GROUPS ACTING ON THE CIRCLE

LAWRENCE CONLON

These are notes for a short course to be given at the meeting in Les Diablerets in March, 2002. This meeting is organised jointly by the Troisiéme Cycle romand de Mathématiques and the Unviversités de la région Rhône-Alpes.

1. Minimal Sets

The circle S^1 is the simplest nontrivial compact manifold without boundary. It is realized in a number of ways, our favorites being the unit circle in the complex plane and the quotient group $\mathbb{R}/\mathbb{Z}$. These realizations are canonically equivalent via the map

$$t + \mathbb{Z} \mapsto e^{2\pi i t}.$$

We consider a left action

$$G \times S^1 \to S^1$$

of a discrete group G on S^1. For the moment, we only assume that this action is continuous, hence defines a homomorphism of groups

$$\varphi : G \to \mathrm{Homeo}(S^1).$$

Generally, we will write gx for $\varphi(g)(x)$, where $g \in G$ and $x \in S^1$.

Example 1.1. A single homeomorphism f of S^1 generates an action of $\mathbb{Z}$ on S^1 by the formula $nz = f^n(z)$, $\forall\, n \in \mathbb{Z}$, $\forall\, z \in S^1$.

Definition 1.2. If $x \in S^1$, the set $Gx = \{gx \mid g \in G\}$ is called the *G–orbit* of x.

One frequently speaks simply of the orbit of x. If $G \cong \mathbb{Z}$ is generated by a single homeomorphism f, we also call a $\mathbb{Z}$–orbit an f–orbit. Evidently, the G–orbits partition S^1 into equivalence classes, two points of S^1 being equivalent if some element of G takes one to the other.

The following is a key concept for analyzing the group action.

Definition 1.3. Let $X \subseteq S^1$ be closed, nonempty, and invariant under the action of G. If X contains no proper subset with these properties, then X is called a *minimal set* for the action of G. This is also called a *G–minimal set.*

In other words, a G–minimal set X is a nonempty union of orbits, each of which has X as its closure.

Lemma 1.4. *Each G–action on S^1 admits a minimal set.*

Proof. Let $\mathcal{A}$ denote the family of closed, nonempty G–invariant subsets of S^1. Then $\mathcal{A} \neq \emptyset$ since $S^1 \in \mathcal{A}$. Partially order this set by inclusion $X \supseteq Y$ and note that every totally ordered subset has a lower bound. Indeed, the intersection of a descending nest of elements of $\mathcal{A}$ is nonempty, compact and G–invariant. By Zorn's lemma, there exists a G–minimal set. $\square$

EXAMPLE 1.5. Let $\alpha = n/m + \mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$, n and m relatively prime. Then the rotation

$$r_\alpha : S^1 \to S^1, \qquad r_\alpha(e^{2\pi i t}) = e^{2\pi i(t+\alpha)}$$

induces an action of the cyclic group $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ on S^1. Each orbit is a set of m distinct points and is a minimal set.

More generally, if an action has a finite orbit, that orbit is a minimal set.

EXAMPLE 1.6. Let $\alpha \in \mathbb{R}/\mathbb{Z}$ be irrational. Then the rotation r_α induces an action of $\mathbb{Z}$ on S^1. It is classical (and an elementary exercise) that each orbit is dense in S^1, hence S^1 itself is the unique minimal set for this action.

DEFINITION 1.7. If a G–minimal set $X \subseteq S^1$ is neither a finite orbit nor the entire circle, then X is said to be *exceptional.*

LEMMA 1.8. *An exceptional G–minimal set $X \subset S^1$ is homeomorphic to the Cantor set and every G–orbit in S^1 clusters at every point of X. In particular, an exceptional minimal set is the unique minimal set.*

Proof. First of all, we note that X can have no interior. Indeed, suppose that $U \subset X$ is open in S^1 and let $y \in X$. Since Gy is dense in X, $Gy \cap U \neq \emptyset$. By G–invariance, y itself lies in the interior of X. Since $y \in X$ is arbitrary, X is open. Since X is closed and nonempty, the connectivity of S^1 implies that $X = S^1$, contrary to hypothesis. We show next that X is a perfect set. Indeed, let $X' \subseteq X$ be the set of cluster points of X. Since X is infinite and compact, $X' \neq \emptyset$. Also, X' is closed and G–invariant, hence $X' = X$ by minimality. We have proven that X is a perfect set without interior, hence a Cantor set. We choose arbitrary $y \in S^1$, $x \in X$, and show that Gy clusters at x. We can assume that $y \notin X$. Let I denote the closure of the component of $S^1 \setminus X$ containing y and let $z \in I$ denote either endpoint of this arc. Then $z \in X$ and there is a sequence $\{z_n = g_n z\}_{n=1}^\infty$ that clusters at x. Since the lengths of the arcs $I_n = g_n I$ must also converge to 0, one concludes that $\{g_n y \in I_n\}_{n=1}^\infty$ clusters at x. □

EXAMPLE 1.9. We construct an action of the free product $\mathbb{Z}_2 * \mathbb{Z}_3$ on S^1 with an exceptional minimal set. For this we view S^1 as the boundary of the unit disk $D \subset \mathbb{C}$ centered at the origin and use the fact that $\mathbf{H} = \operatorname{int} D$ is a model for hyperbolic geometry. The geodesics ("straight lines") in this geometry are the open circular arcs $L_0 = L \cap \mathbf{H}$, where $L \subset D$ is a closed circular arc meeting $S^1 = \partial D$ orthogonally. The open diameters of $\mathbf{H}$ are also considered to be geodesics. In hyperbolic geometry, the angles between intersecting lines are measured exactly as in Euclidean geometry. Given arbitrary $x \in \mathbf{H}$, the hyperbolic rotation about x through an angle α is a well defined isometry of the hyperbolic plane. It is realized as the restriction to $\mathbf{H}$ of a suitable linear fractional transformation of $\mathbb{C}$ that preserves D, hence this rotation extends to S^1, thought of as the "circle at infinity" for $\mathbf{H}$.

Let

$$f : \mathbf{H} \to \mathbf{H}$$

be the hyperbolic rotation about 0 through $2\pi/3$ and also denote by

$$f : S^1 \to S^1$$

the induced map on the circle. Since 0 is the origin, this also happens to be a Euclidean rotation through the same angle. Let s be a geodesic which, as indicated

