Université Paris-Saclay
UFR de Mathématiques

Projet de travail de recherche encadré
en mathématiques

Encadrant de TER : Omar MOHSEN

Le nombre de rotation

Matiss BRUNEL, Quentin GITON, Flore LE ROUX

Année universitaire 2021-2022

Table des matières

Introduction

En 1881, Henri Poincaré publie un article intitulé "Mémoire sur les courbes définies par une équation différentielle". Le point de départ de ce mémoire est le fameux problème à trois corps. Dans sa démarche il se retrouve, de manière naturelle, à commencer une étude du cercle. Cette étude du cercle constitue le point de départ d'un domaine des mathématiques : l'étude des systèmes dynamiques. Ainsi commence donc le travail de Poincaré dans lequel il étudie des systèmes discrets sur le cercle.

C'est dans la partie III de son mémoire, alors publiée en 1885, qu'est introduit le premier invariant dynamique important du cercle : le nombre de rotation. Cet invariant caractérise la vitesse asymptotique à laquelle tourne les points du cercle sous l'action d'un système. On dispose alors d'une classification des systèmes de la sorte.

Le but de ce mémoire est donc de donner un aperçu des résultats sur le nombre de rotation. On commencera donc par une rapide présentation de la théorie des systèmes dynamiques et la présentation de résultats remarquables sur les rotations. On introduira ensuite le nombre de rotation après quoi on discutera des résultats introduits par Poincaré concernant les homéomorphismes du cercle. Viendront ensuite les principaux résultats énoncés et démontrés par Arnaud Denjoy, résultats parus vers 1910, concernant les difféomorphismes du cercle. La dernière partie est une ouverture consacrée à une introduction à la théorie ergodique dans laquelle on énonce certains résultats en lien avec le nombre de rotation.

Finalement, pour les énoncés et démonstrations de ce texte on a suivi [BS02 ; Kue07 ; Nav07 ; San18 ; Pau21].

1 Premières définitions

1.1 Systèmes dynamiques

Commençons par introduire la notion de système dynamique.

Définition 1.1. *Soit X un espace topologique. Un **système dynamique discret** est une application continue $f : X \to X$ de l'espace X dans lui-même.*

Le fait que f envoie X dans lui-même permet de considérer les itérées f^n, $n \in \mathbb{N}$, où

$$f^n = \underbrace{f \circ \cdots \circ f}_{\text{n fois}}.$$

On peut alors définir orbites d'un point :

Définition 1.2. *Si $f : X \to X$ est un système dynamique discret, **l'orbite positive** de $x \in X$ par f est :*

$$\mathcal{O}_+^f(x) = \{f^n(x),\ n \in \mathbb{N}\}$$

*Si f est bijective, on définit **l'orbite** de x par $\mathcal{O}^f(x) = \{f^n(x),\ n \in \mathbb{Z}\}$ ainsi que **l'orbite négative** de x par $\mathcal{O}_-^f(x) = \{f^{-n}(x),\ n \in \mathbb{N}\}$.*

L'objet de la théorie des systèmes dynamiques est l'étude du comportement des orbites et de la façon dont elles varient avec le point initial x. On va donc chercher à étudier $\mathcal{O}_+^f(x)$, ce qui amène de nouvelles définitions :

Définition 1.3. *Un point $x \in X$ est **périodique** s'il existe un entier $n \geq 1$ tel que $f^n(x) = x$. La **période** d'un point périodique x est le plus petit entier $n \geq 1$ tel que $f^n(x) = x$.*

Définition 1.4. *S'il existe $x \in X$ tel que $\mathcal{O}_+^f(x)$ est dense dans X, on dit que f est **topologiquement transitive**.*

Définition 1.5. *On appelle **l'ensemble ω-limite** de x et on note $\overline{\omega}(x)$ l'ensemble*

$$\overline{\omega}(x) = \bigcap_{k \geq 0} \overline{\bigcup_{n \geq k} f^n(x)}.$$

Proposition 1.1.1. *Si X est un espace métrique sans point isolé, f est topologiquement transitive si et seulement s'il existe $x \in X$ tel que $\overline{\omega}(x) = X$.*

Démonstration. Supposons que X soit un espace métrique sans point isolé.

Le sens réciproque de l'équivalence est démontré par le fait que l'ensemble $\overline{\omega}(x)$ est inclus dans l'ensemble $\overline{\mathcal{O}_+^f(x)}$, quel que soit x.

Démontrons le sens direct. Soit $x \in X$ tel que $\mathcal{O}_+^f(x)$ soit dense dans X. Soit $y \in X$. Montrons alors que $y \in \overline{\omega}(x)$.

Commençons pour cela par démontrer que tout voisinage de y contient un point de $\mathcal{O}_+^f(x)$, autre que y si $y \in \mathcal{O}_+^f(x)$. Par l'absurde, supposons que ça ne soit pas le cas. Soit U un voisinage de y ne contenant pas de point de $\mathcal{O}_+^f(x)$ (autre que y si $y \in \mathcal{O}_+^f(x)$), que l'on peut choisir ouvert sans perte de généralité. Alors comme X est sans point isolé, il existe $z \in U \setminus \{y\}$. Comme $\mathcal{O}_+^f(x)$ est dense dans X, il existe une suite d'éléments de $\mathcal{O}_+^f(x)$ qui converge vers z, ce qui contredit le fait que U ne contient pas d'éléments de $\mathcal{O}_+^f(x)$, autre que y si $y \in \mathcal{O}_+^f(x)$.

Donc tout voisinage de y contient un point de $\mathcal{O}_+^f(x)$, autre que y si $y \in \mathcal{O}_+^f(x)$. On construit alors par récurrence une suite $(n_k)_{k\in\mathbb{N}^*}$ telle que la suite $(f^{n_k}(x))_{k\in\mathbb{N}^*}$ converge vers y.
Considérons pour cela la boule de rayon 1 centrée en y. On fixe $n_1 \in \mathbb{N}$ tel que $f^{n_1}(x)$ soit dans la boule et tel que $f^{n_1}(x) \neq y$.
Supposons maintenant que les k_0 premiers termes de la suite $(n_k)_{k\in\mathbb{N}^*}$ soient construits. On considère la boule de centre y et de rayon $\min(\frac{1}{k_0+1}, \mathrm{d}(y, f^{n_{k_0}}(x)))$. Alors on fixe $n_{k_0+1} \in \mathbb{N}$ tel que $f^{n_{k_0+1}}(x)$ soit dans cette boule et tel que $f^{n_{k_0+1}}(x) \neq y$.
Par construction, la suite $(n_k)_{k\in\mathbb{N}^*}$ est injective, donc quitte à extraire, on peut supposer qu'elle est strictement croissante. Donc $(f^{n_k}(x))_{k\in\mathbb{N}}$ est une suite extraite de $(f^n(x))_{n\in\mathbb{N}}$ convergeant vers y, i.e. $y \in \overline{\omega}(x)$. $\square$

Proposition 1.1.2. *Soit $x \in X$. Les ensembles $\mathcal{O}_+^f(x)$, $\omega(x)$ et $\overline{\omega}(x)$ sont invariants par f.*

1.2 Cercle et relèvements

Si l'objet central de notre étude s'avère être le cercle, il est important de le définir. Il est aussi important de remarquer qu'il est possible de le voir de plusieurs manières, toutes équivalentes entre elles.

Définition 1.6. *Dans la suite, nous verrons le **cercle**, dénoté par $\mathbb{S}^1$, comme :*

(*i*) *Le segment $[0, 1]$, dont on identifie implicitement les extrémités ;*

(*ii*) *Le cercle unité complexe $C = \{z \in \mathbb{C} \,:\, |z| = 1\}$;*

(*iii*) *Le quotient ${}^{\mathbb{R}}\!/\!{}_{\mathbb{Z}}$, dont on notera $\pi : \mathbb{R} \to {}^{\mathbb{R}}\!/\!{}_{\mathbb{Z}}$ la projection canonique.*

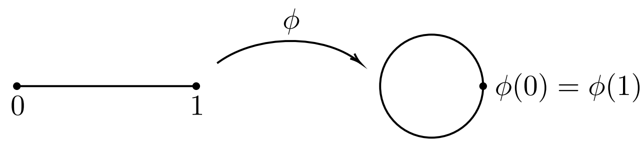

FIGURE 1 – Illustration du point (i)

Remarque. Une famille d'homéomorphismes du cercle se démarque par sa simplicité : l'ensemble des rotations. On entend ici par rotation une application de la forme :

$$R_\alpha : \begin{array}{ccc} \mathbb{R}/\mathbb{Z} & \longrightarrow & \mathbb{R}/\mathbb{Z} \\ x & \longmapsto & x + \alpha \mod 1 \end{array}$$

où $\alpha \in \mathbb{R}/\mathbb{Z}$.

Définition 1.7. *Si $f : \mathbb{S}^1 \to \mathbb{S}^1$ est continue, on appelle* ***relèvement*** *de f toute fonction $F : \mathbb{R} \to \mathbb{R}$ continue qui satisfait la relation :*

$$\pi \circ F = f \circ \pi.$$

Autrement dit, un relèvement de f est une fonction continue F telle que le diagramme suivant commute :

$$\begin{tikzcd} \mathbb{R} \arrow[r, "F"] \arrow[d, "\pi"'] \arrow[dr, phantom, "\circlearrowleft"] & \mathbb{R} \arrow[d, "\pi"] \\ \mathbb{S}^1 \arrow[r, "f"] & \mathbb{S}^1 \end{tikzcd}$$

Théorème 1.2.1. (de relèvement). *Pour toute application continue $f : \mathbb{S}^1 \to \mathbb{S}^1$, il existe une fonction $F : \mathbb{R} \to \mathbb{R}$ qui relève f.*

On pourra se référer à la page Wikipédia du théorème correspondant pour avoir une idée de sa démonstration.

Dans tout ce qui suit, f désignera une fonction continue du cercle dans lui-même et F un de ses relèvements.

Proposition 1.2.2. *Si F_1 est un relèvement de f alors il existe k dans $\mathbb{Z}$ tel que $F_1 = F + k$. Réciproquement, les fonctions de la forme $F + k$, où $k \in \mathbb{Z}$, sont des relèvements de f.*

Démonstration.

— Soit $x \in \mathbb{R}$ et soit F_1 un autre relèvement de f. On a :

$$\pi \circ (F_1 - F)(x) = (f \circ \pi)(x) - (f \circ \pi)(x) = 0,$$

donc $(F_1 - F)(x) \in \mathbb{Z}$. Ainsi, $F_1 - F$ est une fonction continue à valeurs dans l'espace discret $\mathbb{Z}$ et est donc constante par connexité de $\mathbb{R}$. Ainsi, il existe $k \in \mathbb{Z}$ tel que $F_1 = F + k$.

— Soit maintenant $k \in \mathbb{Z}$. On a :

$$\pi \circ (F + k) = \pi \circ F + \pi(k) = \pi \circ F = f \circ \pi,$$

donc $F + k$ est bien un relèvement. □

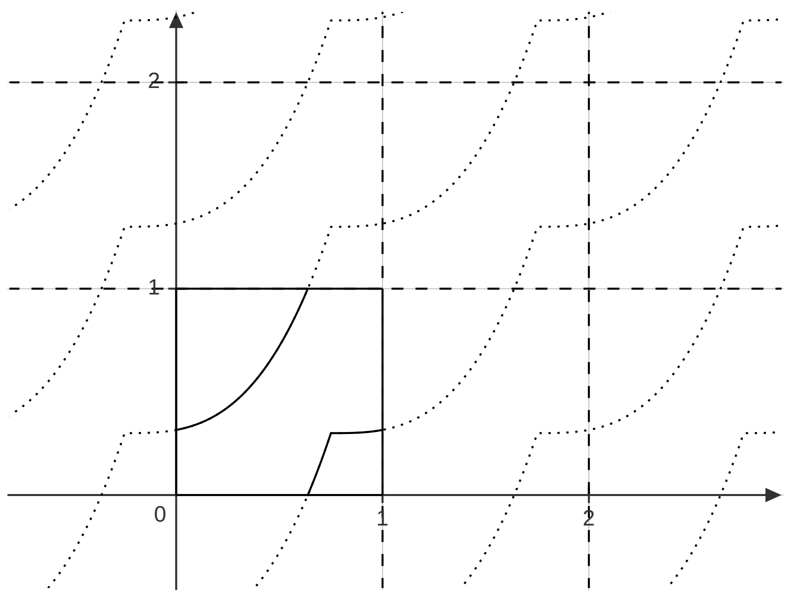

FIGURE 2 – Relèvements d'une fonction du cercle

Proposition 1.2.3. *Soit $x \in \mathbb{R}$, alors :*

(*i*) $F(x+1) - F(x) \in \mathbb{Z}$;

(*ii*) $F(x+1) - F(x)$ *ne dépend ni de x ni du relèvement choisi pour f.*

Démonstration. Soit $x \in \mathbb{R}$.

(i) On a les égalités :

$$\pi \circ (F(x+1) - F(x)) = (f \circ \pi)(x+1) - (f \circ \pi)(x) = 0$$

car $\pi(x+1) = \pi(x)$ par définition du quotient par $\mathbb{Z}$, ce qui signifie bien que $F(x+1) - F(x) \in \mathbb{Z}$.

(ii) La fonction $[x \longmapsto F(x+1) - F(x)]$ est continue à valeurs dans $\mathbb{Z}$, donc est constante par connexité de $\mathbb{R}$. L'indépendance par rapport au relèvement découle de la proposition précédente. $\square$

Définition 1.8. *On définit* ***le degré*** *de f comme la différence* $\deg(f) := F(x+1) - F(x)$.

Proposition 1.2.4.

