ON THE UNIQUENESS OF POLISH GROUP TOPOLOGIES

by

Bojana Pejić
MA, University of Pittsburgh, 2006
MMath, University of Oxford, 2002

Submitted to the Graduate Faculty of the Department of Mathematics in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

University of Pittsburgh
2007
ON THE UNIQUENESS OF POLISH GROUP TOPOLOGIES

Bojana Pejić, PhD

University of Pittsburgh, 2007

This is where the abstract goes.
# TABLE OF CONTENTS

1.0 INTRODUCTION ......................................................... 1
  1.1 Outline and Structure of Thesis .......................... 1

2.0 BACKGROUND .......................................................... 5
  2.1 Polish Spaces and Groups .................................. 5

3.0 GENERAL THEORY ....................................................... 9
  3.1 Automatic Continuity and Uniqueness of Topology ....... 9
  3.2 Separating Group ................................................. 12
  3.3 Identity and Verbal Sets ....................................... 14
  3.4 Topological Status of Identity and Verbal Sets ......... 16
  3.5 Uniqueness and Identity Sets ................................. 18
  3.6 Difficulties Extending to Analytic Sets .................... 19
  3.7 Uniqueness and Verbal Sets .................................. 22
  3.8 Locally Compact Separable Metrizable Group Topology .... 24

4.0 APPLICATIONS .......................................................... 26
  4.1 Infinite Symmetric Group ....................................... 26
  4.2 Compact Lie Groups ............................................. 29
  4.3 Profinite Groups .................................................. 33

5.0 COMPLEXITY OF VERBAL SETS ..................................... 37
  5.1 Abelian Groups ................................................... 38
  5.2 Infinite Symmetric Group ....................................... 38
      5.2.1 Set of Squares ........................................... 39
      5.2.2 Set of \( m \)-th Powers ................................. 43
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.3</td>
<td>Autohomeomorphism Group of the Unit Interval</td>
<td>45</td>
</tr>
<tr>
<td>5.4</td>
<td>Autohomeomorphism Group of the Unit Circle</td>
<td>48</td>
</tr>
<tr>
<td>5.4.1</td>
<td>Definitions and Notation</td>
<td>50</td>
</tr>
<tr>
<td>5.4.2</td>
<td>The Proof</td>
<td>52</td>
</tr>
<tr>
<td>5.5</td>
<td>Automorphism Group of the Rational Circle</td>
<td>62</td>
</tr>
<tr>
<td>5.5.1</td>
<td>Definitions and Notation</td>
<td>64</td>
</tr>
<tr>
<td>5.5.2</td>
<td>The Proof</td>
<td>65</td>
</tr>
</tbody>
</table>

**BIBLIOGRAPHY**                                  | 72   |
LIST OF FIGURES

1  Sequence \((a_{n,r})\) ....................................................... 47
2  Showing completeness of an analytic set. .......................... 49
3  A function in \(M\) and its inverse. ................................. 52
4  Sequences \((a_{n,0})\) and \((b_{n,0})\). ................................. 53
5  A square root of \(f \mid A\). .............................................. 54
6  Intervals \((s_n, t_n)\) for \(n = 0, 1, \ldots, 4\), when \(2 < a_3 < a_1 < a_4\). .............................. 57
7  Map \(F(\alpha)\). ........................................................... 59
8  Map \(F(\alpha)\). ........................................................... 68
1.0 INTRODUCTION

1.1 OUTLINE AND STRUCTURE OF THESIS

This will be revised in the end... A Polish group is a topological group that is separable and metrizable by a complete metric. These groups are ubiquitous in mathematics — to understand a mathematical object one often needs to understand its symmetries, and groups of symmetries of reasonably small objects come naturally equipped with a topological structure making them into a Polish group. Banach spaces, unitary groups of separable Hilbert spaces, automorphism groups, Lie groups, automorphism groups of first order structures, profinite groups etc. are some of the examples of Polish groups.

When does a group admit a unique Polish group topology?

This question is an important part of the greater, and intensively studied, problem of the size and structure of the lattice of group topologies on a topological group. Further, the problem of the existence of a unique topological group topology of some type is closely related to the problem of automatic continuity — under what conditions on groups or homomorphism can we deduce that an algebraic homomorphism between topological groups must automatically be continuous?

Both problems — automatic continuity and uniqueness of certain types of topology — have come to the fore in a diverse range of subject areas. The study of automatic continuity in Banach algebras has been very fertile (see Dales’s comprehensive Banach algebras and automatic continuity, [4]). One of the fundamental problems in the theory of profinite (i.e. compact zero-dimensional) groups is Serre’s Conjecture which essentially asks if every finitely generated profinite group has a unique profinite group topology. And the problem of recovering the model from an automorphism group of a first order
structure is equivalent to asking which automorphism groups have a unique Polish group topology.