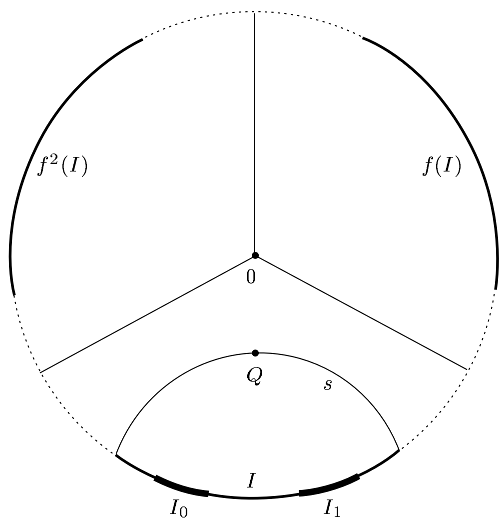

FIGURE 1. The action of f and g on S^1

in Figure 1, does not pass through 0 and suppose that there is a compact arc $I \subset S^1$ of length strictly less than $2\pi/3$ subtended by s. Let Q be the Euclidean midpoint of s and let

$$g : \mathbf{H} \to \mathbf{H}$$

be the hyperbolic rotation about Q through the angle π, an isometry carrying s to $-s$. The map

$$g : S^1 \to S^1$$

induced by this rotation interchanges the complementary subarcs of S^1 separated by the endpoints of s. Thus, g carries $f(I)$ to a compact arc $I_0 \subset \operatorname{int} I$ and it carries $f^2(I)$ to another such arc $I_1 \subset \operatorname{int} I$ disjoint from I_0 (Figure 1). Let $\operatorname{Diff}^{\omega}_{+}(S^1)$ denote the group of orientation preserving, real analytic diffeomorphisms of S^1 and let G be the subgroup generated by f and g. This is clearly the image of $\mathbb{Z}_2 * \mathbb{Z}_3$ in $\operatorname{Diff}^{\omega}_{+}(S^1)$ under a group homomorphism. We set

$$h_0 = g \circ f,$$
$$h_1 = g \circ f^2,$$

remarking that

$$I_0 = h_0(I),$$
$$I_1 = h_1(I).$$

Similarly, form disjoint, compact subarcs

$$h_0(I_0) = I_{00} \subset \operatorname{int} I_0, \qquad h_1(I_0) = I_{10} \subset \operatorname{int} I_1,$$
$$h_0(I_1) = I_{01} \subset \operatorname{int} I_0, \qquad h_1(I_1) = I_{11} \subset \operatorname{int} I_1.$$

Inductively, one defines, for each finite sequence $(i_0, i_1, \dots, i_r) \in \{0,1\}^{r+1}$, a compact arc

$$h_{i_0}(I_{i_1 i_2 \dots i_r}) = I_{i_0 i_1 \dots i_r} \subset \operatorname{int} I_{i_0 i_1 \dots i_{r-1}},$$

the two choices of the index i_r giving a pair of disjoint, compact subarcs of the interior of $I_{i_0 i_1 \dots i_{r-1}}$. As $r \uparrow \infty$, it can be shown that the lengths of these arcs shrink to 0. So each infinite sequence

$$\iota = (i_0, i_1, \dots, i_r, \dots) \in \{0,1\}^{\mathbb{N}} = \mathfrak{S}$$

determines a unique nesting

$$I_{i_0} \supset I_{i_0 i_1} \supset \cdots \supset I_{i_0 i_1 \dots i_r} \supset \cdots$$

of compact intervals shrinking to a unique point

$$z_\iota = \bigcap_{j=0}^{\infty} I_{i_0 i_1 \dots i_j} \in I.$$

It is evident from this construction that

$$C_0 = \{z_\iota\}_{\iota \in \mathfrak{S}}$$

is a Cantor set. As an exercise, the reader can check that the Cantor set

$$C = C_0 \cup f(C_0) \cup f^2(C_0)$$

is G–invariant and that Gz clusters at every point of C, $\forall\, z \in S^1$. It is clear, then, that C is an exceptional minimal set for the action of $\mathbb{Z}_2 * \mathbb{Z}_3$.

Example 1.10. Following an exposition by P. Schweitzer [7, Appendix], we sketch the construction of an $f \in \mathrm{Homeo}_+(S^1)$, generating an action of $\mathbb{Z}$ on S^1 with an exceptional minimal set. We also indicate how, with care, the construction gives such $f \in \mathrm{Diff}^1_+(S^1)$, the group of C^1 diffeomorphisms that preserve orientation. This construction is due to Denjoy.

The idea is to consider the bi–infinite sequence $\{x_n = r_\alpha^n x\}_{n=-\infty}^{\infty}$, the orbit of $x \in S^1$ under the rotation r_α, α irrational, and to blow up each x_n to a little interval I_n of length a_n, so chosen that $\sum_{n\in\mathbb{Z}} a_n = a$ is finite. This replaces the ordinary circle $\mathbb{R}/\mathbb{Z} = S^1(1)$, having circumference 1, with a circle $S^1(1+a)$, having circumference $1+a$. One then extends r_α to a homeomorphism

$$f : S^1(1+a) \to S^1(1+a)$$

by choosing each $f|I_n$ to be a suitable homeomorphism onto I_{n+1}.

A bit more formally, identify $S^1(1)$ as the interval $[0,1]$, with endpoints identified, and $S^1(1+a)$ as $[0,1+a]$, with endpoints identified. We then define

$$h : [0,1+a] \to [0,1]$$

by

$$h(y) = \sup\left\{ x_n \mid x_n + \sum_{x_k < x_n} a_k < y \right\}.$$

If we assume, as we may, that no x_n is the point $1 \equiv 0$, this formula makes good sense and takes the endpoints of the first interval to those of the second. A little thought shows that h is nondecreasing. If $y = x_n + \sum_{x_k<x_n} a_k$, then $h(y) = x_n$. Since the image of h is dense in $[0,1]$, there can be no jump discontinuities and the nondecreasing function is continuous and surjective. We can now leave it as an exercise for the reader to prove that each $h^{-1}(x_n)$ is an interval I_n of length a_n and that the pullback of any point not in the sequence $\{x_n\}$ is a single point. The

surjection h exactly collapses each interval I_n onto the point x_n. Finally, h can be identified as a surjection

$$h : S^1(1+a) \to S^1(1).$$

One can now construct a bijective map f making the following diagram commute:

$$\begin{array}{ccc} S^1(1+a) & \xrightarrow{f} & S^1(1+a) \\ {\scriptstyle h}\downarrow & & \downarrow{\scriptstyle h} \\ S^1(1) & \xrightarrow[r_\alpha]{} & S^1(1). \end{array}$$

This can be done by choosing each $f_n = f|I_n : I_n \to I_{n+1}$ to be a suitable homeomorphism and, on the points $h^{-1}(y) \notin h^{-1}\{x_n\}_{n=-\infty}^{\infty}$, choosing f as is forced by the commutativity of the diagram. Rather than check that f is a homeomorphism, we will sketch the steps necessary to assure that it is a C^1 diffeomorphism.

In choosing the lengths a_n of the inserted intervals, one can require that

$$\lim_{|n|\to\infty} \frac{a_{n+1}}{a_n} = 1$$

and that all $a_{n+1}/a_n < 1$. For example, choose $a_n = 1/(1+n^2)$. In order to define $f_n : I_n \to I_{n+1}$, we define a strictly positive function $f'_n : I_n \to \mathbb{R}$ such that

$$\int_{I_n} f'_n(x)\, dx = a_{n+1}.$$

One can define $f'_n = 1 + \varphi_n$ for continuous functions $\varphi_n \le 0$, vanishing at ∂I_n and converging uniformly to 0 as $|n| \to \infty$. Define f' to be the strictly positive continuous function on $[0, 1+a]$ that agrees with f'_n on each I_n and is identically 1 elsewhere. A suitable antiderivative of f' carries $[0, 1+a]$ onto itself and induces the desired C^1 diffeomorphism f.