(*i*) *Soit* $g : \mathbb{S}^1 \to \mathbb{S}^1$ *une fonction continue. Alors,* $\deg(f \circ g) = \deg(f) \cdot \deg(g)$

(*ii*) *Pour tout* $n \in \mathbb{N}$*,* F^n *est un relèvement de* f^n *qui vérifie :*

$$\forall p \in \mathbb{N},\ \forall x \in \mathbb{R}, \quad F^n(x+p) = F^n(x) + \deg(f)^n \cdot p$$

(*iii*) *Si* f *est un homéomorphisme, alors :*

— $\deg(f) = \pm 1$

— F *est bijective*

— F^{-1} *est un relèvement de* f^{-1}

Démonstration.

(i) Soit G un relèvement de g et soit $x \in \mathbb{R}$. Alors :

$$\begin{aligned}(F \circ G)(x+1) - (F \circ G)(x) &= F(G(x) + \deg(g)) - F(G(x)) \\ &= F(G(x) + \deg(g) - 1) + \deg(f) - F(G(x)) \\ &= F(G(x) + \deg(g) - 2) + 2 \cdot \deg(f) - F(G(x)) \\ &= \cdots \\ &= F(G(x)) + \deg(f) \cdot \deg(g) - F(G(x)) \\ &= \deg(f) \cdot \deg(g).\end{aligned}$$

(ii) Remarquons que :

$$\pi \circ F^n = f \circ \pi \circ F^{n-1} = \cdots = f^n \circ \pi.$$

D'après le point précédent, on a $\deg(f^n) = \deg(f)^n$. Ainsi, par récurrence sur p on trouve $F^n(x+p) = F^n(x) + \deg(f^n) \cdot p = F^n(x) + \deg(f)^n \cdot p$.

(iii) Notons que le point (ii) nous assure que $\deg(f) = \pm 1$. En effet, on a

$$\deg(f \circ f^{-1}) = \deg(f)\deg(f^{-1}) = \deg(\mathrm{Id}) = 1.$$

Donc, $\deg(f) = \pm 1$.

— **Injectivité** :
Soit $x, y \in \mathbb{R}$. Si $F(x) = F(y)$, alors par injectivité de f on a $\pi(x-y) = 0$ ce qui signifie que x et y sont dans la même classe d'équivalence modulo $\mathbb{Z}$. Autrement dit, $x - y = k \in \mathbb{Z}$. Or, le point précédent nous donne $F(y+k) = F(x) = F(y) + k \cdot \deg(f) = F(y) \pm k$. On a alors nécessairement $k = 0$ et donc $x = y$.

Surjectivité :
Quitte à considérer la fonction $-f$, supposons que $\deg(f) > 0$. Alors :

$$\lim_{n \to +\infty} F(n) = \lim_{n \to +\infty} [F(0) + n \cdot deg(f)] = +\infty.$$

On montre de même que :

$$\lim_{n \to -\infty} F(n) = -\infty.$$

F étant continue, le théorème des valeurs intermédiaires nous donne sa surjectivité.

— Par définition :

$$f^{-1} \circ \pi = f^{-1} \circ \pi \circ (F \circ F^{-1}) = f^{-1} \circ (\pi \circ F) \circ F^{-1} = f^{-1} \circ f \circ \pi \circ F^{-1} = \pi \circ F^{-1}.$$

$\square$

2 Les rotations

Dans cette section, nous allons définir les rotations introduites dans la section précédente.

La question naturelle qui se pose concerne l'angle d'une rotation : que peut-on dire de l'orbite d'une rotation d'angle rationnel ? Que peut-on dire de celle d'une rotation d'angle irrationnel ? Dans cette section, nous allons voir deux théorèmes qui répondent à ces questions.

2.1 Rotation d'angle rationnel

Théorème 2.1.1. *Soit $\alpha \in \mathbb{Q}$. Alors, pour tout $x \in \mathbb{S}^1$, l'orbite positive $\mathcal{O}_+^{R_\alpha}(x)$ de x par la rotation R_α est finie. Autrement dit, tout point $x \in \mathbb{S}^1$ est périodique.*

Démonstration. Soit $\alpha \in \mathbb{Q}$.
On peut écrire : $\alpha = \dfrac{p}{q}$ avec $p \in \mathbb{Z}$, $q \in \mathbb{Z}^*$ et tels que $\mathrm{pgcd}(p, q) = 1$.
Soit $x \in \mathbb{S}^1$ quelconque. On a alors :

$$R_\alpha(x) = x + \frac{p}{q}$$

Mais alors :

$$R_\alpha^q(x) = x + q \cdot \frac{p}{q} = x + p = x,$$

car $p \in \mathbb{Z}$ et que l'on travaille modulo 1.

De ce fait, l'orbite positive de x par R_α est bien finie puisque $\#\mathcal{O}_+^{R_\alpha}(x) = q$. □

2.2 Rotation d'angle irrationnel

Nous allons maintenant voir que si l'angle de rotation α est irrationnel, R_α n'admet pas de points périodiques. En revanche, les orbites d'une rotation d'angle irrationnel sont équidistribuées :

Définition 2.1. *Soient $x, y \in \mathbb{S}^1$. Notons $\tilde{x}$ et $\tilde{y}$ deux relevés de x et y respectivement tels que $\tilde{y} \in [\tilde{x}, \tilde{x}+1[$. On définit alors un **intervalle** de $\mathbb{S}^1$ par :*

$$[x, y] := \pi([\tilde{x}, \tilde{y}]).$$

Définition 2.2. *Avec les notation précédentes, la **longueur** d'un intervalle I de $\mathbb{S}^1$ est définie par :*

$$|I| := \tilde{y} - \tilde{x}.$$

Remarque. On assimilera un intervalle I de $\mathbb{S}^1$ à un sous-intervalle de $[0, 1[$ en identifiant $x \in I$ à son représentant $\tilde{x}$ dans $[0, 1[$.

Définition 2.3. *Soit* $(x_n)_{n\in\mathbb{N}}$ *une suite d'éléments de* $\mathbb{S}^1$*. On dira que la suite* $(x_n)_{n\in\mathbb{N}}$ *est* ***équidistribuée*** *dans* $\mathbb{S}^1$ *si pour tout intervalle* $I \subset \mathbb{S}^1$*,*

$$\lim_{n\to+\infty} \frac{\#\{0 \leq k < n,\ x_k \in I\}}{n} = |I|.$$

Remarque. Par la suite, on identifiera naturellement une orbite et la suite des itérées qui la génèrent.

Théorème 2.2.1. (de Weyl). *Soient* $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ *et* R_α *la rotation d'angle* α*. Alors pour tout* $x \in \mathbb{S}^1$*,* $\mathcal{O}_+^{\mathcal{R}_\alpha}(x)$ *est équidistribuée dans* $\mathbb{S}^1$*.*

Démonstration. La démonstration étant longue, on va procéder en plusieurs étapes.

Étape 1 :
Cette première étape consiste en la réécriture du problème. Soit $I \subset \mathbb{S}^1$ un intervalle de la forme $[c, d]$. Posons, pour $x \in \mathbb{S}^1$:

$$T(x, n) := \#\{0 \leq k < n \ :\ R_\alpha^k(x) \in I\}.$$

On veut alors montrer que :

$$\forall x \in \mathbb{S}^1, \quad \lim_{n\to+\infty} \frac{T(x,n)}{n} = d - c.$$

Si l'on note $\mathbb{1}_I$ la fonction indicatrice de l'intervalle I, on peut écrire :

$$\forall x \in \mathbb{S}^1, \quad T(x,n) = \sum_{k=0}^{n-1} \mathbb{1}_I(R_\alpha^k(x)),$$

donc l'égalité à démontrer devient :

$$\forall x \in \mathbb{S}^1, \quad \lim_{n\to+\infty} \frac{1}{n} \sum_{k=0}^{n-1} \mathbb{1}_I(R_\alpha^k(x)) = \int_0^1 \mathbb{1}_I(s)\mathrm{d}s. \tag{1}$$

Étape 2 :
Lors de cette étape, nous allons démontrer cette formule pour φ une fonction continue quelconque de $\mathbb{S}^1$ dans lui-même. Introduisons l'ensemble :

$$\mathcal{F} := \{\varphi_m,\ m \in \mathbb{Z}\},$$

où on a posé, pour $x \in \mathbb{S}^1$, $\varphi_m(x) := e^{2i\pi m x}$.
On a alors les deux résultats suivants :

— $\mathcal{F}$ forme une base de l'espace des polynômes trigonométriques sur le cercle ;

— L'ensemble des polynômes trigonométriques est dense, pour la norme uniforme, dans l'ensemble des fonctions continues du cercle (théorème de Féjèr).

Lorsque l'on combine ces deux résultats, on constate qu'il suffit de montrer (1) seulement pour les polynômes trigonométriques $\varphi_m \in \mathcal{F}$.
Soient $m \in \mathbb{Z}$ et $x \in \mathbb{S}^1$. Alors :

$$\varphi_m(R_\alpha(x)) = e^{2i\pi m(x+\alpha)} = e^{2i\pi m\alpha} e^{2i\pi mx} = \mu_m \varphi_m(x),$$

où l'on a posé $\mu_m = e^{2i\pi m\alpha} = \varphi_m(\alpha)$.
Par récurrence sur k, on montre que :

$$\forall k \in \mathbb{N}, \quad \varphi_m(R_\alpha^k(x)) = \mu_m^k \varphi_m(x)$$

Supposons $m \neq 0$. Alors, pour tout $n \in \mathbb{N}$:

$$\sum_{k=0}^{n-1} \varphi_m(R_\alpha^k(x)) = \varphi_m(x) \sum_{k=0}^{n-1} \mu_m^k = \underbrace{\varphi_m(x) \frac{1-\mu_m^n}{1-\mu_m}}_{\text{borné}}.$$

Donc, toujours pour $m \neq 0$:

$$\lim_{n\to+\infty} \frac{1}{n} \sum_{k=0}^{n-1} \varphi_m(R_\alpha^k(x)) = 0.$$

Si maintenant $m = 0$, on a :

$$\lim_{n\to+\infty} \frac{1}{n} \sum_{k=0}^{n-1} \varphi_m(R_\alpha^k(x)) = \lim_{n\to+\infty} \frac{1}{n} \sum_{k=0}^{n-1} 1 = \lim_{n\to+\infty} \frac{n}{n} = 1.$$

De plus, on a :

$$\int_0^1 e^{2i\pi ms} \mathrm{d}s = \left\{ \begin{array}{ll} 0 & \text{si } m \neq 0 \\ 1 & \text{sinon} \end{array} \right. ,$$

et ainsi on a montré que :

$$\forall m \in \mathbb{N},\ \forall x \in \mathbb{S}^1, \quad \lim_{n\to+\infty} \frac{1}{n} \sum_{k=0}^{n-1} \varphi_m(R_\alpha^k(x)) = \int_0^1 \varphi_m(s) \mathrm{d}s.$$

Ainsi, (1) est vraie pour une base de l'ensemble des polynômes trigonométriques, donc vraie pour tous les polynômes trigonométriques. On conclut par argument de densité en se rappelant qu'une convergence uniforme permet d'intervertir limite et intégrale (le cercle $\mathbb{S}^1$ étant compact).

Étape 3 :
Il est temps de prolonger le résultat précédent à la fonction $\mathbb{1}_I$ qui n'est pas continue.
Soit $\varepsilon > 0$. Posons :

$$I_{-\varepsilon} := [c+\varepsilon, d-\varepsilon] \text{ et } I_{\varepsilon} := [c-\varepsilon, d+\varepsilon]$$

et définissons :

— $\chi_{-\varepsilon}$ la fonction plateau de support inclus dans I et valant 1 sur $I_{-\varepsilon}$;

— χ_{ε} la fonction plateau de support inclus dans I_{ε} et valant 1 sur I.

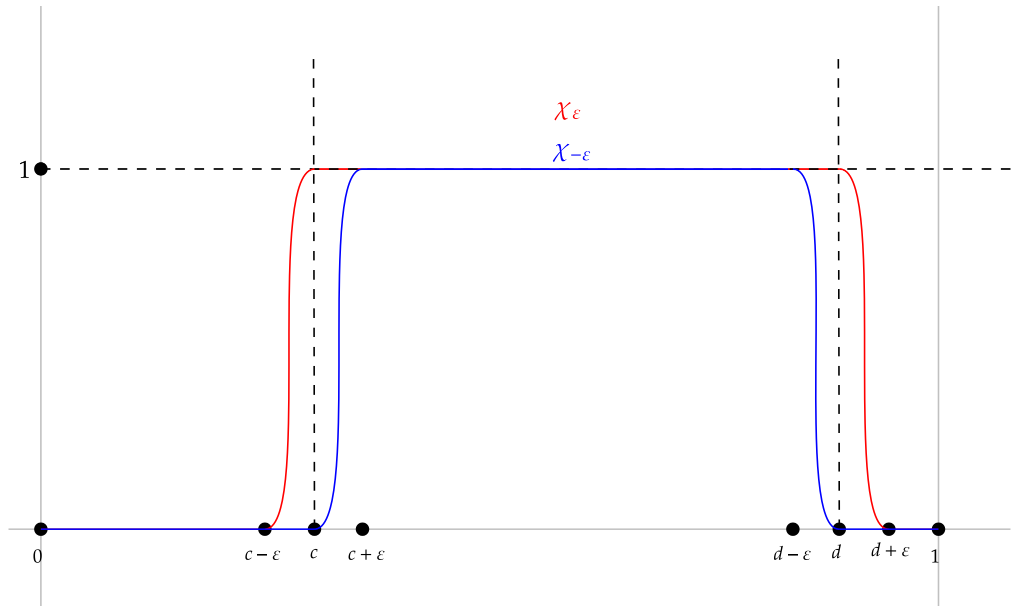

FIGURE 3 – Approximations de $\mathbb{1}_I$

On a alors :

$$\chi_{-\varepsilon} \leq \mathbb{1}_I \leq \chi_{\varepsilon}. \tag{2}$$

$$|I| - 2\varepsilon \leq \int_0^1 \chi_{-\varepsilon}(s)\mathrm{d}s \leq |I| \leq \int_0^1 \chi_{\varepsilon}(s)\mathrm{d}s \leq |I| + 2\varepsilon. \tag{3}$$