A classical result due to Mackey [18], says that if a Polish group has a countable point-separating family of sets that are Borel in any Polish group topology on that group, then the group admits only one Polish group topology. (Here, a family $\mathcal{C}$ of subsets of $G$ is point-separating if for any pair of distinct points $x$ and $y$ in $G$, there is $C \in \mathcal{C}$ such that $x \in C$ and $y \notin C$.) The difficulty in applying Mackey’s theorem is deciding which sets are Borel in any Polish group topology on the group.

If $G$ is a topological group, the subsets of $G$ of the form \( \{ x \in G \mid w(x; a_1, \ldots, a_m) = 1 \} = w^{-1}\{1\} \), where $w$ is a free word and $a_1, \ldots, a_m \in G$, are called the identity sets. The sets of the form \( \{ w(x_1, \ldots, x_n; a_1, \ldots, a_m) \mid x_1, \ldots, x_n \in G \} \), are said to be verbal. If no constants are used in the definition of a verbal set then we call it a full verbal set. For example, centralizers are identity sets, conjugacy classes are (non–full) verbal sets, while $m$-th powers and commutators are examples of full verbal sets.

Note that the identity sets are necessarily closed, and hence Borel, in any Polish group topology on a given Polish group. Hence they are ideal candidates for the countable point-separating family in Mackey’s theorem. Indeed, Kallman [14] used identity sets to show that the autohomeomorphism groups of manifolds admit a unique Polish group topology. Also, identity sets can be used to show that $S_\infty$ admits only one Polish group topology. However, the identity sets are sometimes not sufficient. For example, it follows from Lemma 34 that in the Lie group $SO(3)$ no countable collection of identity sets separates points, and so the identity sets alone can not be used in applying Mackey’s result.

Thus we are forced to move beyond identity sets. Verbal sets are natural candidates. But while verbal sets are clearly analytic (the continuous images of a Polish space) it is not clear if they are Borel, as demanded by Mackey’s Theorem. We show that in Abelian Polish groups (Theorem ??) and in the infinite symmetric group $S_\infty$ (Theorem ??) all full verbal sets are Borel. Further, in a general Polish group all conjugacy classes are Borel (This follows from the fact [19] that all orbits of a Polish group acting continuously on a Polish space are Borel: apply this to the conjugation action of the Polish group on itself). So one might anticipate verbal sets would also be Borel in any Polish group. However, the
example of the squares of the autohomeomorphism group of the circle, which we show is
not Borel, dispels this hope.

This leads us to try to extend Mackey’s theorem by allowing analytic (but not neces-
sarily Borel) sets in the countable point-separating family. The authors can not completely
rule out such an extension, but in the second section we show that any such result can not
be proved by the same technique as used by Mackey.

However, other variants of Mackey’s theorem bring success. Theorems 23 and 24
of section 3, give sufficient conditions for the uniqueness of a Polish group topology,
that avoid the problem of verbal sets not being necessarily Borel. It only requires sets
that possess the Baire property, and the collection of all Baire property sets is a \( \sigma \)-algebra
containing all analytic sets. Thus, any set from the \( \sigma \)-algebra generated by the identity
and verbal sets may be used in applying this theorem.

We give two applications of these results. The first (Theorem ??) is that the compact
connected simple Lie groups with trivial center (for example, \( SO(3) \)) have a unique Polish
group topology. The second application is that the finitely generated profinite groups
admit a unique Polish group topology (Theorem 37).
PART I

UNIQUENESS OF POLISH GROUP TOPOLOGIES
2.0 BACKGROUND

2.1 POLISH SPACES AND GROUPS

In this section we give a summary of basic notions and facts about Polish spaces and groups. All of these can be found in [15] and [1], which are our main references for descriptive set theory.

A Polish space is a separable topological space that is metrizable by a complete metric. We call the topology of such a space Polish.

Recall that a σ-algebra $S$ on a set $X$ is the collection of subsets of $X$ containing the empty set and closed under the operations of complements and countable unions. The pair $(X, S)$ is then called a measurable space. Given a collection $A$ of subsets of $X$, the smallest σ-algebra containing $A$ is called the σ-algebra generated by $A$ and is denoted by $\sigma(A)$.

In a topological space $(X, \tau)$, the set of Borel sets is the σ-algebra generated by the open sets. It is denoted by $\mathcal{B}(X, \tau)$, or simply $\mathcal{B}(X)$, when confusion is impossible. If $X$ is metrizable (so that every closed set is a $G_\delta$-set), the set $\mathcal{B}(X)$ of Borel sets ramifies into a transfinite hierarchy of length at most $\omega_1$. In the first level are the open sets and the closed sets, in the second level the $G_\delta$’s (countable intersections of open sets) and $F_\sigma$’s (countable unions of closed sets), in the third level the $F_{\sigma\delta}$’s and $G_{\delta\sigma}$’s, etc.