Finally, it is easy to see that the union of the interiors of the arcs I_n has complement X in $S^1(1+a)$ that is compact, nowhere dense and is $\mathbb{Z}$–invariant, hence contains a minimal set that is nowhere dense. By the irrationality of α, there are no finite orbits, hence this minimal set is exceptional. (In fact, X is the minimal set.)

We note that both of the above examples have some smoothness. The first, in fact, is real analytic and the second is at least C^1. The degree of smoothness of a group action is often referred to as its "regularity".

The following is the key regularity theorem for groups acting on the circle. It is actually a special case of a more general theorem of R. Sacksteder about pseudogroups of local diffeomorphisms of 1–manifolds.

THEOREM 1.11 (Sacksteder [6]). *Let G be a finitely generated group of orientation preserving C^2 diffeomorphisms of S^1 having an exceptional minimal set X. Then there is $g \in G$ and $x \in X$ such that $gx = x$ and $g'(x) < 1$.*

The second assertion ensures that $g \neq \mathrm{id}$. Since a single diffeomorphism f having an exceptional minimal set cannot have a periodic point, no nontrivial power of f can have a fixed point, so we obtain the following corollary.

COROLLARY 1.12 (Denjoy [1]). *If f is a C^2 diffeomorphism of S^1 having no finite orbit, then S^1 is the minimal set of the associated $\mathbb{Z}$–action.*

Thus, Example 1.10 cannot be improved to make f a diffeomorphism of class C^2 or better and these theorems are not true for only C^1 regularity. The reader should check that, in Example 1.9, the elements h_0 and h_1 have attracting fixed points.

In fact, we will only need Corollary 1.12 in these notes, but Sacksteder's theorem is of considerable importance and is not that much harder to prove. Being a little lengthy, however, this proof will be given in Appendix A. The interested reader will find a direct proof of Corollary 1.12 in the book [3, pp. 145–147] of C. Godbillon.

2. The Poincaré Rotation Number

The material in this section depends significantly on the beautiful exposition of Godbillon in [3, pp. 151–159]

The projection $p : \mathbb{R} \to \mathbb{R}/\mathbb{Z} = S^1$ is the universal covering of the circle. By standard covering space theory, continuous maps $f : S^1 \to S^1$ lift to maps F making the diagram

$$\begin{array}{ccc} \mathbb{R} & \xrightarrow{F} & \mathbb{R} \\ {\scriptstyle p}\downarrow & & \downarrow{\scriptstyle p} \\ S^1 & \xrightarrow[f]{} & S^1 \end{array}$$

commute. Two such lifts differ by a (constant) integer. Furthermore, independently of the choice of lift, there is an integer m, called the *degree* of f, such that

$$F(x+1) = F(x) + m.$$

Orientation preserving homeomorphisms $f : S^1 \to S^1$, have degree 1, and so

$$(*) \qquad F(x+1) = F(x) + 1.$$

Let $\mathcal{G}$ denote the group $\mathrm{Homeo}_+(S^1)$ of orientation preserving homeomorphisms of the circle and $\widetilde{\mathcal{G}}$ the group of lifts of elements of $\mathcal{G}$. There is a natural projection $\pi : \widetilde{\mathcal{G}} \to \mathcal{G}$ such that $\pi(F) = f$ if and only if F is a lift of f. It is often convenient to analyze homeomorphisms f of the circle by analyzing $F \in \pi^{-1}(f)$. Such $F : \mathbb{R} \to \mathbb{R}$ is strictly increasing and any two lifts of f differ by a constant integer. It is clear that π is a group homomorphism (continuous in the uniform topology of these groups) and has kernel the infinite cyclic group of integer translations. The lifts of rotations are translations and *vice-versa*.

Fix $F \in \widetilde{\mathcal{G}}$. By $(*)$, the function $\Phi(t) = F(t) - t$ is periodic of period 1. In particular, it has finite maximum and minimum values on $\mathbb{R}$.

Lemma 2.1. *For Φ as above and arbitrary $x, y \in \mathbb{R}$, $|\Phi(x) - \Phi(y)| < 1$.*

Proof. It will be enough to show that $\max\Phi - \min\Phi < 1$. Otherwise, one finds real numbers $x < y < x+1$ such that

$$F(y) - y = F(x) - x + 1.$$

Thus,

$$F(y) = F(x) + (y - x) + 1 > F(x) + 1 = F(x+1),$$

contradicting the monotonicity of F. □

Consider the positive integral powers (iterates) of F and write $F^q = \mathrm{id} + \Phi_q$, $q \geq 1$, where Φ_q is periodic of period 1. Let α_q denote the global minimum of Φ_q, β_q its global maximum.

LEMMA 2.2. *Let $n \geq q \geq 1$ be integers and write $n = mq + r$, m and r integers, $m > 0$, $0 \leq r < q$. Then, for all $t \in \mathbb{R}$,*

$$\frac{m\alpha_q + r\alpha_1}{mq + r} \leq \frac{F^n(t) - t}{n} \leq \frac{m\beta_q + r\beta_1}{mq + r}.$$

This key lemma is quite elementary. One notices that, for integers $m \geq 1$,

$$F^{qm}(t) - F^{q(m-1)}(t) = \Phi_q(F^{q(m-1)}(t)),$$

hence that

$$\alpha_q \leq F^{qm}(t) - F^{q(m-1)}(t) \leq \beta_q.$$

Similarly,

$$\alpha_1 \leq F^{mq+r}(t) - F^{mq+(r-1)}(t) \leq \beta_1.$$

Now an iterative argument and the application of telescoping sums gives the assertion.

THEOREM 2.3 (Poincaré). *There is a real number $\tau = \tau(F)$, (called the translation number of F) such that*

$$\lim_{n\to\infty} \frac{F^n(t) - t}{n} = \tau$$

uniformly for $-\infty < t < \infty$.

Proof. In Lemma 2.2, first fix q and let $n \to \infty$, hence also $m \to \infty$, to conclude that

$$\frac{\alpha_q}{q} \leq \liminf_{n\to\infty} \frac{F^n(t) - t}{n} \leq \limsup_{n\to\infty} \frac{F^n(t) - t}{n} \leq \frac{\beta_q}{q}.$$

Here, t is arbitrary and both the lim sup and lim inf belong to every interval $[\alpha_q/q, \beta_q/q]$, $q \geq 1$. By Lemma 2.1, these intervals have lengths less than $1/q$, shrinking to 0 as $q \to \infty$, and the assertion follows. □

This proof has the following useful corollary.

COROLLARY 2.4. *For every integer $q \geq 1$,*

$$\alpha_q = \min_{\mathbb{R}}(F^q - \mathrm{id}) \leq q\tau \leq \max_{\mathbb{R}}(F^q - \mathrm{id}) = \beta_q.$$

This result and the fact that $F^q - \mathrm{id}$ is continuous and periodic gives the following.

COROLLARY 2.5. *For every integer $q \geq 1$, there is a set of values of $t \in \mathbb{R}$ having no finite upper or lower bound and such that $F^q(t) = t + q\tau$.*

Thus, in some sense, F is "trying" to be translation by τ. It is trivial to check that the honest translation $T_c(t) = t + c$ has $\tau = c$.