On déduit de (2) : $\forall x \in \mathbb{S}^1$, $\forall n \in \mathbb{N}^*$,

$$\frac{1}{n}\sum_{k=0}^{n-1}(\chi_{-\varepsilon} \circ R_\alpha^k)(x) \leq \frac{1}{n}\sum_{k=0}^{n-1}(\mathbb{1}_I \circ R_\alpha^k)(x) \leq \frac{1}{n}\sum_{k=0}^{n-1}(\chi_{\varepsilon} \circ R_\alpha^k)(x)$$

Les fonctions $\chi_{-\varepsilon}$ et χ_{ε} étant des fonctions continues du cercle, l'étape précédente donne :

$$\forall x \in \mathbb{S}^1 \quad \lim_{n\to+\infty} \frac{1}{n}\sum_{k=0}^{n-1} \chi_{\pm\varepsilon}(R_\alpha^k(x)) = \int_0^1 \chi_{\pm\varepsilon}(s)\mathrm{d}s.$$

Ainsi, pour tout $x \in \mathbb{S}^1$ il existe un rang $n_0 \in \mathbb{N}$ tel que pour tout $n \geq n_0$

$$
\begin{aligned}
|I| - 3\varepsilon \leq \left(\int_0^1 \chi_{-\varepsilon}(s)\mathrm{d}s\right) - \varepsilon \leq \frac{1}{n}\sum_{k=0}^{n-1}(\chi_{-\varepsilon} \circ R_\alpha^k)(x) \leq \frac{1}{n}\sum_{k=0}^{n-1}(\mathbb{1}_I \circ R_\alpha^k)(x) \\
\leq \frac{1}{n}\sum_{k=0}^{n-1}(\chi_{\varepsilon} \circ R_\alpha^k)(x) \leq \left(\int_0^1 \chi_{\varepsilon}(s)\mathrm{d}s\right) + \varepsilon \leq |I| + 3\varepsilon.
\end{aligned}
$$

Ceci étant vrai pour tout $\varepsilon > 0$, on en déduit le résultat annoncé :

$$\forall x \in \mathbb{S}^1 \qquad \lim_{n\to+\infty} \frac{1}{n}\sum_{k=0}^{n-1} \mathbb{1}_I(R_\alpha(x)) = |I|.$$

□

On termine cette partie en montrant que le théorème de Weyl implique que les orbites d'une rotation d'angle irrationnel sont denses dans le cercle.

Corollaire. *Les orbites d'une rotation d'angle irrationnel sont denses dans le cercle.*

Démonstration. Soient α irrationnel, $x \in \mathbb{S}^1$ et $\varepsilon > 0$. On pose pour tout $k \in \mathbb{N}$, $x_k = R_\alpha^k(x)$. Le théorème de Weyl nous assure que

$$\lim_{n\to+\infty} \frac{\#\{0 \leq k < n \,:\, x_k \in [x-\varepsilon, x+\varepsilon]\}}{n} = 2\varepsilon.$$

Ainsi, l'ensemble $\{0 \leq k < n \,:\, x_k \in [x-\varepsilon, x+\varepsilon]\}$ est nécessairement non vide, d'où le résultat. □

3 Les homéomorphismes du cercle

Les rotations sont loin d'être les seules fonctions intéressantes du cercle. Dans cette section nous allons étudier le cas plus général des homéomorphismes du cercle, dont on note l'ensemble par $\mathrm{Homeo}(\mathbb{S}^1)$. L'étude des rotations dans le chapitre précédent n'est cependant pas anodin : on verra qu'une grande partie des homéomorphismes du cercle sont, à conjugaison ou semi-conjugaison près, des rotations.

3.1 Définition du nombre de rotation et cas rationnel

Définition 3.1. *Si $f \in \mathrm{Homeo}(\mathbb{S}^1)$, on dira que f* ***préserve l'orientation*** *si $\deg(f) = 1$ ou, de manière équivalente, si f admet un relèvement croissant.*
On notera $\mathrm{Homeo}^+(\mathbb{S}^1)$ l'ensemble des homéomorphismes du cercle qui préservent l'orientation.

Remarque. Ces deux définitions sont bien équivalentes. Soit f un homéomorphisme du cercle. Si F est un relèvement de f, comme F est bijective, F est monotone. De plus, dire que $\deg(f) = 1$ revient à dire que, si x est un élément du cercle, $F(x+1) = F(x)+1$. Donc F est croissante. Réciproquement, on a vu que nécessairement $\deg(f) = \pm 1$. Donc si F est un relèvement croissant de f, nécessairement $F(x+1) \geq F(x)$ et donc $F(x+1) = F(x)+1$, ce qui entraîne $\deg(f) = 1$.

Théorème 3.1.1. *Soit $f \in \mathrm{Homeo}^+(\mathbb{S}^1)$ et $F : \mathbb{R} \to \mathbb{R}$ un relèvement de f. Alors pour tout $x \in \mathbb{R}$, la limite*

$$\rho(F) = \lim_{n \to +\infty} \frac{F^n(x) - x}{n}$$

existe et est indépendante de x.

Pour montrer ce théorème on va commencer par prouver un lemme plus général et qui facilitera notre démonstration.

Lemme 3.1.2. *Soit $(a_n)_{n\in\mathbb{N}}$ une famille de réels telle qu'il existe $C > 0$ satisfaisant*

$$\forall m, n \in \mathbb{N}, \quad |a_{m+n} - a_m - a_n| \leq C.$$

Alors il existe un unique $\rho \in \mathbb{R}$ tel que $(|a_n - n\rho|)_{n\in\mathbb{N}}$ soit bornée. De plus, $(\frac{a_n}{n})_{n\in\mathbb{N}}$ converge et admet ρ comme limite.

Démonstration. Pour $n \in \mathbb{N}$ on introduit l'intervalle $I_n = [\frac{a_n - C}{n}, \frac{a_n + C}{n}]$.
Avec une récurrence sur m on voit que pour tout $n, m \in \mathbb{N}$, $|a_{mn} - ma_n| \leq (m-1)C$, ce qui permet de déduire que $a_{mn} + C \leq m(a_n + C)$ et $a_{mn} - C \geq m(a_n - C)$. On en conclut donc que

$$\frac{a_{mn} + C}{mn} \leq \frac{a_n + C}{n}, \qquad \frac{a_{mn} - C}{mn} \geq \frac{a_n - C}{n},$$

puis que $I_{mn} \subset I_n$.

Donc pour tout $J \subset \mathbb{N}$ finie, $\bigcap_{n\in J} I_n \neq \varnothing$. En effet, en introduisant $\alpha = \prod_{n\in J} n$, on a $I_\alpha \subset I_n$ pour tout $n \in J$. Ainsi $(I_n)_{n\in\mathbb{N}}$ est une famille de parties de I_1, qui est compact. La contraposée du passage au complémentaire de la propriété de Borel-Lebesgue nous montre que $I = \bigcap_{n\in\mathbb{N}} I_n \neq \varnothing$.

Si $\rho \in I$, il appartient en particulier à I_n pour tout entier naturel n. Ce qui montre que $(|a_n - n\rho|)_{n\in\mathbb{N}}$ est bornée par C.
Pour ce qui est de l'unicité, si $\rho' \neq \rho$,

$$|a_n - n\rho'| = |(a_n - n\rho) + n(\rho - \rho')| \geq n|\rho - \rho'| - C,$$

dont on déduit que $(|a_n - n\rho'|)_{n\in\mathbb{N}}$ diverge vers $+\infty$.

Par ailleurs, en divisant par n la majoration de $|a_n - n\rho|$, on voit que $\lim\limits_{n\to+\infty} \dfrac{a_n}{n} = \rho$. □

Passons enfin à la démonstration du théorème :

Démonstration (du théorème 3). Soient donc $f \in \mathrm{Homeo}^+(\mathbb{S}^1)$ et $F : \mathbb{R} \to \mathbb{R}$ un relèvement de f.

On remarque dans un premier temps que l'on peut se ramener à étudier les éléments de $[0, 1[$. En effet, à l'aide de la proposition 1.2.4, si $x \in \mathbb{R}$ et $n \in \mathbb{N}$, $F^n(x) = F^n((x - \lfloor x\rfloor) + \lfloor x\rfloor) = F^n(x - \lfloor x\rfloor) + \lfloor x\rfloor$ et de plus

$$\lim_{n\to+\infty} \frac{\lfloor x\rfloor}{n} = 0.$$

Ainsi, si $x, y \in [0, 1[$ et $n \in \mathbb{N}$, comme F^n est croissante et $\deg(f^n) = 1$, $|x - y| \leq 1 \Rightarrow |F^n(x) - F^n(y)| \leq 1$. L'inégalité triangulaire nous donne donc

$$\big||F^n(x) - x| - |F^n(y) - y|\big| \leq 2. \tag{4}$$

Ainsi, $\lim\limits_{n\to+\infty} \frac{1}{n}\big||F^n(x) - x| - |F^n(y) - y|\big| = 0$. Si une telle limite existe, elle est donc bien indépendante de x.
On se donne définitivement $x_0 \in [0, 1[$ et on pose $a_n = F^n(x_0) - x_0$. En utilisant (4) on trouve que

$$\begin{aligned}|a_{m+n} - a_m - a_n| &\leq |F^{m+n}(x_0) - x_0 - F^m(x_0) + x_0 - F^n(x_0) + x_0| \\ &\leq \big||F^m(F^n(x_0)) - F^n(x_0)| - |F^m(x_0) - x_0|\big| \leq 2.\end{aligned}$$

La suite $(a_n)_{n\in\mathbb{N}}$ vérifie donc les hypothèses du lemme précédent. Il existe donc un unique ρ tel que $(\frac{a_n}{n})_{n\in\mathbb{N}}$ converge vers ρ. □

Il est intéressant de remarquer qu'un cas de figure ne nécessite pas tout cet attirail : si f admet un point de périodicité. Dans ce cas, il est aisé de montrer la convergence de la suite, et on peut même déterminer la valeur de sa limite.

Proposition 3.1.3. *Soient $f \in \text{Homeo}^+(\mathbb{S}^1)$ et $F : \mathbb{R} \to \mathbb{R}$ un de ses relèvements. S'il existe $q \in \mathbb{N}$ et $x_0 \in \mathbb{S}^1$ tels que $f^q(x_0) = x_0$, il existe alors $p \in \mathbb{Z}$ tel que $\rho(F) = \frac{p}{q}$.*

Démonstration. Soient $q \in \mathbb{N}$ et $x_0 \in \mathbb{S}^1$ tels qu'énoncés. Soit $\tilde{x_0} \in \mathbb{R}$ un représentant de x_0. Pour la convergence, on se rappelle que F^q est un relèvement de f^q,

$$\pi(F^q(\tilde{x_0})) = \pi(F^q(\pi(\tilde{x_0})) + \lfloor \tilde{x_0} \rfloor) = f^q(\pi(\tilde{x_0})) = \pi(\tilde{x_0}).$$

Ainsi, par additivité de π, on voit que $p = F^q(\tilde{x_0}) - \tilde{x_0} \in \mathbb{Z}$.

Soit $n \in \mathbb{N}$. On peut en faire la division euclidienne par q. Il existe donc $m \in \mathbb{Z}$ et $0 \leq r < q$ tels que $n = mq + r$. D'où

$$\frac{F^n(\tilde{x_0}) - \tilde{x_0}}{n} = \frac{F^r \circ F^q(F^q \cdots F^q(\tilde{x_0})) \cdots) - \tilde{x_0}}{n} = \frac{F^r(\tilde{x_0}) + mp - \tilde{x_0}}{mq + r}.$$

$F^r(\tilde{x_0})$ ne prenant qu'un nombre fini de valeurs, ce quotient tend vers $\frac{p}{q}$ lorsque n tend vers l'infini. □

Si $\rho(F)$ dépend du relèvement choisit, cela peut poser problème. En effet, l'information apportée par les nombres de rotation des relèvements n'ont, a priori, aucune raison de caractériser un homéomorphisme. Dans les faits, la remarque suivante montre que ce n'est pas un problème.

Proposition 3.1.4. *Soient $f \in \text{Homeo}^+(\mathbb{S}^1)$ et $F_1, F_2 : \mathbb{R} \to \mathbb{R}$ deux de ses relèvements. Alors $\rho(F_1) - \rho(F_2) \in \mathbb{Z}$.*

Démonstration. On a déjà vu qu'il existe $k \in \mathbb{Z}$ tel que $F_1 = F_2 + k$. Si $x \in \mathbb{R}$, $n \in \mathbb{N}$,

$$\rho(F_1) = \lim_{n\to+\infty} \frac{F_1^n(x) - x}{n} = \lim_{n\to+\infty} \frac{F_2^n(x) + nk - x}{n} = \lim_{n\to+\infty} \frac{F_2^n(x) - x}{n} + k = \rho(F_2) + k$$

□

Définition 3.2. *Si $f \in \text{Homeo}^+(\mathbb{S}^1)$ et $F : \mathbb{R} \to \mathbb{R}$ est un de ses relèvements, on définit le **nombre de rotation** de f comme étant :*

$$\rho(f) := \rho(F) \; mod \; 1$$

.

Une première remarque intéressante est de constater que le nombre de rotation est invariant par conjugaison topologique.

