives sont "suffisamment proches" de** 0, **la résolution de l'équation non linéaire (ENL) est équivalente à la résolution le l'équation suivante, dite** ***équation cohomologique*** **:**

Étant donnée $f \in C^\infty(\mathbb{S}^1, \mathbb{R})$ ***vérifiant***
$I(f) = 0$ ***existe-t-il*** $h \in C^\infty(\mathbb{S}^1, \mathbb{R})$ ***telle que :***
$h(x) - h(x + 2\pi\alpha) = f(x)$ ***?***

Pour résoudre ce problème, on développe f et h en série de Fourier :

$$f(x) = \sum_{n \in \mathbb{Z}} f_n e^{inx} \qquad \text{et} \qquad h(x) = \sum_{n \in \mathbb{Z}} h_n e^{inx}.$$

Comme f est déjà donnée dans $C^\infty(\mathbb{S}^1, \mathbb{R})$, ses coefficients de Fourier f_n sont tels que :

pour tout $r \in \mathbb{N}$, la série $\sum_{n \in \mathbb{Z}} |n|^r |f_n|$ converge.

L'équation $h(x) - h(x + 2\pi\alpha) = f(x)$ se ramène alors, au niveau des coefficients de Fourier des fonctions f et h, au système :

$$(S) \qquad (1 - e^{2i\pi n\alpha})h_n = f_n \qquad \text{pour} \qquad n \in \mathbb{Z}.$$

Pour $n = 0$ on a $1 - e^{2i\pi n\alpha} = 0$; ce qui impose la condition $f_0 = 0$; mais elle est déjà vérifiée puisque $f_0 = I(f) = 0$.

Comme α est irrationnel, $1 - e^{2i\pi n\alpha} \neq 0$ pour $n \neq 0$. On a donc une solution formelle en posant :

$$h_n = \begin{cases} 0 & \text{pour } n = 0 \\ \frac{f_n}{1 - e^{2i\pi n\alpha}} & \text{pour } n \neq 0. \end{cases}$$

Les h_n définissent-ils une fonction $h \in C^\infty(\mathbb{S}^1, \mathbb{R})$?

Il faudrait à cet effet que :

pour tout $r \in \mathbb{N}$, la série $\sum_{n\in\mathbb{Z}} |n|^r |h_n|$ converge !

La réponse dépend de la *nature arithmétique* du nombre α.

Définition

*On dira qu'un nombre irrationnel α est **diophantien** s'il existe des constantes $A > 0$ et $\delta > 0$ telles que, pour tout $m \in \mathbb{Z}$ et tout $n \in \mathbb{N}^*$, on ait :*

$$\left|\alpha - \frac{m}{n}\right| \geq \frac{A}{|n|^{2+\delta}}$$

*Cela signifie que α est **très mal approché** par les rationnels.*

C'est aussi équivalent à dire (un calcul simple permet de le voir) :

Il existe $A > 0$ et $\delta > 0$ tel que $\left|1 - e^{2i\pi n\alpha}\right| \geq \frac{A}{|n|^{1+\delta}}$

Par exemple, tout irrationnel *algébrique* (*i.e.* racine d'un polynôme à coefficients entiers) est diophantien.

Les irrationnels "très bien approchés" par les rationnels sont appelés *nombres de Liouville*.
On en construit par des sommes de séries de nombres rationnels à décroissance rapide, par exemple :

$$\alpha = \sum_{s=1}^{\infty} 2^{-s!}$$

(dont Liouville a démontré la *transcendance*).

Supposons α diophantien et montrons que les coefficients h_n définissent bien une fonction h de classe C^∞. Il suffit de montrer que, pour tout $r \in \mathbb{N}$, la série numérique :

$$\sum_{n \in \mathbb{Z}} |n|^r |h_n|$$

converge. On a, pour $n \neq 0$:

$$\begin{aligned} |n|^r|h_n| &= |n|^r\left|\frac{f_n}{1-e^{2i\pi n\alpha}}\right| \\ &= |n|^r\frac{|f_n|}{|1-e^{2i\pi n\alpha}|} \\ &\leq |n|^r\frac{|f_n|}{\frac{A}{|n|^{1+\delta}}} \\ &\leq \frac{1}{A}|n|^{r+\delta+1}|f_n|. \end{aligned}$$

D'où :

$$\sum_{n\in\mathbb{Z}}|n|^r|h_n| \leq \frac{1}{A}\sum_{n\in\mathbb{Z}}|n|^{r+\delta+1}|f_n| < +\infty.$$

Ce qui montre que h est de classe C^∞. L'équation cohomologique (EC) a donc une solution et par suite F est C^∞-conjugué à la rotation R_α.

On a finalement le :

Théorème (Arnold - Moser)

Soit $F \in Diff_+(\mathbb{S}^1)$ ayant un nombre de rotation $\alpha = \rho(F)$ irrationnel et diophantien. On suppose que $F - R_\alpha$ est proche de 0 ainsi que toutes ses dérivées. Alors il existe $H \in Diff_+(\mathbb{S}^1)$ tel que :

$$R_\alpha = H \circ F \circ H^{-1}.$$

Si en plus F est analytique, il en est de même pour H.

La suite est une histoire passionnante qui mérite d'être contée. Mais elle est longue et difficile !

Henri Poincaré

POUR EN SAOIR PLUS !

[Arn] – ARNOLD, V. *Chapitres supplémentaires de la théorie des équations différentielles ordinaires.* Éditions MIR, Moscou (1980).

[Den] – DENJOY, A. *Sur les courbes définies par les équations différentielles à la surface du tore.* J. Math. Pures et App. Vol. 11, (1932) 333-375.

[Her] – HERMAN, M. *Sur la conjugaison différentiable des difféomorphismes du cercle à des rotations.* Publ. Math. IHES, n^o 49 (1979), 5-234.

[Yoc] – YOCCOZ, J.-C. *Petits diviseurs en dimension 1.* Astérisque 231, SMF (1995).