If $f \in \mathcal{G}$ and $F, \widetilde{F}$ are two lifts of f, then $\widetilde{F} = F + m$ for some integer m, $\widetilde{F}^q = F^q + qm$ (since F commutes with integer translations) and

$$\tau(\widetilde{F}) = \tau(F) + m.$$

Thus, the coset $\rho(f) = \tau(F) + \mathbb{Z} \in \mathbb{R}/\mathbb{Z}$ depends only on f.

DEFINITION 2.6. For $f \in \mathcal{G}$, the number $\rho(f) \in \mathbb{R}/\mathbb{Z}$ is called the rotation number of f.

Since the rotation r_α, $\alpha = a + \mathbb{Z}$, lifts to translation by a, we have $\rho(r_\alpha) = \alpha$.

THEOREM 2.7. *A homeomorphism $f \in \mathcal{G}$ has a periodic point of period $m \in \mathbb{Z}$ if and only if $\rho(f) = n/m + \mathbb{Z}$ for some integer n.*

Proof. If the rotation number has the given form, the periodicity of f at some point $z \in S^1$ follows easily from Corollary 2.5. For the converse, if $f^m(z) = z$, some $z \in S^1$, let F be a lift and note that $F^m(t) = t + n$, some $n \in \mathbb{Z}$, where $t \in \mathbb{R}$ projects to z. Thus also $F^{rm}(t) = t + rn$ for this value of t. Letting $q = rm + s$, $0 \leq s < m$, we get

$$\frac{F^q(t)}{q} = \frac{F^s(t)}{q} + \frac{rn}{rm+s}.$$

Keeping t fixed and passing to the limit as q (hence r) goes to ∞, we see that

$$\lim_{q\to\infty} \frac{F^q(t) - t}{q} = \lim_{q\to\infty} \frac{F^q(t)}{q} = \frac{n}{m}.$$

□

COROLLARY 2.8. *If $\rho(f)$ is irrational, then the action of $\mathbb{Z}$ on S^1 generated by f has a unique minimal set, either exceptional or all of S^1. The latter is the case if f is a C^2 diffeomorphism.*

THEOREM 2.9. *Let $f, g \in \mathcal{G}$, $h : S^1 \to S^1$ a continuous map of degree 1, and suppose that $g \circ h = h \circ f$ (one says that f and g are semiconjugate by h). Then $\rho(g) = \rho(f)$.*

Proof. Let $F, H : \mathbb{R} \to \mathbb{R}$ be lifts of f and h, respectively. Then one can find a lift G of g such that $G \circ H = H \circ F$. For all integers $n \geq 1$, it follows that $G^n \circ H = H \circ F^n$, hence

$$\frac{G^n(H(t))}{n} = \frac{H(F^n(t))}{n} = \frac{H(F^n(t)) - F^n(t)}{n} + \frac{F^n(t)}{n}.$$

But $H - \mathrm{id}$ is periodic of period 1 (the degree of h), hence this function is bounded. Thus, for fixed but arbitrary $t \in \mathbb{R}$,

$$\tau(G) = \lim_{n\to\infty} \frac{G^n(H(t))}{n} = \lim_{n\to\infty} \frac{F^n(t)}{n} = \tau(F).$$

Reduced mod $\mathbb{Z}$, this gives the assertion. □

EXAMPLE 2.10. In Example 1.10, the C^1 diffeomorphism f having an exceptional minimal set was semiconjugate to r_α, with α irrational. Thus, $\rho(f) = \alpha$.

EXAMPLE 2.11. In the case that h is an orientation preserving homeomorphism, the relation in Theorem 2.9 becomes $h^{-1} \circ g \circ h = f$ and one says that f and g are topologically conjugate. In this sense, the rotation number is a topological invariant.

DEFINITION 2.12. An action $G \times S^1 \to S^1$ is free if the only element of G that has a fixed point in S^1 is the identity. The action is faithful if no nontrivial element of G acts as the identity on S^1.

Note that free actions are faithful, but not conversely.

We can now state the principal results of these notes.

THEOREM 2.13. *Let G be a group containing at least one element of infinite order. If $G \times S^1 \to S^1$ is a free action by orientation preserving C^2 diffeomorphisms, then G is topologically conjugate to a subgroup $hGh^{-1} \subset \mathrm{SO}(2)$ of rotations of S^1. In particular, G is abelian. Under the natural identification $\mathrm{SO}(2) = S^1 = \mathbb{R}/\mathbb{Z}$, the rotation number map $\rho : G \to \mathrm{SO}(2)$ is the isomorphism $g \mapsto hgh^{-1}$ onto this subgroup of rotations.*

We remark that the conjugating homeomorphism $h : S^1 \to S^1$ may not have any smoothness properties. In fact, it may not even be *absolutely continuous*. (Absolutely continuous homeomorphisms preserve the sets of Lebesgue measure zero.)

COROLLARY 2.14 (Denjoy). *If $g \in \mathrm{Diff}^2_+(S^1)$ has $\rho(g) = \alpha$ irrational, then g is topologically conjugate to the rotation r_α.*

Proof. Indeed, by Theorem 2.7, g has no finite orbit, hence nontrivial powers of g have no fixed points. Theorem 2.13 gives the assertion. □

By Example 1.10, the C^2 hypotheses in these theorems are essential. The following theorem is purely C^0.

THEOREM 2.15. *Let G be a finite group and let $G \times S^1 \to S^1$ be a free action by orientation preserving homeomorphisms. then G is topologically conjugate to a subgroup $hGh^{-1} \subset \mathrm{SO}(2)$ of rotations of S^1. In particular, G is abelian. Under the natural identification $\mathrm{SO}(2) = S^1 = \mathbb{R}/\mathbb{Z}$, the rotation number map $\rho : G \to \mathrm{SO}(2)$ is the isomorphism $g \mapsto hgh^{-1}$ onto this subgroup of rotations.*

The following theorem is closely related to Theorem 2.13.

THEOREM 2.16 (Wood [8]). *If G is an abelian group, $G \times S^1 \to S^1$ a faithful C^2 action such that some element of G has irrational rotation number, then G is topologically conjugate to a group of rotations. In particular, the action is free.*

The next section will be devoted to the proof of Theorems 2.13, 2.15 and 2.16.

3. FREE ACTIONS

We consider a free action $G \times S^1 \to S^1$ by orientation preserving homeomorphisms. For the moment there is no requirement on the group nor on the smoothness of the action. By lifting these homeomorphisms, we obtain a group action

$$\widetilde{G} \times \mathbb{R} \to \mathbb{R}$$

which is also free. Note that the canonical projection $\pi : \widetilde{G} \to G$ has as kernel exactly the group of integer translations.

Since the action is free, we can totally order the group $\widetilde{G}$ by setting $g < h$ if and only if $g(t) < h(t)$, for some, hence every, $t \in \mathbb{R}$. If $g < h$, then

$$fg < fh,$$
$$gf < hf,$$

for arbitrary $f \in \widetilde{G}$. The first inequality uses the fact that f preserves orientation. The second uses only the definition of the total order. Also, we easily see that

$$g > \mathrm{id} \text{ and } h > \mathrm{id} \Rightarrow gh > \mathrm{id},$$
$$g > \mathrm{id} \Rightarrow g^{-1} < \mathrm{id}\,.$$

We say that $\widetilde{G}$ is an *ordered* group.