Proposition 3.1.5. *Soient f et h des homéomorphismes du cercle préservant l'orientation. On alors*

$$\rho(f) = \rho(h \circ f \circ h^{-1}).$$

Démonstration. Soient F et H des relevés de f et h. En utilisant les propositions précédentes, $H \circ F \circ H^{-1}$ est un relevé de $h \circ f \circ h^{-1}$.
Soit maintenant $x \in \mathbb{R}$.

$$\begin{aligned}\frac{(H \circ F \circ H^{-1})^n(x) - x}{n} &= \frac{(H \circ F^n \circ H^{-1})(x) - x}{n} \\ &= \frac{(H \circ F^n \circ H^{-1}(x))(x) - F^n \circ H^{-1}(x)}{n} + \frac{F^n \circ H^{-1}(x) - H^{-1}(x)}{n} \\ &+ \frac{H^{-1}(x) - x}{n}.\end{aligned}$$

Il a déjà été évoqué que l'application qui à y associe $H(y) - y$ est bornée. Ainsi, le numérateur du premier et du troisième terme étant bornés indépendamment de n, la limite des deux quotient est nul. On a finalement

$$\rho(H \circ F \circ H^{-1}) = \lim_{n \to +\infty} \frac{F^n \circ H^{-1}(x) - H^{-1}(x)}{n} = \rho(F).$$

En passant modulo 1 on trouve le résultat annoncé. □

Proposition 3.1.6. *Soit $f \in \mathrm{Homeo}^+(\mathbb{S}^1)$. Si $\rho(f)$ est rationnel, f admet un point périodique.*

Démonstration. On commence par remarquer que, si $m \in \mathbb{N}$,

$$\rho(F^m) = \lim_{n \to +\infty} \frac{F^{mn}(x) - x}{n} = m \times \lim_{n \to +\infty} \frac{F^{mn}(x) - x}{mn} = m\rho(F),$$

où F est un relèvement de f.

Ainsi, il suffit de montrer que la proposition est vraie dans le cas $\rho(f) = 0$. En effet, si $\rho(f) = \frac{p}{q}$ avec p et q des entiers, $\rho(f^q) = q\rho(f)\ mod\ 1 = 0$ et il est assez clair que si f^q admet un point périodique, f en admet un.

Soit donc f telle que $\rho(f) = 0$. On décide de raisonner par l'absurde : on suppose que f n'admet pas de point périodique, donc en particulier pas de point fixe. Il existe donc $F : \mathbb{R} \to \mathbb{R}$ un relèvement de f tel que $F(0) \in]0, 1[$. 0 et 1 sont exclus car F n'admet pas de point fixe.

Notons $g : x \in \mathbb{R} \mapsto F(x) - x$. La fonction g est continue et ne peut pas prendre de valeurs dans $\mathbb{Z}$, sinon f aurait un point de périodicité. De plus, $g(0) \in]0,1[$, donc $g(x) \in]0,1[$ $\forall x \in \mathbb{R}$.
On peut aussi voir que g est $\mathbb{Z}$-périodique. Par le théorème des bornes atteintes il existe $m, M > 0$ tels que pour tout $x \in]0,1[$, $0 < m < g(x) < M < 1$. La périodicité nous permet d'étendre cet encadrement à tout $\mathbb{R}$.

On peut sommer cet encadrement pour avoir une somme télescopique :

$$nm < \sum_{k=0}^{n-1} g(F^k(0)) = F^n(0) < nM.$$

Ce qui, en divisant par n puis prenant la limite en l'infini donne :

$$0 < m \leq \rho(F) \leq M < 1.$$

On en déduit donc que $\rho(f) \neq 0$, ce qui est absurde. □

Notons que grâce aux propositions 3.1.3 et 3.1.6, on a montré la proposition suivante :

Proposition 3.1.7. *Soit $f \in \mathrm{Homeo}^+(\mathbb{S}^1)$. Alors f admet un point périodique si, et seulement si, son nombre de rotation est rationnel.*

3.2 Cas irrationnel et classification de Poincaré

Nous avons déjà vu que le nombre de rotation était un invariant de conjugaison topologique. Nous allons maintenant montrer que dans le cas où le nombre de rotation ρ est irrationnel, l'homéomorphisme est toujours semi-conjugué à la rotation d'angle ρ et dans un certain nombre de cas, il y est même conjugué.

Lemme 3.2.1. *Soit $f \in \mathrm{Homeo}^+(\mathbb{S}^1)$ de nombre de rotation $\rho(f)$ irrationnel. Soit $x \in \mathbb{S}^1$ et soit $n \in \mathbb{N}^*$. Alors, l'intersection de toute orbite positive de f avec l'intervalle $I = [x, f^n(x)]$ est non vide.*

Démonstration. On veut montrer que pour tout $y \in \mathbb{S}^1$, $\mathcal{O}_+^f(y) \cap I \neq \varnothing$, c'est-à-dire qu'il existe $p \in \mathbb{N}$ tel que $f^p(y) \in I$. Cela équivaut à montrer que pour tout $y \in \mathbb{S}^1$, il existe $p \in \mathbb{N}$ tel que $y \in f^{-p}(I)$. Il suffit donc de montrer que :

$$\mathbb{S}^1 = \bigcup_{k=0}^{\infty} f^{-k}(I).$$

Supposons par l'absurde que ça ne soit pas le cas. Alors en particulier, on a :

$$\mathbb{S}^1 \not\subset \bigcup_{p=0}^{\infty} f^{-pn}(I) = \bigcup_{p=0}^{\infty} [f^{-pn}(x), f^{-(p-1)n}(x)].$$

Pour tout $p \in \mathbb{N}$, on pose $I_p = [f^{-pn}(x), f^{-(p-1)n}(x)]$. On remarque que, pour tout $p \in \mathbb{N}$, I_p et I_{p+1} sont adjacents (on entend par là que les intervalles I_p et I_{p+1} ont une borne en commun).

Notons a_0 un antécédent par π de x, et a_1 l'antécédent par π de $f^n(x)$ appartenant à $[a_0, a_0+1[$. Par les propriétés des relèvements vues en sous-section 1.2, il existe un unique relèvement F de f^n tel que $F(a_0) = a_1$. Posons alors, pour tout $p \in \mathbb{Z}$, $a_p = F^p(a_0)$.
Comme $f^n \in \mathrm{Homeo}^+(\mathbb{S}^1)$, F est strictement croissante et donc F^{-1} aussi. Comme de plus $a_0 \leq a_1$, la suite $(a_{-p})_{p\in\mathbb{N}}$ est décroissante.
Par ailleurs, d'après la définition d'un intervalle du cercle, $I = \pi([a_0, a_1])$. Par récurrence, on obtient que pour tout p dans $\mathbb{N}$, $I_p = \pi([a_{-p}, a_{-(p-1)}])$. Du fait que la réunion des I_p, pour $p \in \mathbb{N}$, ne recouvre pas le cercle, la réunion des $[a_{-p}, a_{-(p-1)}]$ ne recouvre pas $]a_0 - 1, a_0]$. Donc la suite $(a_{-p})_{p\in\mathbb{N}}$ est minorée par $a_0 - 1$. Donc la suite $(a_{-p})_{p\in\mathbb{N}}$ converge vers un certain a dans $\mathbb{R}$.

Par continuité de π, la suite $(f^{-pn}(x))_{p\in\mathbb{N}}$ converge dans le cercle vers un certain $z \in \mathbb{S}^1$. Comme

$$\forall p \in \mathbb{N}, \quad f^{-(p+1)n}(x) = f^{-n}(f^{-pn}(x)),$$

par passage à la limite, on obtient $z = f^{-n}(z)$. Ainsi z est un point périodique de f^{-n}, ce qui contredit l'irrationalité du nombre de rotation de f d'après la proposition 3.1.3. □

Remarque. En appliquant le lemme précédent à $f^m(x)$ pour un certain $m \in \mathbb{Z}$, on obtient une deuxième version plus générale :

Lemme 3.2.2. *Soit $f \in \mathrm{Homeo}^+(\mathbb{S}^1)$ de nombre de rotation $\rho(f)$ irrationnel. Soit $x \in \mathbb{S}^1$ et soient $m, n \in \mathbb{Z}$ tels que $m > n$. Alors l'intersection de toute orbite positive de f avec l'intervalle $I = [f^n(x), f^m(x)]$ est non vide.*

Proposition 3.2.3. *Soit $f \in \mathrm{Homeo}^+(\mathbb{S}^1)$. Si $\rho(f)$ est irrationnel, alors pour tout points $x, y \in \mathbb{S}^1$, $\overline{\omega}(x) = \overline{\omega}(y)$. De plus, pour tout $x, y \in \mathbb{S}^1$:*

- *Ou bien $\overline{\omega}(x) = \mathbb{S}^1$,*
- *Ou bien $\overline{\omega}(x)$ est parfait, i.e. fermé sans point isolé, et nulle part dense, i.e. son adhérence est d'intérieur vide.*

Démonstration. Soient $x, y \in \mathbb{S}^1$. Montrons tout d'abord que $\overline{\omega}(x) = \overline{\omega}(y)$.

Soit $x_0 \in \overline{\omega}(x)$. Soit $(a_n)_{n\in\mathbb{N}}$ une suite strictement croissante telle que $(f^{a_n}(x))_{n\in\mathbb{N}}$ converge vers x_0. D'après le lemme précédent, il existe $b_1 \in \mathbb{N}$ tel que $f^{b_1}(y) \in [f^{a_0}(x), f^{a_1}(x)]$. Toujours d'après le lemme précédent, en supposant construit les k premiers termes de la suite $(b_n)_{n\in\mathbb{N}}$, il existe $c_{k+1} \in \mathbb{N}$ tel que

$$f^{c_{k+1}}(f^{b_k+1}(y)) \in [f^{a_k}(x), f^{a_{k+1}}(x)].$$

Posons alors $b_{k+1} = b_k + 1 + c_{k+1}$. On a ainsi construit par récurrence une suite $(b_n)_{n\in\mathbb{N}}$, strictement croissante par construction. Par encadrement, la suite $(f^{b_n}(y))_{n\in\mathbb{N}}$ converge vers x_0 et donc $x_0 \in \overline{\omega}(y)$.
Ceci étant vrai pour tout $x_0 \in \overline{\omega}(x)$, $\overline{\omega}(x) \subset \overline{\omega}(y)$. Par symétrie, $\overline{\omega}(x) = \overline{\omega}(y)$.

Montrons maintenant que $\overline{\omega}(x)$ est parfait. D'abord, notons que $\overline{\omega}(x)$ est fermé en tant qu'intersection de fermés.
Ensuite, soit $z \in \overline{\omega}(x)$. Montrons que z n'est pas isolé, c'est à dire qu'il existe une suite de $\overline{\omega}(x)$ ne prenant pas la valeur z et qui tend vers z. Comme $\overline{\omega}(x) = \overline{\omega}(z)$ d'après ce que l'on vient de faire, on a $z \in \overline{\omega}(z)$. Donc il existe une suite strictement croissante $(n_k)_{k\in\mathbb{N}}$ telle que $(f^{n_k}(z))_{k\in\mathbb{N}}$ converge vers z.
De plus, pour tout $k \in \mathbb{N}$, $f^{n_k}(z) \neq z$. Sinon, z serait un point périodique de f, ce qui contredirait l'irrationalité de $\rho(f)$. Comme $\overline{\omega}(x)$ est invariant par f, pour tout $k \in \mathbb{N}$, $f^{n_k}(z) \in \overline{\omega}(x)$. Donc z est non isolé.

Supposons à présent que $\overline{\omega}(x) \neq \mathbb{S}^1$. Montrons que $\overline{\omega}(x)$ est nulle part dense, ce qui revient ici à montrer que $\overline{\omega}(x)$ est d'intérieur vide.
On considère la frontière de $\overline{\omega}(x)$, que l'on note $\partial\overline{\omega}(x)$. Cet ensemble est fermé. En effet :

$$\partial\overline{\omega}(x) = \overline{\omega}(x) \cap (\mathbb{S}^1 \setminus \overset{\circ}{\widehat{\overline{\omega}(x)}}).$$

De plus, cet ensemble est non vide. En effet, supposons par l'absurde qu'il le soit. On aurait :

$$\mathbb{S}^1 = \partial\overline{\omega}(x) \sqcup \overset{\circ}{\widehat{\overline{\omega}(x)}} \sqcup (\mathbb{S}^1 \setminus \overline{\omega}(x)).$$

Donc :

$$\mathbb{S}^1 = \overset{\circ}{\widehat{\overline{\omega}(x)}} \sqcup (\mathbb{S}^1 \setminus \overline{\omega}(x)).$$

Ainsi $\mathbb{S}^1$ est réunion disjointe de deux ouverts non vides (car $\overline{\omega}(x) \neq \mathbb{S}^1$) ce qui est absurde car $\mathbb{S}^1$ est connexe.
De plus, comme f est un homéomorphisme de $\mathbb{S}^1$ et que $\overline{\omega}(x)$ est invariant par f, on a :

$$f(\partial\overline{\omega}(x)) = \partial f(\overline{\omega}(x)) = \partial\overline{\omega}(x).$$

Donc $\partial\overline{\omega}(x)$ est invariante par f.
Soit $z \in \partial\overline{\omega}(x)$. Comme $\partial\overline{\omega}(x)$ est invariante par f, on a $\{f^n(z), n \in \mathbb{N}\} \subset \partial\overline{\omega}(x)$.
De plus, comme $\partial\overline{\omega}(x)$ est fermé, on a l'inclusion $\overline{\omega}(z) \subset \partial\overline{\omega}(x)$. Or, $\overline{\omega}(z) = \overline{\omega}(x)$.
Donc $\overline{\omega}(x) \subset \partial\overline{\omega}(x)$, ce qui signifie précisément que $\overline{\omega}(x)$ est d'intérieur vide. □

Lemme 3.2.4. *Soit $f \in \mathrm{Homeo}^+(\mathbb{S}^1)$ tel que $\rho(f)$ soit irrationnel. Soit F un relèvement de f, de nombre de rotation ρ. Soient $x \in \mathbb{R}$ et $(m_1, m_2, n_1, n_2) \in \mathbb{Z}^4$. Alors*

$$n_1\rho + m_1 < n_2\rho + m_2 \iff F^{n_1}(x) + m_1 < F^{n_2}(x) + m_2.$$

Démonstration. On commence par remarquer que si $n_1 = n_2$, l'équivalence est une tautologie. On supposera donc $n_1 \neq n_2$ dans la suite de la preuve.
Supposons que $F^{n_1}(x) + m_1 < F^{n_2}(x) + m_2$. Alors, en appliquant F^{-n_2} à cette inégalité, on obtient :

$$F^{n_1-n_2}(x) < x + m_2 - m_1,$$

car f préserve l'orientation.
De plus, cette inégalité est vraie pour tout $x \in \mathbb{R}$. En effet, supposons par l'absurde qu'il existe $y \in \mathbb{R}$ tel que $F^{n_1}(y) + m_1 \geq F^{n_2}(y) + m_2$. Alors, par continuité de F et théorème des valeurs intermédiaires, il existe $z \in \mathbb{R}$ tel que $F^{n_1}(z) + m_1 = F^{n_2}(z) + m_2$. Donc $\pi(F^{n_1}(z)) = \pi(F^{n_2}(z))$. Donc $f^{n_1}(\pi(z)) = f^{n_2}(\pi(z))$. Donc $\pi(z)$ est un point périodique de f (car $n_1 \neq n_2$), ce qui contredit l'irrationalité de $\rho(f)$.
En particulier, pour $x = 0$, on a :

$$F^{n_1-n_2}(0) < m_2 - m_1.$$

Par récurrence, on obtient :

$$\forall k \in \mathbb{N}^*, F^{k(n_1-n_2)}(0) < k(m_2 - m_1).$$

On a donc deux cas :

— Ou bien $n_1 - n_2 > 0$. Alors :

$$\frac{F^{n_1-n_2}(0) - 0}{k(n_1 - n_2)} < \frac{m_2 - m_1}{n_1 - n_2}.$$

Donc :

$$\rho \leq \frac{m_2 - m_1}{n_1 - n_2}.$$

Cette inégalité est en fait stricte, sinon ρ est rationnel.
Donc $n_1\rho + m_1 < n_2\rho + m_2$.

