Furstenberg Theorem

Dominique MALICET

1 Notations and statement

Let $\mathbb{T}$ be the 1-dimmensional torus $\mathbb{R}/\mathbb{Z}$.
For α in $\mathbb{T}$ we denote by $T_\alpha : \mathbb{T} \to \mathbb{T}$ the translation operator defined by $T_\alpha(x) = x + \alpha \mod 1$.
For n in $\mathbb{N}$ we denote by $M_n : \mathbb{T} \to \mathbb{T}$ the multiplication operator defined by $M_n(x) = nx \mod 1$.

Theorem A. *(Furstenberg)*
Let a and b be two positive integers which are not powers of a same integer, and let F be a closed subset of $\mathbb{T}$ invariant by M_a and M_b. Then either F is finite or $F = \mathbb{T}$.

Remarks 1.1.
-In the case where F is an invariant finite set, it is actullay constituted of rational numbers (indeed if F contains some irrational number x, then it contains $a^n x$ for every n and these numbers are all distinct modulo 1.*)*

-The conclusion does not hold if the closed set is invariant by only one transformation M_a. For exemple the triadic Cantor set is invariant by M_3.

-We can reformulate the theorem as follows: if a, b are integers which are not powers of a same integer, then for any irrational number x the set $\{a^m b^n x, (m,n) \in \mathbb{N}^2\}$ is dense modulo 1.

2 Proof of the theorem

We will mainly follow the proof of Furstenberg, except that we try to avoid the unnecessary use of the existence of minimal invariant closed subsets. For the whole proof, we fix integers a and b which are not powers of a same integer. It is equivalent to say such that $\log a$ and $\log b$ are independant over $\mathbb{Q}$. Let F be a closed subset of $\mathbb{T}$ invariant by M_a and M_b. If F is infinite, it means that it has some accumulation point, and we want to deduce that actually $F = \mathbb{T}$. We divide the proof in two parts:

The first part treat the particular case where the accumulation point of F is a rational number. "Spreading" points of F close to this rational number by using

M_a and M_b, we manage to prove that $F = \mathbb{T}$, mainly by combinatorial technics.

The second part treat the general case where the accumulation point can be irrational. The idea here is to use translations T_α commuting with M_a and M_b, and to prove that there is "some T_α-invariance" in F. The first treated case will help at some key points. Note however the following fact which can be checked by a simple computation:

Lemma 2.1. *A translation T_α commute with M_a and M_b if and only if $(a-1)\alpha = (b-1)\alpha = 0 \mod 1$, or equivalently that α is a rational number (modulo 1) whose denominator divide $a-1$ and $b-1$.*

This condition on α is too much restrictive to be useful (there is only a finite numbers of solutions, and even no solution at all if $a-1$ and $b-1$ are coprime!). That is why we will actually use translations commuting with some large powers of M_a and M_b.

2.1 The particular case

In this part we prove the following weak version of the theorem:

Proposition 2.2. *If F is closed, invariant by M_a and M_b and has some rational number $\frac{p}{q}$ as an accumulation point, then $F = \mathbb{T}$.*

The proof relies on the following combinatorial lemma, which is actually the only step where we use that we have two transformations M_a and M_b instead of one.

Lemma 2.3. *Let us enumerate the set $S = \{a^m b^n, (m,n) \in \mathbb{N}^2\}$ by an increasing sequence of integers $(s_k)_{k\in\mathbb{N}}$. Then $\lim_{k\to+\infty} \frac{s_{k+1}}{s_k} = 1$*

Proof. The key point is to use that the additive group generated by $\log a$ and $\log b$ is dense in $\mathbb{R}$ (since $\log a$ and $\log b$ are independant over $\mathbb{Q}$) and hence that the set $\{a^m b^n, (m,n) \in \mathbb{Z}^2\}$ is dense in $\mathbb{R}_+$. In particular one can find a sequence $(x_k)_{k\in\mathbb{N}}$ of the form $x_k = a^{m_k} b^{n_k}$ with m_k, n_k in $\mathbb{Z}$, which converges to 1 by superior values.