LEMMA 3.1. *The above ordering makes $\widetilde{G}$ an Archimedean ordered group.*

Proof. If g and h are both $>$ id, we must show that $g^n > h$ for some integer $n \geq 1$. Otherwise,

$$0 < g(0) < g^2(0) < \cdots < g^n(0) < \cdots < h(0).$$

The least upper bound x of $\{g^n(0)\}_{n=1}^{\infty}$ satisfies $0 < x \leq h(0)$, hence is finite, and $g(x) = x$. This contradicts the hypothesis that $g > \text{id}$. □

THEOREM 3.2 (Hölder). *Every Archimedean ordered group is order isomorphic to an additive subgroup of* $\mathbb{R}$ *and, in particular, is abelian.*

This classical result is proven by Dedekind cuts. Let $(H, >)$ be an Archimedean ordered group and fix $\gamma > \text{id}$ in H. Given $f \in H$, set

$$S_f = \left\{ \frac{n}{m} \mid m \in \mathbb{Z}^+, n \in \mathbb{Z}, f^m < \gamma^n \right\}.$$

One checks that this is the upper half of a Dedekind cut and sets $\varphi(f)$ equal to the cut number. It can be shown that $\varphi : H \to \mathbb{R}$ is the unique order preserving group homomorphism (necessarily injective) such that $\varphi(\gamma) = 1$. Details are given in Appendix B.

COROLLARY 3.3. *If* $G \times S^1 \to S^1$ *is free, then* G *is an abelian group.*

Indeed, the above discussion has shown that the lift $\widetilde{G}$ is abelian and G is a quotient of $\widetilde{G}$.

We now consider probability measures ν on S^1. That is, ν is a regular, nonnegative Borel measure with $\nu(S^1) = 1$. We will say that a measure is *atomic* if there is a point of positive measure.

DEFINITION 3.4. The measure ν is said to be continuous if it is nonatomic and takes strictly positive values on open subarcs of S^1.

DEFINITION 3.5. Given a group action $G \times S^1 \to S^1$ and a probability measure ν on S^1, we say that ν is G–invariant if, for every $g \in G$ and every Borel set $B \subseteq S^1$, $\nu(gB) = \nu(B)$.

REMARK. Given a Borel map $f : S^1 \to S^1$ and a measure ν on S^1, there is a "push–forward" measure $\mu = f_*\nu$ defined on each Borel set $B \subseteq S^1$ by $\mu(B) = \nu(f^{-1}(B))$. Applying this notion to $f \in G$, we see that ν is G–invariant if and only if $f_*\nu = \nu$, for all $f \in G$.

PROPOSITION 3.6. *If* G *is a finite group acting on* S^1 *by homeomorphisms, then there is a continuous* G*–invariant probability measure on* S^1.

Proof. Indeed, start with any continuous probability measure ν (Lebesgue measure, for example) and average it over the group:

$$\mu = \sum_{g \in G} \frac{g_*\nu}{|G|},$$

where $|G|$ denotes the cardinality of G. □

We recall that the *support* of the measure ν is the set of points $x \in S^1$ such that ν is strictly positive on every neighborhood of x. This is designated by $\operatorname{supp} \nu$. The reader can check that $\operatorname{supp} \nu$ is a closed subset of S^1 and that, if ν is G–invariant, so is $\operatorname{supp} \nu$.

LEMMA 3.7. *If the action $G \times S^1 \to S^1$ has S^1 itself as minimal set, then every G–invariant probability measure is continuous.*

Proof. Indeed, $\operatorname{supp} \nu = S^1$, so ν is strictly positive on all open subarcs. Furthermore, no orbit is finite, hence, if ν were atomic, G–invariance would imply that $\nu(S^1) = \infty$. □

Let $C^0(S^1)$ denote the space of continuous, $\mathbb{R}$–valued functions on S^1. Every regular, bounded Borel measure μ on S^1 determines a linear functional on the vector space $C^0(S^1)$ by

$$\mu(h) = \int_{S^1} h \, d\mu, \qquad \forall\, h \in C^0(S^1).$$

By the Riesz representation theorem [5], the measure μ is completely determined by this associated linear functional. If $f : S^1 \to S^1$ is continuous, we also have the formula

$$f_*\mu(h) = \int_{S^1} h \circ f \, d\mu = \mu(h \circ f), \qquad \forall\, h \in C^0(S^1).$$

In the proof of the following proposition, we will use the well known fact that the set of probability measures on a compact space is countably compact [2]. This means that every sequence $\{\nu_k\}_{k=1}^{\infty}$ of probability measures on S^1 has a weakly convergent subsequence. More precisely, there is a probability measure μ and a subsequence $\{\nu_{k_n}\}_{n=1}^{\infty}$ such that

$$\lim_{n \to \infty} \nu_{k_n}(h) = \mu(h), \qquad \forall\, h \in C^0(S^1).$$

PROPOSITION 3.8. *If g is an orientation preserving homeomorphism of S^1 without periodic points, then the action $\mathbb{Z} \times S^1 \to S^1$ generated by g admits an invariant probability measure μ. If g is a C^2 diffeomorphism, μ is continuous.*

Proof. Choose an arbitrary probability measure ν and note that, for each $k \geq 1$,

$$\nu_k = \frac{\nu + g_*\nu + \cdots g_*^k \nu}{k}$$

is a probability measure. Let μ be the weak limit of a suitable subsequence of $\{\nu_k\}_{k=1}^{\infty}$ and note that the sequence of signed measures

$$\nu_k - g_*\nu_k = \frac{\nu - g_*^{k+1}\nu}{k}$$

converges weakly to zero. It follows that μ is g–invariant. Finally, if g is a C^2 diffeomorphism, Corollary 1.12 guarantees that S^1 is the g–minimal set, hence Lemma 3.7 guarantees that μ is continuous. □

We assume that the free, orientation preserving action $G \times S^1 \to S^1$ admits a continuous, G–invariant probability measure μ and use this to construct an orientation preserving homeomorphism $h : S^1 \to S^1$ such that hGh^{-1} is a group of rotations.

To begin with, we can lift μ uniquely to a continuous, σ–finite measure $\widetilde{\mu}$ on $\mathbb{R}$ via the covering map $p : \mathbb{R} \to S^1$. Indeed, any borel set $B \subseteq [n, n+1)$, $n \in \mathbb{Z}$, is carried one–to–one onto a Borel set $p(B) \subseteq S^1$ and we set $\widetilde{\mu}(B) = \mu(p(B))$. For general Borel sets $B \subseteq \mathbb{R}$, set $B_n = B \cap [n, n+1)$, $n \in \mathbb{Z}$ and define

$$\widetilde{\mu}(B) = \sum_{n=-\infty}^{\infty} \widetilde{\mu}(B_n).$$

It is elementary that, relative to the lifted action

$$\widetilde{G} \times \mathbb{R} \to \mathbb{R},$$

$\widetilde{\mu}$ is $\widetilde{G}$–invariant.