— Ou bien $n_1 - n_2 < 0$. Alors :

$$\frac{F^{n_1-n_2}(0) - 0}{k(n_1 - n_2)} > \frac{m_2 - m_1}{n_1 - n_2}.$$

Donc :

$$\rho \geq \frac{m_2 - m_1}{n_1 - n_2}.$$

Comme au cas précédent, cette inégalité est en fait stricte.
Donc, comme $n_1 - n_2 < 0$, $n_1\rho + m_1 < n_2\rho + m_2$.

Supposons maintenant que $F^{n_1}(x) + m_1 \geq F^{n_2}(x) + m_2$. En reprenant le même raisonnement, on obtient :

$$n_1\rho + m_1 \geq n_2\rho + m_2.$$

□

Théorème 3.2.5. (Classification de Poincaré). *Soit $f \in \mathrm{Homeo}^+(\mathbb{S}^1)$ de nombre de rotation ρ irrationnel. Alors il existe une application $h : \mathbb{S}^1 \to \mathbb{S}^1$ continue, surjective et croissante (i.e. dont l'un des relèvements est croissant) h de $\mathbb{S}^1$ tel que $h \circ f = R_\rho \circ h$.*

Si, de plus, f est topologiquement transitif, alors h est un homéomorphisme et $f = h^{-1} \circ R_\rho \circ h$, autrement dit f est topologiquement conjugué à R_ρ.

Démonstration. Soient F un relèvement de f et F_ρ un relèvement de R_ρ.

On cherche une application $h : \mathbb{S}^1 \to \mathbb{S}^1$, continue et monotone, telle que $h \circ f = R_\rho \circ h$. Cela revient à trouver un relèvement monotone $H : \mathbb{R} \to \mathbb{R}$ tel que $H \circ F = F_\rho \circ H$ que l'on passera au quotient par la suite..

Soit $x_0 \in \mathbb{R}$. Posons $A = \{F^n(x_0) + m \ : \ n, m \in \mathbb{Z}\}$ et $B = \{n\rho + m \ : \ n, m \in \mathbb{Z}\}$. On remarque que B est de la forme $\mathbb{Z}\alpha + \mathbb{Z}$ où α est irrationnel. Donc B est dense dans $\mathbb{R}$.

On définit $H : A \to B$ par $H(F^n(x_0) + m) = n\rho + m$. D'après le lemme précédent, H est bijective et croissante. On prolonge alors H à $\mathbb{R}$ en posant :

$$\forall y \in \mathbb{R}, \quad H(y) = \sup\{n\rho + m \ : \ F^n(x_0) + m < y\}.$$

On remarque que l'on a aussi :

$$\forall y \in \mathbb{R}, \quad H(y) = \inf\{n\rho + m \ : \ F^n(x_0) + m > y\},$$

sinon $\mathbb{R} \setminus B$ contiendrait un intervalle, ce qui contredirait la densité de B.
Cette définition de H coïncide avec la définition précédente sur A. En effet, soit $F^{n_0}(x_0) + m_0 \in A$.

— Si $n\rho + m$ est tel que $F^n(x_0) + m < F^{n_0}(x_0) + m_0$, alors, par le lemme 3.2.4 :

$$n\rho + m < n_0\rho + m_0.$$

Donc :

$$\sup\{n\rho + m \ : \ F^n(x_0) + m < F^{n_0}(x_0) + m_0\} \leq n_0\rho + m_0.$$

— De même, si $n\rho + m$ est tel que $F^n(x_0) + m > F^{n_0}(x_0) + m_0$, on a, par le lemme 3.2.4 :

$$n\rho + m > n_0\rho + m_0.$$

Donc :

$$\inf\{n\rho + m \ : \ F^n(x_0) + m > F^{n_0}(x_0) + m_0\} \geq n_0\rho + m_0.$$

Donc :

$$\sup\{n\rho+m : F^n(x_0)+m < F^{n_0}(x_0)+m_0\} = \inf\{n\rho+m : F^n(x_0)+m > F^{n_0}(x_0)+m_0\} = n_0\rho+m_0.$$

Montrons tout d'abord que H est croissante.
Soient $x, y \in \mathbb{R}$ tels que $x \leq y$. Alors :

$$\{n\rho + m \ : \ F^n(x_0) + m < x\} \subset \{n\rho + m \ : \ F^n(x_0) + m < y\}.$$

Donc :

$$\sup\{n\rho + m \ : \ F^n(x_0) + m < x\} \leq \sup\{n\rho + m \ : \ F^n(x_0) + m < y\}.$$

Donc $H(x) \leq H(y)$.

Montrons à présent que H est surjective. Soit $y \in \mathbb{R}$. Comme B est dense dans $\mathbb{R}$, il existe une suite croissante $(b_k)_{k\in\mathbb{N}}$ de B qui converge vers y. Notons que les termes de cette suite sont de la forme $n_k\rho + m_k$. Puisque cette suite est croissante, en utilisant à nouveau le lemme 3.2.4, on obtient que l'ensemble $\{F^{n_k}(x_0) + m_k \ : \ k \in \mathbb{N}\}$ est majoré par tous les éléments de la forme $F^n(x_0) + m$ tels que $n\rho + m > y$.
Posons $x = \sup\{F^{n_k}(x_0) + m_k \ : \ k \in \mathbb{N}\}$. Alors on a :

$$H(x) = \sup\{n\rho + m \ : \ F^n(x_0) + m < x\}.$$

Or, si $n\rho+m$ est tel que $F^n(x_0)+m < x$, on peut fixer un entier $k \in \mathbb{N}$ tel que $F^n(x_0)+m \leq F^{n_k}(x_0) + m_k$. On a alors, par croissance de H :

$$n\rho + m = H(F^n(x_0) + m) \leq H(F^{n_k}(x_0) + m_k) = n_k\rho + m_k.$$

Or :

$$H(F^{n_k}(x_0) + m_k) \leq \sup_{k\in\mathbb{N}} H(F^{n_k}(x_0) + m_k) = \sup_{k\in\mathbb{N}} b_k = y.$$

On a donc, pour tout $n\rho + m$ tel que $F^n(x_0) + m < x$:

$$n\rho + m \leq y.$$

Donc :

$$H(x) = \sup \ \{n\rho + m, \ F^n(x_0) + m < x\} \leq y.$$

De plus, on a aussi :

$$H(x) = \inf \ \{n\rho + m, \ F^n(x_0) + m > x\}.$$

Le même argument donne alors :

$$H(x) \geq y.$$

Donc $H(x) = y$, et H est surjective.

Montrons maintenant que H est continue. Pour cela, montrons que toute application de $\mathbb{R}$ dans $\mathbb{R}$ surjective et croissante est continue. Soit $f : \mathbb{R} \to \mathbb{R}$ une fonction surjective et croissante. Supposons par l'absurde qu'il existe un point $x \in \mathbb{R}$ tel que f ne soit pas continue en x.

— Ou bien f n'est pas continue à droite en x. Alors :

$$f(x) \neq \lim_{y \to x^+} f(y).$$

Par croissance de f, on a

$$\lim_{y \to x^+} f(y) = \inf_{y > x} f(y).$$

Soit z dans l'intervalle $\left] f(x), \inf_{y>x} f(y) \right[$. Par surjectivité de f, il existe $t \in \mathbb{R}$ tel que $f(t) = z$. Comme f est croissante et comme $f(t) \neq f(x)$, on a $t > x$. On a donc trouvé $t > x$ tel que $f(t) < \inf_{y>x} f(y)$, ce qui est absurde.

— Ou bien f n'est pas continue à gauche en x. Un raisonnement similaire donne également une contradiction.

On a ainsi montré que f est continue.
Comme H est croissante et surjective de $\mathbb{R}$ dans $\mathbb{R}$, elle est continue.

Montrons que H passe au quotient. Soit $x \in \mathbb{R}$.

$$\begin{aligned} H(x+1) &= \sup\{n\rho + m \ : \ F^n(x_0) + m < x + 1\} \\ &= \sup\{n\rho + m \ : \ F^n(x_0) + m - 1 < x\} \\ &= \sup\{n\rho + m + 1 \ : \ F^n(x_0) + m < x\} \\ &= \sup\{n\rho + m \ : \ F^n(x_0) + m < x\} + 1 \\ &= H(x) + 1. \end{aligned}$$

Donc H passe au quotient et induit une application $h : \mathbb{S}^1 \to \mathbb{S}^1$ continue, croissante et surjective.

Montrons que $H \circ F = F_\rho \circ H$. Soit $x \in \mathbb{R}$.

$$\begin{aligned} H(F(x)) &= \sup\{n\rho + m \ : \ F^n(x_0) + m < F(x)\} \\ &= \sup\{n\rho + m \ : \ F^{n-1}(x_0) + m < x\} \\ &= \sup\{(n+1)\rho + m \ : \ F^n(x_0) + m < x\} \\ &= \sup\{n\rho + m \ : \ F^n(x_0) + m < x\} + \rho \\ &= H(x) + \rho. \end{aligned}$$

Donc $H \circ F = F_\rho \circ H$.

Montrons pour finir que $h \circ f = R_\rho \circ h$. On sait que l'on a $H \circ F = F_\rho \circ H$. En composant par la surjection canonique, on a $\pi \circ H \circ F = \pi \circ F_\rho \circ H$. Puisque l'on a montré que H est un relèvement de h, il vient $h \circ \pi \circ F = R_\rho \circ \pi \circ H$. Donc $h \circ f \circ \pi = R_\rho \circ h \circ \pi$. Finalement, comme π est surjective, on a : $h \circ f = R_\rho \circ h$.

Montrons maintenant la deuxième partie du théorème en supposant de plus que f est transitive. Soit $x \in \mathbb{S}^1$. Comme f est transitive, A est dense dans $\mathbb{R}$ (la réciproque est vraie). H est constante sur les intervalles de $\mathbb{R} \setminus A$. En effet, soit $I \subset \mathbb{R} \setminus A$ un intervalle non vide. Soient x et y des éléments de I. Alors par hypothèse

$$\{n\rho + m \ : \ F^n(x_0) + m < y\} = \{n\rho + m \ : \ F^n(x_0) + m < x\}.$$

Les valeurs de H en x et y étant un sup sur ces ensembles, ces deux valeurs sont égales. Évidemment, H ne peut pas être constante sur des intervalles qui ne sont pas entièrement contenues dans $\mathbb{R}\setminus A$, car $H_{|A}$ est injective. Comme H est monotone, dire que H est injective revient à dire que H n'est constante sur aucun intervalle. En combinant ces remarques, on aboutit au fait que h est injective si, et seulement si, f est transitive. En sachant que h est tout le temps continue et surjective, l'injectivité en fait un homéomorphisme, ce qui conclut cette preuve. $\square$

4 Les $\mathcal{C}^1$-difféomorphismes du cercle

La classification de Poincaré, qui a été énoncée et démontrée juste au dessus, est en fait la première étape de la démonstration d'un théorème plus précis, le théorème de Denjoy. Ledit théorème permettant d'avoir un résultat plus fort que la classification de Poincaré, pourvu que notre homéomorphisme possède de meilleurs hypothèses de régularité.
On commence par se donner un nouveau moyen de quantifier la régularité des fonctions, que nous n'avons pas croisé jusqu'à présent.

4.1 Théorème de Denjoy

Définition 4.1. *Soit* $f : \mathbb{S}^1 \to \mathbb{R}$*. On définit la* ***variation*** *de* f *comme étant*

$$\mathrm{Var}(f) = \sup \sum_{k=1}^{n} |f(x_k) - f(x_{k+1})|,$$

où le supremum est pris sur toutes les partitions strictement croissantes de $[0,1]$*, d'extrémités* x_k *et* x_{k+1}*. On dira alors que* f *est à variation bornée si* $\mathrm{Var}(f)$ *est finie.*

Remarque. Il est intéressant de noter que toute fonction $\mathcal{C}^1$ est à variation bornée.

Théorème 4.1.1. (de Denjoy). *Soit* f *un* $\mathcal{C}^1$*-difféomorphisme de nombre de rotation* ρ *irrationnel. Si* f' *se trouve être à variation bornée alors* f *est topologiquement conjuguée à la rotation* R_ρ*. Autrement dit, il existe un homéomorphisme* h *tel que* $f = h \circ R_\rho \circ h^{-1}$*.*

Remarque. La remarque précédente permet de voir qu'en particulier, être $\mathcal{C}^2$ est suffisant.