As a consequence, we claim that for any $\varepsilon > 0$, one can find two real numbers u and v in $(1, 1+\varepsilon)$ of the form $u = \frac{a^m}{b^n}$ and $v = \frac{b^{m'}}{a^{n'}}$ with m, n, m', n' positive integers. Indeed, for k larger that some k_0, we have $x_k = a^{m_k} b^{n_k} \in (1, 1+\varepsilon)$, and in particular m_k and n_k have alternate signs. If for some k_1, k_2 one have $m_{k_1} > 0$ (hence $n_{k_1} < 0$) and $m_{k_2} < 0$ (hence $n_{k_2} > 0$) then one can choose $u = x_{k_1}$ and $v = x_{k_2}$. If not, let say for exemple that $m_k > 0$, $n_k < 0$ for any k larger than k_0 (the other case is identical), then one can choose $u = x_{k_0}$ and $v = x_{k_0} x_k^{-1}$ with $k >> k_0$ (so that $v = a^{m_{k_0} - m_k} b^{n_{k_0} - n_k} \approx x_{k_0} \in (1, 1+\varepsilon)$ with $m_{k_0} - m_k < 0$ and $n_{k_0} - n_k > 0$).

Now, we can conclude as follows: let us write the enumeration $(s_k)_{k\in\mathbb{N}}$ as $s_k = a^{m_k}b^{n_k}$ with m_k, n_k in $\mathbb{N}$, and let us fix $\varepsilon > 0$, and $u = \frac{a^m}{b^n}$ and $v = \frac{b^{m'}}{a^{n'}}$ in $(1, 1+\varepsilon)$ as before. Then for k large, either m_k or n_k is large enough so that at least one of the numbers $s_k u$ or $s_k v$ belongs to S. In consequence,

$$s_{k+1} \leq \max(s_k u, s_k v) \leq s_k(1+\varepsilon),$$

and so $\lim_{k\to+\infty} \frac{s_{k+1}}{s_k} = 1$. □

Let us prove Proposition 2.2:

Proof. We denote by $x \mapsto \bar{x}$ the canonical projection of $\mathbb{R}$ onto $\mathbb{T}$.

Let us treat first the case where the accumulation point of F is 0 (modulo 1). Then, up to replace F by $-F$ we assume that for any $\varepsilon > 0$, there exists x_ε in $(0, \varepsilon)$ such that $\bar{x}_\varepsilon$ belongs to F. Let $x \in (0,1)$ arbitrary, and for each $\varepsilon > 0$ let k_ε be such that $s_{k_\varepsilon} x_\varepsilon \leq x < s_{k_\varepsilon+1} x_\varepsilon$. We write that

$$d(\bar{x}, F) \leq |x - s_k x_0| \leq s_{k_\varepsilon+1}x_\varepsilon - s_{k_\varepsilon}x_\varepsilon = \left(\frac{s_{k_\varepsilon+1}}{s_{k_\varepsilon}} - 1\right) s_{k_\varepsilon}x_\varepsilon \leq \left(\frac{s_{k_\varepsilon+1}}{s_{k_\varepsilon}} - 1\right) x$$

Letting ε going to 0, we have that $k_\varepsilon \to +\infty$ hence the last term tends to 0 by the lemma, and we conclude that $\bar{x}$ belongs to F. Thus $F = \mathbb{T}$.

In the general case where the accumulation point of F is a rational number $\frac{p}{q}$, then the point $p = 0 \mod 1$ is an accumulation point of $M_q(F)$, and since M_q commute with M_a and M_b, the set $M_q(F)$ is also invariant by M_a and M_b, and we deduce by the first case that $M_q(F) = \mathbb{T}$. As a consequence, we also have that $M_q^{-1}(M_q(F)) = \mathbb{T}$, that is:

$$F \cup T_{\frac{1}{q}}(F) \cup \cdots \cup T_{\frac{q-1}{q}}(F) = \mathbb{T}.$$

Since a finite union of closed sets with empty interiors has empty interior, we conclude that F contains some non trivial interval I. But for n large, $M_a^n(I) = \mathbb{T}$, hence $F = \mathbb{T}$ by M_a-invariance of F. □

2.2 The general case

We establish some lemmas relating F with dynamics of translations T_α.