Define a map $H : \mathbb{R} \to \mathbb{R}$ by

$$H(x) = \begin{cases} \widetilde{\mu}[0, x], & x \geq 0, \\ -\widetilde{\mu}[x, 0], & x \leq 0. \end{cases}$$

By the continuity of $\widetilde{\mu}$, this function is strictly increasing without jump discontinuities, hence is one–to–one and continuous. Since $\widetilde{\mu}$ is unbounded on $[0, \infty)$ and $(-\infty, 0]$, H is also onto. Finally, by the Brouwer theorem on invariance of domain, H is a homeomorphism.

LEMMA 3.9. *If $F \in \widetilde{G}$, then HFH^{-1} is a translation.*

Proof. By the definition of H, $\widetilde{\mu}[a, b] = H(b) - H(a)$, for every closed, bounded interval $[a, b]$. By this remark and the $\widetilde{G}$–invariance of $\widetilde{\mu}$, we obtain

$$b - a = \widetilde{\mu}[H^{-1}(a), H^{-1}(b)] = \widetilde{\mu}[FH^{-1}(a), FH^{-1}(b)] = HFH^{-1}(b) - HFH^{-1}(a).$$

That is, HFH^{-1} carries each $[a, b]$ onto an interval of the same length. As an orientation–preserving isometry of $\mathbb{R}$, HFH^{-1} is a translation. □

Proof of Theorems 2.13, 2.15 and 2.16. For an infinite cyclic group $\mathbb{Z}$, acting freely on S^1 by orientation preserving C^2 diffeomorphisms, our discussion thus far has produced an orientation preserving homeomorphism $H : \mathbb{R} \to \mathbb{R}$ that conjugates the lifted group action to a subgroup $H\widetilde{\mathbb{Z}}H^{-1}$ of the group of translations. By the definition of H and the fact that μ is a probability measure on S^1, it follows that $H(x + 1) = H(x) + 1$, for all $x \in \mathbb{R}$, hence that H is a lift of a homeomorphism $h : S^1 \to S^1$. For each $f \in \mathbb{Z}$, hfh^{-1} lifts to a translation HFH^{-1}, hence is itself a rotation.

If the group G acts freely by orientation preserving C^2 diffeomorphisms and has an element g of infinite order, let $hgh^{-1} = r_\alpha$ be the rotation produced above. Here, α is necessarily irrational by Theorem 2.7. For general $f \in G$, let $\overline{f} = hfh^{-1}$. Fix a point $x_0 \in S^1$ and let r_β be the rotation such that $\overline{f}(x_0) = r_\beta(x_0)$. Using the fact that G is abelian, we see that

$$\overline{f}(r_\alpha^n(x_0)) = r_\alpha^n(\overline{f}(x_0)) = r_\alpha^n(r_\beta(x_0)) = r_\beta(r_\alpha^n(x_0)),$$

for every integer n. That is, $\overline{f}$ and r_β agree on the dense r_α–orbit of x_0, hence agree everywhere on S^1. Note that no two distinct elements f_1 and f_2 are conjugated to the same rotation, as this would imply that $f_1 f_2^{-1}$ acts as the identity transformation of S^1.

In the above argument, the freeness of the action was only used to guarantee that G is abelian and acts faithfully. Thus, Theorem 2.16 is proven by the same argument.

If the group G is finite and acts freely as orientation preserving homeomorphisms of S^1, Proposition 3.6 gives the continuous, G–invariant measure that is then used as above to produce the desired conjugating homeomorphism h.

Finally, since the rotation number is a topological invariant, the map

$$\rho : G \to \mathbb{R}/\mathbb{Z} = \mathrm{SO}(2)$$

is naturally equivalent to the map $f \mapsto hfh^{-1}$. □

Appendix A. Sacksteder's Theorem

The finitely generated group G is acting on S^1 as a group of orientation preserving, C^2 diffeomorphisms having an exceptional minimal set X. Let

$$G_1 = \{h_1, h_2, \ldots, h_n\}$$

be a generating set for G, assumed to be *symmetric* in the sense that G_1 contains also the inverse of each of its elements. Since S^1 is locally isometric to $\mathbb{R}$, first and second derivatives of elements of G are well defined and bounded. We choose positive constants A and B so that, for $1 \le i \le n$,

$$h_i' > A,$$
$$|h_i''| \le B,$$

uniformly on S^1. Set

$$\theta = B/A$$

and

$$\lambda = \exp(2\theta).$$

We establish some conventions. If u and $v \in S^1$, we let uv denote the counterclockwise oriented arc from u to v. In case $u = v$, we remove the ambiguity by decreeing that $uu = \{u\}$. The length of an arc J is measured by the length of any lift of J to an interval in $\mathbb{R}$ and will be denoted by $|J|$. We also write $|S^1| = 1$. If $g = h_{i_m} h_{i_{m-1}} \cdots h_{i_1}$, we set $g_p = h_{i_p} \cdots h_{i_1}$, for $0 \le p \le m$. Here it is understood that $g_0 = \mathrm{id}$. Similarly, for a point $u \in S^1$ (respectively, for an arc $J \subset S^1$) we write $u_p = g_p u$ (respectively, $J_p = g_p J$), $0 \le p \le m$. Again, $u_0 = u$ and $J_0 = J$.

Lemma A.1. *If $g = h_{i_m} h_{i_{m-1}} \cdots h_{i_1}$ is as above and $u, v \in S^1$ are distinct points, then*

$$\frac{g'(u)}{g'(v)} < \exp\left(\theta \sum_{p=0}^{m} |u_p v_p|\right).$$

Proof. First, for each $h \in G_1$ we have

$$\begin{aligned}
0 &< \frac{h'(u)}{h'(v)} \\
&= \left| 1 + \frac{h'(u) - h'(v)}{h'(v)} \right| \\
&\le 1 + \left| \frac{h'(u) - h'(v)}{h'(v)} \right| \\
&\le 1 + \left| \frac{h''(\xi)}{h'(v)} \right| |uv| \\
&< 1 + \theta |uv| \\
&\le \exp(\theta |uv|),
\end{aligned}$$

where $\xi \in uv$ is given by the mean value theorem. Using this and the chain rule, we obtain

$$\begin{aligned}\frac{g'(u)}{g'(v)} &= \frac{h'_{i_m}(u_{m-1})h'_{i_{m-1}}(u_{m-2})\cdots h'_{i_1}(u_0)}{h'_{i_m}(v_{m-1})h'_{i_{m-1}}(v_{m-2})\cdots h'_{i_1}(v_0)}\\ &= \prod_{p=0}^{m-1}\frac{h'_{i_{p+1}}(u_p)}{h'_{i_{p+1}}(v_p)}\\ &< \prod_{p=0}^{m-1}\exp(\theta|u_pv_p|)\\ &= \exp\left(\theta\sum_{p=0}^{m-1}|u_pv_p|\right).\end{aligned}$$

□

Remark. The above proof shows equally well that

$$\frac{g'(u)}{g'(v)} < \exp\left(\theta\sum_{p=0}^{m}|v_pu_p|\right).$$

Indeed, in the first string of inequalities, the interval uv can be replaced by vu without otherwise reversing the roles of u and v. In this case, ξ is chosen in vu.

Definition A.2. The word $g = h_{i_m}h_{i_{m-1}}\cdots h_{i_1}$ is a simple chain at the point $u = u_0$ if the points $u_0, u_1, \dots, u_m$ are all distinct. Similarly, g is a simple chain at the arc $J = J_0$ if the arcs $J_0, J_1, \dots, J_m$ are all disjoint.