Avant de montrer le théorème de Denjoy, énonçons le lemme suivant qui nous sera utile.

Lemme 4.1.2. *Soient* J *un intervalle ouvert de* $\mathbb{S}^1$ *et* n *un entier tels que les ensembles* J*,* $f(J)$*,...,* $f^n(J)$ *(qui sont des intervalles grâce à la continuité de* f*) soient disjoints. Soient de plus* x *et* y *des éléments de* J*. Alors,*

$$\mathrm{Var}(\log(f')) \geq |\log((f^n)')(x) - \log((f^n)')(y)|.$$

Comme expliqué en introduction, la majorité du travail a déjà été fait. En effet, si f est transitive, la classification de Poincaré permet de conclure quant à la conjugaison de f et R_ρ. Supposons donc que f n'est pas transitive et attelons-nous à montrer une contradiction.

Démonstration (du lemme 4.1.2). Dans la définition de la variation d'une fonction, le supremum est pris sur les partitions du cercle. Avec l'hypothèse du lemme, on peut compléter la famille des $[f^k(x), f^k(y)]$, $0 \leq k \leq n$, en une partition du cercle. On en déduit ainsi les inégalités suivantes, en ayant noté $g = \log(f')$:

$$\begin{aligned}\mathrm{Var}(g) &\geq \sum_{k=0}^{n-1} |g(f^k(x)) - g(f^k(y))| \geq \Big|\sum_{k=0}^{n-1} g(f^k(x)) - g(f^k(y))\Big| \\ &= \Big|\log\big(\prod_{k=0}^{n-1} f'(f^k(x))\big) - \log\big(\prod_{k=0}^{n-1} f'(f^k(y))\big)\Big| \\ &= \big|\log((f^n)')(x) - \log((f^n)')(y)\big|,\end{aligned}$$

la dernière égalité se démontrant par récurrence sur n en remarquant, grâce à la formule de dérivation composée, que $(f^n)' = (f^{n-1})' \cdot f'(f^{n-1})$. $\square$

Démonstration (du théorème de Denjoy). Repassons à la démonstration du théorème de Denjoy. En reprenant le résultat de la proposition 3.2.3, $\omega(0)$ est parfait et nul part dense. On en déduit donc que $\mathbb{S}^1 \backslash \omega(0)$ s'écrit comme réunion disjointe d'intervalles ouverts. Soit $I =]a, b[$ un des ces intervalles. On remarque maintenant que les intervalles de la famille $(f^n(I))_{n \in \mathbb{Z}}$ sont deux à deux disjoints. Si ce n'était pas le cas, f aurait un point périodique. Supposons en effet que $f^n(I)$ et $f^m(I)$ ne soient pas disjoints, n et m étant des entiers. Ces deux ensembles sont des composantes connexes de $\mathbb{S}^1 \backslash \omega(0)$, leur intersection n'étant pas vide, elles sont égales. On en déduit ainsi la périodicité des extrémités de I grâce à la continuité de f et du fait qu'elle préserve l'orientation. On aboutit finalement au fait que

$$\sum_{n \in \mathbb{Z}} \ell(f^n(I)) \leq 1,$$

où $\ell(f^n(I))$ désigne la longueur de l'intervalle $f^n(I)$, que l'on peut définir comme $\ell(f^n(I)) = \int_a^b (f^n)'(t) \mathrm{d}t$. Ce résultat nous servira plus tard.

Fixons-nous maintenant un x dans $\mathbb{S}^1$. On veut commencer par montrer qu'il existe une infinité d'entiers n tels que les intervalles de la famille $(I_j)_{0 \leq j \leq n}$ soient disjoints deux à deux, où $I_j =]f^j(x), f^{j-n}(x)[$. Si deux intervalles de la sorte s'intersectent, disons I_p et I_q, alors, quitte à ré-indexer, $f^p(x) \in I_q$. Ainsi, en appliquant $n-q$ fois f à l'intervalle I_q, on voit que $f^{p+n-q}(x)$ appartient à l'intervalle $]f^{-n}(x), x[$. Il suffit donc de montrer qu'il existe une infinité d'entiers n tels que $f^k(x)$, $-n \leq k \leq n$, ne soient pas dans $]x, f^n(x)[$ pour avoir la contraposée du résultat.
Pour la suite de la preuve nous allons avoir besoin d'ordonner des points sur le cercle. On décide alors de prendre le temps d'énoncer clairement ce que l'on entend par là, détour qui se veut nécessaire pour la bonne compréhension du lecteur.

Tout d'abord, on (ré-)affirme que l'on choisit d'orienter le cercle dans le sens trigonométrique. Il est ensuite important de constater que cette notion d'orientation n'a que peu, si ce n'est pas, de sens lorsque l'on ne prend que deux points : si a et b sont nos deux points, "l'ordre" dépend du point de départ. La définition d'ordre nécessite donc de prendre trois points, que l'on nommera a, b et c. On notera alors $a \leq b \leq c$, que l'on préférera penser comme "b est entre a et c" à "a est plus petit que b, qui lui même est plus petit que c", lorsque pour tout relevé $\tilde{a}$ de a, il existe des relevés $\tilde{b}$ et $\tilde{c}$ de b et c tels que :

$$\tilde{a} \leq \tilde{b} \leq \tilde{c} \leq \tilde{a} + 1.$$

Le lecteur doit être au courant que, malgré une définition qui se veut formelle, la suite de la démonstration demande une gymnastique intellectuelle non triviale pour utiliser cette notion.

Rappelons donc où nous en sommes. On veut montrer qu'il existe une infinité d'entiers n tels que $f^k(x)$, $-n \leq k \leq n$, ne soient pas dans $]x, f^n(x)[$. Pour ce faire on dispose, grâce au théorème de Poincaré, d'une application surjective h qui semi-conjugue f à R_ρ i.e $h \circ f = R_\rho \circ h$. Cette application h est en fait un passage au quotient d'une autre application H, définit par $H(y) = \sup \{n\rho + m : F^n(x) + m < y\}$, et qui vaut en particulier $n\rho + m$ en $F^n(x) + m$. On montre alors, par récurrence, que pour tout entier n,

$$h \circ f^n = R_\rho^n \circ h. \; (*)$$

On peut donc utiliser le lemme 3.2.4. En effet, au vu de la définition d'ordre que l'on a donné et en utilisant la définition de h et H, on voit que ce lemme nous dit exactement que h préserve l'ordre sur le cercle. Par $(*)$ et la remarque précédente, les orbites de f sont ordonnées de la même manière que celle de la rotation R_ρ. La figure suivante illustre ce fait avec un exemple assez simple.

On peut maintenant se rappeler un résultat fort intéressant : les orbites des rotations d'angle irrationnel sont denses dans le cercle. Ainsi, à n fixé, il existe forcément un entier minimal (la minimalité est importante) N tel que $R_\rho^N(x)$ (ou $R_\rho^{-N}(x)$) soit entre x et $f^n(x)$. Et ainsi la remarque précédente nous permet de conclure que pour ce même N, $f^N(x)$ est le premier élément de l'orbite de f entre x et $f^n(x)$. Pour un tel N il est donc impossible de trouver un élément de la forme $f^k(x)$, pour $-n \leq k \leq n$, entre x et $f^N(x)$ car cela contredirait la minimalité de N.
On est donc maintenant en capacité de se donner un ensemble $\mathcal{N}$ infini d'entiers respectant la condition précédente.

Soit donc maintenant n un élément de $\mathcal{N}$. En utilisant le lemme démontré avec $y = f^{-n}(x)$ on obtient

$$\begin{aligned} \mathrm{Var}(g) &\geq \left| \log \frac{(f^n)'(x)}{(f^n)'(f^{-n}(x))} \right| \\ &= \left| \log\big((f^n)'(x)(f^{-n})'(x)\big) \right|. \end{aligned}$$

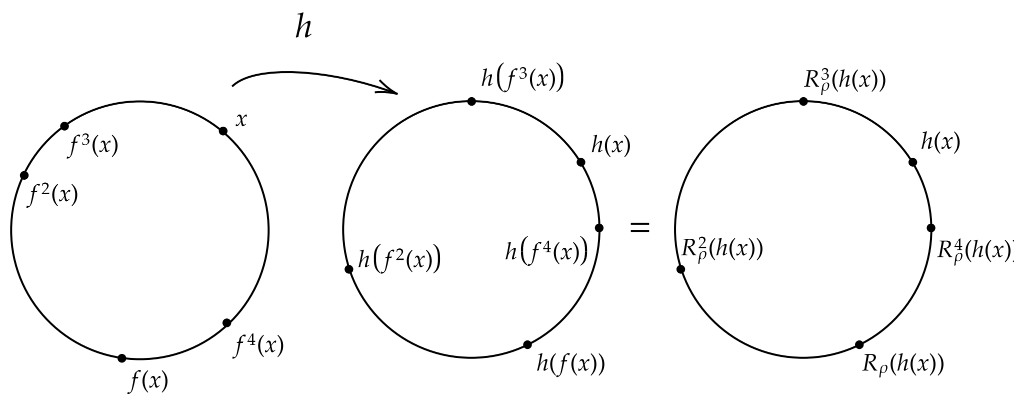

FIGURE 4 – h conserve l'ordre cyclique

Ainsi,

$$\begin{aligned}
\ell(f^n(I)) + \ell(f^{-n}(I)) &= \int_I (f^n)'(t) + (f^{-n})'(t)\mathrm{d}t \\
&\geq \int_I \sqrt{(f^n)'(t)\cdot(f^{-n})'(t)}\mathrm{d}t \\
&\geq \int_I \sqrt{\exp(-\mathrm{Var}(g))}\mathrm{d}t \\
&= \exp\left(-\frac{1}{2}\mathrm{Var}(g)\right)\ell(I).
\end{aligned}$$

Ceci étant vrai pour une infinité de n, la somme des longueurs des intervalles I_n n'est pas bornée, ce qui contredit le fait que l'on peut en trouver un nombre arbitrairement grand disjoints deux à deux.
On peut donc conclure que f est nécessairement transitive et donc f est conjuguée à R_ρ. $\square$

C'est Poincaré qui, historiquement, a démontré ce résultat pour la première fois dans "Mémoire sur les courbes définies par une équation différentielle", chapitre XV. Il se pose cependant la question de l'existence de difféomorphismes non-transitifs, question dont il ne possède par la réponse. Il faudra attendre une trentaine d'années avant que Denjoy réponde à cette question en mettant au point une famille d'exemples, dont on en détaille la teneur juste en dessous.

4.2 Exemples de Denjoy

Théorème 4.2.1. (Exemples de Denjoy). *Pour tout nombre irrationnel ρ comprit entre 0 et 1 il existe un $\mathcal{C}^1$ difféomorphisme du cercle f non-transitif, préservant l'orientation et de nombre de rotation ρ.*

Démonstration. Comme discuté dans la preuve précédente, le lemme 3.2.4 impose que pour tout x dans $\mathbb{S}^1$, l'orbite de x est ordonnée de la même manière que les orbite de R_ρ. Notre seul degré de liberté est donc l'espacement entre les différents points, et c'est sur cela que nous allons jouer.

Soit $(l_n)_{n\in\mathbb{Z}}$ une famille de réels strictement positifs sommable et strictement décroissante lorsque n tend vers $\pm\infty$ (avec donc un maximum en 0) de somme égale à 1. Soit de plus $x_0 \in \mathbb{S}^1$. On définit alors

$$a_n = \sum_{k\in A_n} l_k$$
$$b_n = a_n + l_n,$$

où $A_n = \{k \in \mathbb{Z} : R_\rho^k(x_0) \in [x_0, R_\rho^n(x_0)[\}$. On montre dans la suite que les intervalles de la forme $[a_n, b_n]$ sont disjoints deux à deux. Soient n et m deux entiers distincts et supposons $[a_n, b_n]\cap[a_m, b_m] \neq \varnothing$. Quitte à échanger les rôles, cela implique que a_m appartient à $[a_n, b_n]$ et donc $a_m - a_n \leq b_n - a_n = l_n$. Deux possibilités s'offrent à nous : $R_\rho^m(x_0) < R_\rho^n(x_0)$ ou $R_\rho^n(x_0) < R_\rho^m(x_0)$.
Dans le premier cas, $A_m \subset A_n$ donc $a_n \geq a_m$ i.e $a_n - a_m \geq 0$. L'inégalité est en fait une inégalité stricte car la densité des orbites de R_ρ impose qu'il y a d'autre éléments entre $R_\rho^m(x_0)$ et $R_\rho^n(x_0)$. Absurde car $a_m \geq a_n$ par hypothèse.
Dans le second cas $A_n \subset A_m$ et de plus n est dans A_m. Ainsi, $a_m \geq a_n + l_n$ i.e $a_m - a_n \geq l_n$. Comme l'inégalité est en fait une inégalité large avec le même argument que précédemment, on aboutit à une contradiction. On vient donc de voir que les $[a_n, b_n]$ sont bien disjoints deux à deux.