Lemma 2.4. *For any closed set F invariant by M_a and M_b and for any translation T_α, we have that $T_\alpha(F) \cap F \neq \emptyset$ unless maybe if F is finite.*

Proof. Note that

$$T_\alpha(F) \cap F \neq \emptyset \Leftrightarrow \alpha \in F - F,$$

where $F - F = \{x - y, (x, y) \in F \times F\}$. The set $F - F$ is closed and invariant by M_a and M_b. Moreover, if F is infinite, then F has some accumulation point x and hence $0 = x - x$ is a accumulation point of $F - F$ so that by Proposition 2.2, $F - F = \mathbb{T}$, and hence $T_\alpha(F) \cap F \neq \emptyset$.

□

Lemma 2.5. *If F is an infinite closed set invariant by M_a and M_b, and if T_α is a translation commuting with M_a and M_b, then there exists a nonempty closed set $\tilde{F} \subset F$ invariant by T_α.*

Proof. Since F is infinite, the set F' of the accumulation points of F is non empty. Let us define by induction $F_0 = F'$ and $F_{n+1} = F_n \cap T_\alpha(F_n)$, and let $\tilde{F} = \cap_n F_n$. The sequence $(F_n)_{n\in\mathbb{N}}$ is a decreasing sequence of closed sets, all of them invariant by M_a and M_b (because T_α commute with M_a and M_b), and $T_\alpha(F_{n+1}) \subset F_n$. The intersection $\tilde{F}$ is obviously a closed subset of F invariant by T_α, so the only non trivial point to check is that $\tilde{F} \neq \emptyset$.

Let us assume by contradiction that $\tilde{F} = \emptyset$. Then by compacity we have that $F_n = \emptyset$ for some $n > 0$, and choosing n minimal we can assume that $F_{n-1} \neq \emptyset$. Then, by Lemma 2.4, F_{n-1} is a finite set, hence in particular it is constituted of rational numbers (See the first remark after Theroem A). Since $F_{n-1} \neq \emptyset$ and $F_{n-1} \subset F_0 = F'$, that means that we can find a rational number in F', so that by Proposition 2.2, $F = \mathbb{T}$ and hence $\tilde{F} = \mathbb{T}$, which contradicts the assumption $\tilde{F} = \emptyset$ and conclude the proof. □

Remarks 2.6. *We will use the previous lemma with rational translations T_α, and in this case one easily check that $\tilde{F}$ is actually the finite intersection $\tilde{F} = F' \cap T_\alpha(F') \cap \cdots T_\alpha^{k-1}(F')$ where k is the denominator of α.*

We are now ready to prove Theorem A:

Proof. Let F a closed set invariant by M_a and M_b that we assume infinite. Let k a large number coprime with a and b, and let $n = \varphi(k)$ the cardinal of $(\mathbb{Z}/k\mathbb{Z})^\times$ so that $a^n = b^n = 1 \mod k$. Then, F is invariant by $M_{a^n} = M_a^n$ and $M_{b^n} = M_b^n$, and the translation $T_{\frac{1}{k}}$ commute with M_{a^n} and M_{b^n} (Lemma 2.1). Applying Lemma 2.5 (with M_{a^n} and M_{b^n} instead of M_a and M_b), we find $\tilde{F} \subset F$ non empty invariant by $T_{\frac{1}{k}}$. In particular $\tilde{F}$ is $\frac{1}{k}$-dense, and hence so does F. Since k can be chosen arbitrarily large, $F = \mathbb{T}$. □