Now let $X \subset S^1$ be a G–invariant Cantor set. At the moment, it is not required that X be G–minimal. Note that if $J = xy$ is a gap of this Cantor set (that is, $J \cap X = \{x, y\}$), then a word g as above is a simple chain at x (respectively, at y) if and only if it is a simple chain at xy.

Lemma A.3 (Key Lemma). *Let J_0 be a gap of X, K_0 a compact subarc of S^1 such that*

- *$J_0 \cap K_0 = \{x_0\}$ is a single point of ∂J_0 (hence $J_0 \cup K_0$ is a proper subarc of the circle);*
- *$|K_0|/|J_0| \le 1/\lambda$.*

If $g \in G$ is a simple chain at x_0, then

(1) $|gK_0| < |gJ_0|$,
(2) $g'(u)/g'(v) < \lambda$, $\forall u, v \in J_0 \cup K_0$.

Proof. Since $\lambda > 1$, it is clear that $|K_0| < |J_0|$. We set $K_p = g_pK_0$ and $J_p = g_pJ_0$ and assume, inductively on p, that $|K_i| < |J_i|$, $0 \le i \le p-1$. If, in (2), $u = v$, the assertion is trivial since $\lambda > 1$. Thus, assume these points are distinct and, for definiteness, assume that $uv \subseteq J_0 \cup K_0$. If $vu \subseteq J_0 \cup K_0$, the only modification required in the following is in the right hand side of the first inequality.

$$\begin{aligned}\frac{g_p'(u)}{g_p'(v)} &< \exp\left(\theta \sum_{i=0}^{p-1} |u_i v_i|\right) \\ &\leq \exp\left(\theta \sum_{i=0}^{p-1} |K_i \cup J_i|\right) \\ &< \exp\left(\theta \sum_{i=1}^{p-1} 2|J_i|\right), \qquad \text{(inductive hypothesis)} \\ &\leq \exp(2\theta) \\ &= \lambda,\end{aligned}$$

since each J_i appears exactly once and all are disjoint. By the mean value theorem, there are $u \in K_0$ and $v \in J_0$ such that

$$\frac{|K_p|}{|J_p|} = \frac{g_p'(u)|K_0|}{g_p'(v)|J_0|} < \lambda \frac{1}{\lambda} = 1.$$

By finite induction on p, the assertions follow. □

Let $J_0 = u_0 v_0$ be a gap of X. If $g = h_{i_m} \circ \cdots \circ h_{i_1}$ is a word in elements of G_1 and g cannot be expressed as a shorter word, set $|g| = m$ and call this the *length* of g. Denote by $\mathcal{C}_{u_0}$ the set of chains at u_0. For each $u \in Gu_0$, set

$$n(u) = \min\{|g| \mid g \in \mathcal{C}_{u_0},\ gu_0 = u\}.$$

Definition A.4. If $g \in \mathcal{C}_{u_0}$, $g(u_0) = u$, and $|g| = n(u)$, then g is called a *shortcut* from u_0 to u.

Remark that a shortcut is necessarily a simple chain at u_0. It is elementary that shortcuts exist from u_0 to each $u \in Gu_0$.

Proof of Theorem 1.11. We now assume that X is a G–minimal Cantor set, with $J_0 = u_0 v_0$ a gap of X. Choose K_0 as in Lemma A.3 so that, say, $\{u_0\} = J_0 \cap K_0$. By minimality, Gu_0 clusters at u_0 and we can choose $z \in K_0 \cap Gu_0$. Let g_z be a shortcut from u_0 to z. This being a simple chain at u_0, Lemma A.3 ensures that $|g_z K_0| < |g_z J_0|$. Since z can be chosen as close to u_0 as desired, these intervals are as small as desired and as close to u_0 as desired, hence we can assume that $g_z K_0 \subset \operatorname{int} K_0$. We also assume that $|g_z J_0| < \delta$, where $\delta > 0$ is so small that $\lambda\delta/|K_0| < 1$. By the mean value theorem, there is $y_0 \in K_0$ such that

$$g_z'(y_0)|K_0| = |g_z K_0| < \delta.$$

By Lemma A.3, every $y \in K$ satisfies

$$g_z'(y) < \lambda g_z'(y_0) < \lambda\delta/K_0 < 1.$$

It follows that

$$g_z : K_0 \to \operatorname{int} K_0$$

is a contraction mapping, hence has a fixed point $x_0 \in \operatorname{int} K_0$ to which g_z contracts K_0. Since $K_0 \cap X \neq \emptyset$, x_0 is a cluster point of X, hence $x_0 \in X$. Finally, we also have $g_z'(x_0) < 1$. □

Appendix B. Hölder's Theorem

We consider an Archimedean ordered group $(G, >)$ and prove that it is order isomorphic to an additive subgroup of $\mathbb{R}$. In fact, given $g \in G$, $g > \mathrm{id}$ the order preserving isomorphism φ will be uniquely determined by the requirement that $\varphi(g) = 1$. For a different proof of this theorem, the reader can consult [4, pp. 186-190].

The basic properties of the order relation are that it is a total order (any two distinct elements of G are comparable via $>$) and that, whenever $h > g$ and $f \in G$, then

$$\begin{aligned} fh &> fg, \\ hf &> gf. \end{aligned}$$

Elementary consequences are

$$(\#) \qquad g > h \Rightarrow h^{-1} > g^{-1},$$

$$(\#\#) \qquad g > h \iff g^m > h^m, \quad \forall\, m \geq 1.$$

The second of these properties is established by a simple induction, left to the reader. As usual, one writes $g \geq h$ as shorthand for "$g > h$ or $g = h$". We also use "$\leq$" and "$<$" in the usual ways

One sets $G_+ = \{g \in G \mid g > \mathrm{id}\}$. The Archimedean property is that, whenever $f, g \in G_+$, there is an integer $m \geq 1$ such that $f^m > g$.

Lemma B.1. *If $gh \leq hg$ and $m \geq 1$, then*

$$g^m h^m \leq (gh)^m \leq h^m g^m.$$

Proof. The inequalities are trivial for $m = 1$. Assume that they are true for $m - 1$, some $m \geq 2$. For the first, write

$$\begin{aligned} (gh)^m &= (gh)^{m-1} gh \\ &\geq g^{m-1} h^{m-1} gh \\ &= g^{m-1} h^{m-2} hgh \\ &\geq g^{m-1} h^{m-2} gh^2. \end{aligned}$$

Iterating this argument, keep pushing an h on the left of g to the right, using the inequality $hg \geq gh$, until the desired inequality has been reached. For the second inequality, write

$$\begin{aligned} (gh)^m &= gh(gh)^{m-1} \\ &\leq ghh^{m-1} g^{m-1} \\ &\leq hgh^{m-1} g^{m-1} \\ &= h(gh)h^{m-2} g^{m-1} \\ &\leq h^2 gh^{m-2} g^{m-1}. \end{aligned}$$

Iterating this procedure, continue pushing an h on the right of g to the left, using the inequality $gh \leq hg$, until the desired inequality has been reached. □

Fix $\gamma \in G_+$. We want to produce an order–preserving group monomorphism $\varphi : G \to \mathbb{R}$ such that $\varphi(\gamma) = 1$.