En se rappelant que la somme des l_n vaut 1, l'union des intervalles de la forme $[a_n, b_n]$ est de mesure 1 dans $[0, 1]$ et est donc dense dans le cercle. Construire un $\mathcal{C}^1$-difféomorphisme revient donc à construire une fonction continue et positive g dont l'intégrale vaut 1. Notre exemple de Denjoy sera alors l'intégrale de g. Naturellement il existe plusieurs moyens pour définir g sur les $[a_n, b_n]$. On décide ici d'utiliser la fonction suivante :

$$g(x) = 1 + \frac{6(l_{n+1} - l_n)}{l_n^3}(b_n - x)(x - a_n).$$

On commence par remarquer que $\displaystyle\int_{a_n}^{b_n} g(t)\mathrm{d}t = l_{n+1}$. En effet,

$$
\begin{aligned}
\int_{a_n}^{b_n} g(t)\mathrm{d}t &= \left[t + \frac{6(l_{n+1}-l_n)}{l_n^3}\left(\frac{b_n+a_n}{2}t^2 - \frac{t^3}{3} - a_nb_nt\right)\right]_{a_n}^{b_n} \\
&= b_n - a_n + \frac{6(l_{n+1}-l_n)}{l_n^3}\left(\frac{b_n+a_n}{2}(b_n^2-a_n^2) - \frac{b_n^3-a_n^3}{3} - a_nb_n(b_n-a_n)\right) \\
&= l_n + \frac{6(l_{n+1}-l_n)}{l_n^3}\left(\frac{(b_n+a_n)^2}{2}l_n - \frac{a_n^2+a_nb_n+b_n^2}{3}l_n - a_nb_nl_n\right) \\
&= l_n + \frac{l_{n+1}-l_n}{l_n^2}\Big(3(b_n+a_n)^2 - 2\big(a_n^2+a_nb_n+b_n^2\big) - 6a_nb_n\Big) \\
&= l_n + \frac{l_{n+1}-l_n}{l_n^2}\big(b_n^2 - 2a_nb_n + a_n^2\big) \\
&= l_n + \frac{l_{n+1}-l_n}{l_n^2}l_n^2 \\
&= l_{n+1}.
\end{aligned}
$$

En faisant une étude de variation on se rend compte que l'application définie sur $[a_n, b_n]$ et qui à x associe $(b_n - x)(a_n - x)$ admet un maximum en $\frac{2a_n+l_n}{2}$. De plus pour $n \geq 0$ on a $l_{n+1} - l_n < 0$. Ainsi

$$\frac{3l_{n+1}-l_n}{2l_n} = 1 - \frac{6(l_{n+1}-l_n)}{l_n^3}\left(\frac{l_n}{n}\right)^2 \leq g(x) \leq 1.$$

De même pour $n < 0$,

$$\frac{3l_{n+1}-l_n}{2l_n} = 1 - \frac{6(l_{n+1}-l_n)}{l_n^3}\left(\frac{l_n}{n}\right)^2 \geq g(x) \geq 1.$$

On définit enfin une famille de réels qui nous intéresse, à savoir

$$
\begin{aligned}
&l_n = \alpha(|n|+2)^{-1}(|n|+3)^{-1} \\
&\text{où } \alpha = \frac{1}{\sum_{n\in\mathbb{Z}}(|n|+2)^{-1}(|n|+3)^{-1}}.
\end{aligned}
$$

Avec cette famille particulière,

$$\frac{3l_{n+1}-l_n}{2l_n} = \frac{3(|n|+2)(|n|+3) - (|n+1|+2)(|n+1|+3)}{2(|n|+2)(|n|+3)(|n+1|+2)(|n+1|+3)} \cdot (|n|+2)(|n|+3),$$

ce qui tend vers 1 quand $|n|$ tend vers l'infini car le numérateur ainsi que le dénominateur sont équivalents à $|n|^4$ en l'infini. Cette famille de réels est clairement sommable de somme 1 et est strictement décroissante.
Pour résumer, on dispose à présent d'une fonction g, définie sur l'union des intervalles de la forme $[a_n, b_n]$ (que l'on notera U). On décide maintenant de prolonger g sur $\mathbb{S}^1$ en disant que $g(y) = 1$ pour tout y dans $\mathbb{S}^1\backslash U$. On dispose donc des résultats suivants :

(i) $\displaystyle\int_{a_n}^{b_n} g(t)\mathrm{d}t = l_{n+1}$

(ii) $g(a_n) = g(b_n) = 1$

(iii) $\displaystyle\lim_{n\to+\infty} \frac{3l_{n+1} - l_n}{2l_n} = 1$

(iv) Si $(x_n)_{n\in\mathbb{N}} \in U$ converge vers y dans $\mathbb{S}^1\backslash U$, $\displaystyle\lim_{n\to+\infty} g(x_n) = 1$.

Les points (i), (ii) et (iii) sont clairement vérifiés avec ce qui a été fait précédemment. Pour le point (iv) il faut remarquer qu'une telle suite sort définitivement tout intervalle $[a_n, b_n]$ à partir d'un certain rang. On utilise donc les deux encadrements faits sur g et le point (iii) pour voir que $g(y) = 1$. Ces considérations faites on voit que g est en fait continue sur le cercle.

Finalement, on pose, pour tout x élément du cercle,

$$f(x) = a_1 + \int_0^x g(t)\mathrm{d}t,$$

et il ne nous reste alors plus qu'à montrer que l'on a bien un $\mathcal{C}^1$-difféomorphisme, de nombre de rotation ρ et qu'il est non-transitif.

Comme g est strictement positive, f est strictement croissante et donc injective. Le point (i) nous permet de voir que $\int_0^1 g(t)\mathrm{d}t = 1$ et par conséquent f est surjective, donc bijective. La continuité de g nous permet quant à elle d'affirmer que f est $\mathcal{C}^1$. Ainsi, f est une fonction réelle $\mathcal{C}^1$ bijective, donc de réciproque $\mathcal{C}^1$ par le théorème de la bijection. Autrement dit, f est bien un $\mathcal{C}^1$-difféomorphisme .

Montrons maintenant que le nombre de rotation de f est ρ. On remarque rapidement que $f^n(0) = a_n$ pour tout n. Soit F l'unique relevé de f tel que $F(\widetilde{a_n}) = \widetilde{a_n}$ où $\widetilde{a_n}$ désigne l'unique relevé de a_n de l'intervalle $[0, 1[$. On voit alors assez facilement que $F^n(0) = \widetilde{a_n} + \lfloor n\rho \rfloor$. Intuitivement, le membre de droite donne le nombre de tours parcourus par 0 après n itérations de f et le membre de gauche donne l'emplacement sur le cercle de l'itérée $n$ème de 0. On trouve alors

$$\lim_{n\to+\infty} \frac{F^n(0)}{n} = \frac{\widetilde{a_n} + \lfloor n\rho \rfloor}{n} = \rho.$$

Il ne nous reste qu'à montrer que f n'est pas transitive. Comme $f^n(0) = a_n$, l'ensemble ω-limite de 0 est tel que $\overline{\omega}(0) = \mathbb{S}^1 \setminus U$ et est donc fermé et parfait de mesure 0. On en conclut donc que f n'est pas transitive. $\square$

Remarque. On vient donc de construire un difféomoprhisme comme voulu. L'hypothèse de régularité sur la dérivé d'un $\mathcal{C}^1$-difféomoprhisme est donc très importante et il n'est pas possible de faire beaucoup mieux que le théorème de Denjoy. Il est cependant possible d'affaiblir les hypothèses en imposant seulement que $\log(f')$ est à variation bornée. [KH95]

5 Mesures invariantes

Cette partie va tourner autour du théorème de Bogolioubov-Krylov, que nous allons énoncer juste après, et du lien qu'il a avec le nombre de rotation.

5.1 Mesure invariante du cercle et lien avec le nombre de rotation

Théorème 5.1.1. (de Bogolioubov-Krylov). *Soient (X, d) un espace métrique compact et $T : X \to X$ une fonction continue. Alors, il existe une mesure de probabilité borélienne μ invariante par T, c'est à dire que pour tout U dans $\mathcal{B}(X)$, l'ensemble des boréliens de X,*

$$\mu(U) = \mu(T^{-1}(U)).$$

Démonstration. On introduit $T_* : \mathcal{M}(X) \to \mathcal{M}(X)$, où $\mathcal{M}(X)$ désigne l'ensemble des mesures de probabilité boréliennes sur X, définie par

$$\forall \nu \in \mathcal{M}(X),\ \forall A \in \mathcal{B}(X), \quad T_*(\nu)(A) = \nu(T^{-1}(A)).$$

Soient $x_0 \in X$ et μ la mesure de Dirac en x_0 (notons que l'on aurait pu choisir une autre mesure de probabilité μ absolument quelconque : la démonstration ne dépend pas de la mesure choisie).

On pose alors pour tout n dans $\mathbb{N}^*$:

$$\mu_n = \frac{1}{n} \sum_{k=0}^{n-1} T_*^k(\mu).$$

Les mesures de probabilité boréliennes étant des applications dans le dual topologique de $\mathcal{C}^0(X)$ d'après le théorème de Riesz – Markov ; on peut donc appliquer le théorème de Banach – Alaoglu qui nous dit que les boules bornées de $\mathcal{M}(X)$ sont $*$-faiblement compactes. La suite $(\mu_n)_{n\in\mathbb{N}}$ est clairement bornée : la norme de μ_n est la masse totale de l'espace, à savoir 1. La suite $(\mu_n)_{n\in\mathbb{N}}$ est donc une suite de la boule unité de $\mathcal{C}^0(X)'$ qui est faiblement compacte et on peut alors en extraire une sous-suite $(\mu_{n_k})_{k\in\mathbb{N}}$ qui converge *-faiblement vers $\nu \in \mathcal{M}(X)$.

Montrons que ν est un point fixe de T_* : soit $A \in \mathcal{B}(X)$,

$$\begin{aligned} T_*(\nu)(A) &= \left(\lim_{k\to+\infty} \frac{1}{n_k} \sum_{i=0}^{n_k-1} T_*^i(\mu)\right)(T^{-1}(A)) \\ &= \lim_{k\to+\infty} \frac{1}{n_k} \sum_{i=0}^{n_k-1} T_*^i[\mu(T^{-1}(A))] \\ &= \lim_{k\to+\infty} \frac{1}{n_k} \sum_{i=0}^{n_k-1} T_*^{i+1}(\mu)(A) \\ &= \lim_{k\to+\infty} \left(\frac{1}{n_k} \sum_{i=0}^{n_k-1} T_*^i(\mu)(A) - \frac{\mu(A)}{n_k} + \frac{T_*^{n_k}(\mu)(A)}{n_k}\right) = \nu(A). \end{aligned}$$

Ainsi notre mesure invariante par T. $\square$

Proposition 5.1.2. *Soient $f \in \mathrm{Homeo}^+(\mathbb{S}^1)$ et μ une mesure invariante par f. Alors la quantité $\mu([x, f(x)[)$ ne dépend pas de x et on la notera $\rho_\mu(f)$.*

Démonstration. Soient $x, y \in \mathbb{S}^1$ distincts. Quitte à échanger leur rôle, on peut supposer $y < f(x) < f(y)$. En effet, si $f(x)$ n'est pas dans $[y, f(y)]$, nécessairement $f(x)$ est entre x et y avec $f(y)$ entre y et x donc entre $f(x)$ et x (la seule autre possibilité serait que $f(x)$ soit entre $f(y)$ et x, ce qui contredirait la préservation de l'orientation). Ainsi, on peut supposer $y < f(x) < f(y)$.

$$\mu([y, f(y)[) = \mu([y, f(x)[) + \mu([f(x), f(y)[) = \mu([y, f(x)[) + \mu([x, y[) = \mu([x, f(x)[).$$

$\square$

Vient maintenant un résultat des plus surprenant, qui éclaire ce choix de notation pour la valeur précédente :

Théorème 5.1.3. *Si f est un homéomorphisme du cercle préservant l'orientation, $\rho_\mu(f)$ coïncide, modulo 1, avec le nombre de rotation de f.*

Démonstration. La mesure μ se relève en une mesure $\tilde{\mu}$ σ-finie sur $\mathbb{R}$. En effet, $[k, k+1[$ et $\mathbb{S}^1$ sont en bijection et cela nous permet de définir une mesure μ_k sur $[k, k+1[$ telle que si A est un borélien de $[k, k+1[$, $\mu_k(A) = \mu(\pi(A))$. On a donc une nouvelle mesure $\tilde{\mu}$ sur $\mathbb{R}$ en disant que si A est un borélien de $\mathbb{R}$, alors

$$\tilde{\mu}(A) = \sum_{k\in\mathbb{Z}} \mu_k(A \cap [k, k+1[).$$

Intuitivement, on "translate" la mesure de $[0, 1[$ sur tout $\mathbb{R}$ en faisant coïncider la densité de $[0, 1[$ avec $[k, k+1[$ pour tout k dans $\mathbb{Z}$.

L'application $\tilde{\mu}$ ainsi définie est bien une mesure sur les boréliens de $\mathbb{R}$.

Soient maintenant $x \in \mathbb{S}^1$, de représentant $\tilde{x} \in \mathbb{R}$, et F un des relèvements de f.
Soit $n \in \mathbb{N}$. Il existe $k \in \mathbb{Z}$ tel que $F^n(\tilde{x}) \in [\tilde{x}+k, \tilde{x}+k+1[$. Comme $\tilde{\mu}([\tilde{x}, \tilde{x}+k[) = k$ pour tout $k \in \mathbb{Z}$, on trouve

$$F^n(\tilde{x}) - \tilde{x} - 1 \leq k \leq \tilde{\mu}([\tilde{x}, F^n(\tilde{x})[) \leq k+1 \leq F^n(\tilde{x}) - \tilde{x} + 1.$$

En divisant par n on voit que

$$\lim_{n\to+\infty} \frac{F^n(\tilde{x}) - \tilde{x}}{n} = \lim_{n\to+\infty} \frac{\tilde{\mu}([\tilde{x}, F^n(\tilde{x})[)}{n} = \lim_{n\to+\infty} \frac{1}{n} \sum_{k=0}^{n-1} \tilde{\mu}([F^k(\tilde{x}), F^{k+1}(\tilde{x})[),$$

la dernière égalité découlant de l'additivité de la mesure et de la stricte croissance de F.
On peut aussi remarquer que $\tilde{\mu}$ est invariante par F. En effet,

$$\begin{aligned}
\tilde{\mu}(F^{-1}(A)) &= \sum_{k\in\mathbb{Z}} \mu_k(F^{-1}(A) \cap [k, k+1[) \\
&= \sum_{k\in\mathbb{Z}} \mu(\pi(F^{-1}(A) \cap [k, k+1[)) \\
&= \sum_{k\in\mathbb{Z}} \mu(f^{-1}(\pi(A \cap [k, k+1[)) \\
&= \sum_{k\in\mathbb{Z}} \mu(\pi(A \cap [k, k+1[)) \\
&= \sum_{k\in\mathbb{Z}} \mu_k(A \cap [k, k+1[) = \tilde{\mu}(A).
\end{aligned}$$

Cette dernière remarque nous permet donc de dire que $\tilde{\mu}([F^k(\tilde{x}), F^{k+1}(\tilde{x})[) = \tilde{\mu}([\tilde{x}, F^1(\tilde{x})[)$ pour tout entier naturel k et donc finalement,

$$\rho(f) = \lim_{n\to+\infty} \frac{F^n(\tilde{x}) - \tilde{x}}{n} \mod 1 = \tilde{\mu}([\tilde{x}, F(\tilde{x})[) \mod 1.$$

Il ne nous reste plus qu'à montrer que cette quantité est bien égale à $\rho_\mu(f)$. On a

$$\begin{aligned}
\tilde{\mu}([\tilde{x}, F(\tilde{x})[) &= \tilde{\mu}([\tilde{x}, \lfloor\tilde{x}\rfloor + 1[) + \tilde{\mu}([\lfloor F(\tilde{x})\rfloor, F(\tilde{x})[) \\
&= \mu([x, 1[) + \mu([1, f(x)[) \\
&= \mu([x, f(x)[) = \rho_\mu(f),
\end{aligned}$$

où la deuxième égalité découle du fait que chacun des intervalles considérés sont contenus dans un intervalle de la forme $[k, k+1[$ pour un unique entier relatif k. Ainsi, la $\tilde{\mu}$-mesure d'un tel intervalle est égale à sa μ_k-mesure qui s'exprime comme la μ-mesure de la projection sur $\mathbb{Z}$ de cet intervalle. $\square$

5.2 Digression ergodique

Nous avons montré l'existence d'une mesure invariante pour les homéomorphismes du cercle, mais qu'en est-il de l'unicité ? Pour cela nous allons étudier, dans un cadre plus général, la convexité de $\mathcal{M}(X)$, où X est un ensemble compact.

Proposition 5.2.1. *$\mathcal{M}(X)$ est convexe.*

Démonstration. Soient $\mu, \nu \in \mathcal{M}(X)$ et $t \in [0,1]$. Montrons d'abord que $t\mu + (1-t)\nu = m$ est une mesure, puis que c'est une mesure de probabilité :

(i) $m(\varnothing) = t\mu(\varnothing) + (1-t)\nu(\varnothing) = 0$

(ii) Si $(A_i)_{i\in\mathbb{N}}$ est une famille boréliens disjoints de X,

$$\begin{aligned} m\left(\bigsqcup_{i\in\mathbb{N}} A_i\right) &= t\mu\left(\bigsqcup_{i\in\mathbb{N}} A_i\right) + (1-t)\nu\left(\bigsqcup_{i\in\mathbb{N}} A_i\right) \\ &= t\sum_{i\in\mathbb{N}} \mu(A_i) + (1-t)\sum_{i\in\mathbb{N}} \nu(A_i) \\ &= \sum_{i\in\mathbb{N}} t\mu(A_i) + (1-t)\nu(A_i) \\ &= \sum_{i\in\mathbb{N}} m(A_i) \end{aligned}$$

(iii) $m(X) = t\mu(X) + (1-t)\nu(X) = t + (1-t) = 1$

Et donc $m \in \mathcal{M}(X)$, i.e. $\mathcal{M}(X)$ est convexe. $\square$

Définition 5.1. *Si C est un ensemble convexe, on dira que $c \in C$ est un **point extrémal** (ou simplement **extrémal**) de C si*

$$\forall x, y \in C,\ \forall t \in [0,1],\ c = tx + (1-t)y \Rightarrow t = 1 \text{ ou } t = 0.$$

Remarque. On n'en détaillera pas la preuve ici, mais il est intéressant de savoir que les points extrémaux de $\mathcal{M}(X)$ sont les mesures de Dirac. Si T est un homéomorphisme de X, nous allons nous intéresser aux points extrémaux de l'ensemble des mesures de probabilité boréliennes invariantes par T, que l'on désignera dans la suite par $\mathcal{M}_T(X)$ - ensemble que nous savons non vide grâce au théorème de Bogolioubov-Krylov montré précédemment.

Commençons par quelques définitions :

Définition 5.2. *Soit T une application d'un espace probabilisé $(X, \mathcal{A}, \mu)$ dans lui même.*

— *On dira que T est **mesure-invariante** si μ est invariante par T.*

— *Si $f : X \to \mathbb{R}$ est mesurable, on dira que f est **essentiellement T-invariante** si,*

$$\mu(\{x \in X : f(T(x)) \neq f(x)\} = 0.$$

- *$A \subset X$ mesurable sera dite* ***essentiellement T-invariante*** *si $\mathbb{1}_A$ est essentiellement T-invariante.*
- *Finalement, μ est* ***ergodique*** *si toute partie de X essentiellement T-invariante est de mesure nul ou total.*

Ces définitions posées, il existe une caractérisation très simple des points extrémaux de $\mathcal{M}_T(X)$.

Théorème 5.2.2. *Les points extrémaux de $\mathcal{M}_T(X)$ sont exactement les mesures ergodiques T-invariante.*

Lemme 5.2.3. *Dire que $A \subset X$ mesurable est essentiellement T-invariante est équivalent à dire que $\mu(T^{-1}(A)\Delta A) = 0$.*

Démonstration.

$$\begin{aligned} x \in \{y \in X : \mathbb{1}_A(T(y)) \neq \mathbb{1}_A(y)\} &\Leftrightarrow (x \in A \text{ et } T(x) \notin A) \text{ ou } (x \notin A \text{ et } T(x) \in A) \\ &\Leftrightarrow (x \in A \text{ et } x \notin T^{-1}(A)) \text{ ou } (x \notin A \text{ et } x \in T^{-1}(A)) \\ &\Leftrightarrow x \in A\Delta T^{-1}(A) \end{aligned}$$

□

Lemme 5.2.4. *Avec les même objets et notations que précédemment, si A et B sont mesurables et si A essentiellement T-invariante,*

$$\mu(T^{-1}(A) \cap B) = \mu(A \cap B)$$

Démonstration.

$$\begin{aligned} \mu(T^{-1}(A) \cap B) &= \mu((T^{-1}(A) \cap A) \cap B)) + \mu((T^{-1}(A)\backslash A) \cap B)) \\ &\overset{1}{=} \mu((T^{-1}(A) \cap A \cap B)) \\ &\overset{2}{=} \mu((T^{-1}(A) \cap A \cap B)) + \mu((A\backslash T^{-1}(A)) \cap B)) \\ &= \mu(A \cap B) \end{aligned}$$

Les égalités 1 et 2 viennent respectivement du fait que $(T^{-1}(A)\backslash A)$ et $(A\backslash T^{-1}(A))$ sont dans $T^{-1}(A)\Delta A$ et sont donc de mesure nulle par hypothèse. □

Il est maintenant temps de montrer que les mesures ergodiques T-invariante sont en fait exactement les points extrémaux de $\mathcal{M}_T(X)$.

Démonstration (du théorème 5.2.2). Commençons par montrer que les points extrémaux de $\mathcal{M}_T(X)$ sont ergodiques.

Soit donc μ extrémale et supposons que μ n'est pas ergodique. Il existe alors A une partie mesurable essentiellement T-invariante dont le poids est strictement compris entre 0 et 1. On pose alors pour tout B mesurable,

$$\mu_A(B) = \frac{\mu(A \cap B)}{\mu(A)} \text{ et } \mu_{X \backslash A}(B) = \frac{\mu((X \backslash A) \cap B)}{\mu(X \backslash A)}.$$

μ_A et $\mu_{X \backslash A}$ sont aussi T-invariantes. En effet, si B est mesurable,

$$\begin{aligned}
\mu_A(T^{-1}(B)) &= \frac{\mu(T^{-1}(A) \cap T^{-1}(B))}{\mu(A)} \\
&= \frac{\mu(T^{-1}(A \cap B))}{\mu(A)} \\
&= \frac{\mu(A \cap B)}{\mu(A)} = \mu_A(B),
\end{aligned}$$

la première égalité venant du lemme précédent. Ainsi on peut décomposer μ de manière non triviale, de la façon suivante $\mu = \mu(A)\mu_A + (1 - \mu(A))\mu_{X \backslash A}$. Il en découle que μ ne serait pas un point extrémal, ce qui est absurde, donc μ est ergodique.

On va maintenant montrer la réciproque.

Soit donc $\mu \in \mathcal{M}_T(X)$ une mesure ergodique. Supposons que $\mu = tm_1 + (1 - t)m_2$ avec t dans $]0, 1[$ et m_1, m_2 des éléments de $\mathcal{M}_T(X)$. Comme l'image d'une mesure est positive, m_1 est absolument continue par rapport à μ, car $tm_1 \leq \mu$. D'après le théorème de Radon–Nikodym il existe r mesurable positive telle que

$$\forall A \in \mathcal{B}(X), \quad m_1(A) = \int_A r \mathrm{d}\mu.$$

On remarque que $r \leq \frac{2}{t}$ μ presque partout. En effet, si $Z = \{x \in X : r(x) > \frac{2}{t}\}$ est tel que $\mu(Z) > 0$, on aurait

$$m_1(Z) = \int_Z r \mathrm{d}\mu > \frac{2\mu(Z)}{t},$$

ce qui n'est pas possible car $\mu = tm_1 + (1 - t)m_2$. Ainsi, r est de carré μ-intégrable.

On veut maintenant montrer que $r \circ T = r$.

$$\begin{aligned}
\int (r \circ T - r)^2 \mathrm{d}\mu &= \int r^2 \circ T \mathrm{d}\mu - 2 \int r \circ T r \mathrm{d}\mu + \int r^2 \mathrm{d}\mu \\
&= \int r^2 \mathrm{d}\mu - 2 \int r \circ T \mathrm{d}m_1 + \int r^2 \mathrm{d}\mu \\
&= \int r^2 \mathrm{d}\mu - 2 \int r \mathrm{d}m_1 + \int r^2 \mathrm{d}\mu \\
&= \int r^2 \mathrm{d}\mu - 2 \int r^2 \mathrm{d}\mu + \int r^2 \mathrm{d}\mu \\
&= 0
\end{aligned}$$

Comme $(r \circ T - r)^2$ est toujours positive, il suit que $(r \circ T - r)^2 = 0$ μ-presque partout, et donc $r \circ T = r$ μ-presque partout. Il nous reste à en déduire que r est constante.

Pour tout c dans $\mathbb{R}$ on pose $A_c = \{r < c\}$. On voit que $T^{-1}(A_c) = A_c$ et donc A_c est essentiellement T-invariante pour tout réel c. Comme μ est ergodique, $\mu(A_c) = 0$ ou 1. De plus r est finie presque partout (sinon elle ne serait pas de carré intégrable) donc $\mu(A_c)$ vaut 1 pour un c assez grand. On peut alors sereinement définir $c_0 = \inf(\{c \in \mathbb{R} : \mu(A_c)\}) = 1$.

On voit finalement que r vaut c_0 μ-presque partout. En effet, pour tout entier naturel n, $c_0 > c_0 - \frac{1}{n}$ et donc $r \geq c_0 - \frac{1}{n}$ μ-presque partout. Ceci étant vrai pour tout n, $r \geq c_0$ μ-presque partout. De même, $c_0 < c_0 + \frac{1}{n}$. Il existe donc c' tel que $c_0 < c' < c_0 + \frac{1}{n}$ et $r < c'$ μ-presque partout. Ainsi, $r \leq c_0 + \frac{1}{n}$ μ-presque partout. Finalement, $r = c_0$ μ-presque partout.

La fonction r étant constante μ-p.p, m_1 est un multiple de μ et il est de même pour m_2 avec le même raisonnement, donc μ est extrémale. $\square$

Ce que ce résultat nous dit est que, tout comme dans un espace convexe de dimension finie dans lequel les points s'écrivent comme combinaison convexe de points extrêmaux, toute mesure borélienne de probabilité invariante par T s'écrit comme une intégrale de mesure ergodique (l'intégrale étant ici "l'analogue" de la combinaison convexe dans un espace beaucoup plus grand). Cela permet, entre autre, de simplifier l'étude d'un certain nombre de problèmes en se restreignant à l'étude des mesures ergodiques.

Bibliographie

Références

[BS02] Michael Brin et Garrett Stuck. *Introduction to dynamical systems.* Cambridge University Press, Cambridge, 2002, p. xii+240. ISBN : 0-521-80841-3. DOI : 10.1017/CBO9780511755316. URL : https://doi-org.revues.math.u-psud.fr/10.1017/CBO9780511755316.

[KH95] Anatole Katok et Boris Hasselblatt. *Introduction to the modern theory of dynamical systems.* Cambridge University Press, Cambridge, 1995.

[Kue07] Christian Kuehn. *An Introduction to Rotation Theory.* Cornell University, 2007. URL : https://tutorials.siam.org/dsweb/circlemaps/circle.pdf.

[Nav07] Andrés Navas. *Groups of diffeomorphisms of the circle.* Sociedade Brasileira de Matemática, Rio de Janeiro, 2007, p. ii+249. ISBN : 978-85-85818-36-4. URL : https://arxiv.org/pdf/math/0607481.pdf.

[Pau21] Frédéric Paulin. *Introduction aux systèmes dynamiques topologiques et différentiables.* Université Paris-Saclay, Orsay, 2021. URL : https://www.imo.universite-paris-saclay.fr/~paulin/notescours/cours_SysDynM2.pdf.

[San18] Diego A. S. Sanhueza. *Homeomorphisms on the Circle.* UFRJ Rio de Janeiro, Brasil, 2018. URL : http://www.im.ufrj.br/~gelfert/cursos/2019-1-SisDin/Homeomorphisms%20on%20the%20circle.pdf.