LEMMA B.2. *If φ exists, it is unique.*

Proof. If m and n are integers, $m \geq 1$, and $f \in G$ is arbitrary, then

$$f^m < \gamma^n \iff m\varphi(f) < n\varphi(\gamma) = n \iff \varphi(f) < n/m.$$

Similarly,

$$f^m > \gamma^n \iff \varphi(f) > n/m,$$
$$f^m = \gamma^n \iff \varphi(f) = n/m.$$

Thus, $\varphi(f)$ is determined by the fact that $\mathbb{Q}$ is dense in $\mathbb{R}$. □

The construction of φ is forced by the proof of Lemma B.2. Given $f \in G$, set

$$S_f = \left\{ \frac{n}{m} \mid m, n \in \mathbb{Z}, m > 0, f^m < \gamma^n \right\}.$$

LEMMA B.3. *The set S_f is the upper half of a Dedekind cut in $\mathbb{Q}$.*

Proof. By the Archimedean property, $S_f \neq \emptyset$. Indeed, if $f \in G_+$, there is a positive integer n such that $f < \gamma^n$ and $n \in S_f$. If $f \notin G_+$, then $f < \gamma$ and $1 \in S_f$. Similarly, by the Archimedean property and (#), there is a negative integer n such that $f > \gamma^n$, hence $S_f \neq \mathbb{Q}$. To show the cut property, we need to show that, if $p/q \geq n/m \in S_f$, $q > 0$, then $p/q \in S_f$. But

$$f^m < \gamma^n \Rightarrow f^{mq} < \gamma^{nq}$$

by (##). We are given that $pm \geq nq$ and so $\gamma^{nq} \leq \gamma^{pm}$. Thus, we obtain

$$f^{mq} < \gamma^{nq} \leq \gamma^{mp} \text{ and this } \Rightarrow f^q < \gamma^p \Rightarrow \frac{p}{q} \in S_f,$$

where the first implication is again by (##). □

Thus, for each $f \in G$, we define $\varphi(f) = \inf S_f$.

LEMMA B.4. $\varphi(\gamma) = 1$.

Proof. Indeed, if $n, m \in \mathbb{Z}$ and $m > 0$,

$$\gamma^m < \gamma^n \iff \gamma^{m-n} < \text{id} \iff m - n < 0 \text{ (since } \gamma > \text{id)} \iff \frac{n}{m} > 1.$$

It follows that $\inf S_\gamma = 1$. □

LEMMA B.5. $\varphi(\text{id}) = 0$.

Proof. Indeed, appealing to the fact that $\gamma > \text{id}$, one sees that

$$S_{\text{id}} = \left\{ \frac{n}{m} \mid m > 0 \text{ and } n > 0 \right\},$$

hence $\inf S_{\text{id}} = 0$. □

LEMMA B.6. *If $h, g \in G$ and $gh \leq hg$, then $\varphi(gh) = \varphi(g) + \varphi(h)$.*

Proof. First we prove that, if $n/m \in S_g$ and $p/q \in S_h$, then the sum of these fractions belongs to S_{gh}. This will give $\varphi(gh) \leq \varphi(g) + \varphi(h)$. By Lemma B.1,

$$(gh)^{mq} \leq h^{mq} g^{mq}.$$

By the definition of S_g and S_h, we have

$$h^{mq} < \gamma^{mp}$$
$$g^{mq} < \gamma^{nq},$$

and so

$$(gh)^{mq} < \gamma^{mp+nq}.$$

That is,

$$\frac{nq+mp}{mq} \in S_{gh}.$$

For the inequality $\varphi(gh) \geq \varphi(g)+\varphi(h)$, we prove that, if $n/m \notin S_g$ and $p/q \notin S_h$, then the sum of these fractions does not belong to S_{gh}. By Lemma B.1,

$$(gh)^{mq} \geq g^{mq}h^{mq}.$$

By the definition of S_g and S_h, we have

$$g^{mq} \geq \gamma^{nq}$$
$$h^{mq} \geq \gamma^{mp},$$

and so

$$(gh)^{mq} \geq \gamma^{nq+mp}.$$

That is,

$$\frac{nq+mp}{mq} \notin S_{gh}.$$

□

Lemma B.7. *For arbitrary $g \in G$, $\varphi(g^{-1}) = -\varphi(g)$*

Proof. Indeed, $g^{-1}g \leq gg^{-1}$ and Lemmas B.5 and B.6 give

$$0 = \varphi(\mathrm{id}) = \varphi(g^{-1}g) = \varphi(g^{-1}) + \varphi(g).$$

□

Lemma B.8. *If $h, g \in G$ and $gh \geq hg$, then $\varphi(gh) = \varphi(g) + \varphi(h)$.*

Proof. By (#), we have $h^{-1}g^{-1} \leq g^{-1}h^{-1}$, and so Lemma B.6 implies that

$$\varphi(h^{-1}g^{-1}) = \varphi(g^{-1}) + \varphi(h^{-1}).$$

By Lemma B.7, the desired equality follows. □

The lemmas proven thus far establish that φ is a homomorphism of the group G into $\mathbb{R}$.

Lemma B.9. *The homomorphism φ is injective.*

Proof. Suppose that $\varphi(g) = 0$. Equivalently, $1/m \in S_g$ and so $g^m < \gamma$, for all positive integers m. By the Archimedean property, $g \leq \mathrm{id}$. Similarly $g^{-1} \leq \mathrm{id}$, hence an application of (#) proves that $g = \mathrm{id}$. □

Our final lemma completes the proof of Theorem 3.2.

Lemma B.10. *If $g, h \in G$ and $g \leq h$, then $\varphi(g) \leq \varphi(h)$.*

Proof. Let $p/q \in S_h$. Then, appealing to (##), we obtain

$$g^q \leq h^q < \gamma^p,$$

which implies that $p/q \in S_g$. That is, $S_h \subseteq S_g$ and $\varphi(g) \leq \varphi(h)$. □

References

[1] A. Denjoy. Sur les courbes définies par les équations différentielles à la surface du tore. *J. Math. Pures Appl.*, **11**:333–375, 1932.

[2] J. Dieudonné. *Eléments d'Analyse, Vol 2.* Gauthiers-Villars, Paris, 1969.

[3] C. Godbillon. *Dynamical Systems on Surfaces.* Springer–Verlag, New York, NY, 1983. Translated by H. G. Helfenstein.

[4] G. Hector and U. Hirsch. *Introduction to the Geometry of Foliations, Part B.* Vieweg and Sohn, Braunschweig, 1983.

[5] W. Rudin. *Real and Complex Analysis.* McGraw–Hill, New York, NY, 2nd edition, 1974.

[6] R. Sacksteder. Foliations and pseudogroups. *Amer. J. Math.*, **87**:79–102, 1965.

[7] P. Schweitzer. Counterexamples to the Seifert conjecture and opening closed leaves of foliations. *Ann. of Math.*, **100**:386–400, 1974.

[8] J. Wood. Foliated S^1–bundles and diffeomorphisms of S^1. In *Proc. Sympos. Univ. Bahia, Salvador, 1971*, pages 671–681, New York, 1973. Academic Press.