A measurable space $(X, \mathcal{S})$ is a standard Borel space if there is a Polish topology $\tau$ on $X$ with $\mathcal{S} = \sigma(\tau)$.

In a topological space $X$, a set is called nowhere dense if its closure has empty interior. A set is meager (or first category) if it is the union of a countable collection of nowhere dense sets. A set $A$ is said to have the Baire property if there is an open set $U$ such that
the symmetric difference $A \Delta U = (A \setminus U) \cup (U \setminus A)$ is meager. The sets having the Baire property form the smallest $\sigma$-algebra containing all open sets and all meager sets.

A function $f : X \rightarrow Y$ is Borel measurable, or Borel, if the inverse image of any open set in $Y$ is Borel in $X$. Similarly, we say that a map $f : X \rightarrow Y$ is Baire measurable if the inverse image of every open set in $Y$ has the Baire property in $X$. Every Borel set has the Baire property and so every Borel function is Baire measurable.

A subset $A$ of a Polish space $X$ is analytic if it is the continuous image of a Polish space, or, equivalently, of any Borel subset of a Polish space. Borel sets are analytic, but not vice versa. A subset of $X$ is co-analytic if it is the complement of an analytic set. The class of analytic sets is closed under continuous images and countable intersections and unions. The class of co-analytic sets is closed under countable intersections and unions.

An analytic set $B$ in a Polish space $Y$ is complete if for any Polish space $X$ and any analytic set $A$ in $X$ there is a continuous function $F : X \rightarrow Y$ such that $F^{-1}(B) = A$. Such a function is called a continuous reduction of $A$ to $B$. Kechris showed in [16] that it is sufficient to find a Borel reduction, that is: an analytic set $B$ in a Polish space $Y$ is complete if and only if for any Polish space $X$ and any analytic set $A$ in $X$ there is a Borel function $F : X \rightarrow Y$ such that $F^{-1}(B) = A$.

A true analytic set is an analytic set that is not Borel. It is known that there are true analytic sets and this implies that complete analytic sets are not Borel. It is not provable in ZFC that every true analytic set is complete [2].

All analytic sets have the Baire property.

**Theorem 1.** The Perfect Set Theorem for Analytic Sets (Souslin). Let $X$ be a Polish space and $A \subseteq X$ an analytic set. Either $A$ is countable, or else it contains a Cantor set.

A Polish group is a topological group whose topology is Polish.

In this thesis, a central problem is that of the uniqueness of the Polish group topology: under what conditions does a given Polish group admit only one topology making it into a Polish group. We include here important technical results that will be used in later chapters in investigating the uniqueness of Polish group topologies.

**Theorem 2.** Let $X, Y$ be Polish spaces and $f : X \rightarrow Y$ a Borel map. If $A \subseteq X$ is Borel and $f$ is
injective, then \( f(A) \) is Borel and \( f \) is a Borel isomorphism of \( A \) with \( f(A) \) (i.e. \( f : A \to f(A) \) is a bijection and both \( f \) and \( f^{-1} \) are Borel).

**Theorem 3.** Let \( G \) and \( H \) be Polish groups and \( f : G \to H \) a homomorphism. If \( f \) is Baire measurable then \( f \) is continuous. Further, if \( f \) is also surjective, then it is open.

Applying Theorems 2 and 3 respectively to the identity map, one obtains the following corollaries:

**Corollary 4.** If \((X, S_1)\) and \((X, S_2)\) are two standard Borel spaces, then either the two \(\sigma\)-algebras are equal: \( S_1 = S_2 \), or incomparable: \( S_1 \not\subseteq S_2 \) and \( S_2 \not\subseteq S_1 \).

**Corollary 5.** Let \( G \) be a group and \( \tau_1 \) and \( \tau_2 \) Polish group topologies on \( G \). Then the two topologies are either equal: \( \tau_1 = \tau_2 \), or incomparable: \( \tau_1 \not\subseteq \tau_2 \) and \( \tau_2 \not\subseteq \tau_1 \).

We say that a family \( A \) of sets in a space \( X \) separates (or \( T_1 \)-separates) points of \( X \) is for every pair of distinct points \( x \) and \( y \) in \( X \) there is a set \( A \in A \) such that \( x \in A \), but \( y \notin A \). We say that \( A \) is a point-separating, or \( T_1 \)-separating family of \( X \). Similarly, we say that \( A \) \( T_0 \)-separates points in \( X \) if for any \( x \neq y \) in \( X \) we can find \( A \in A \) that contains one of the points but not the other. Call \( A \) a \( T_0 \)-separating family of \( X \).

Borel sets are generated (as a \(\sigma\)-algebra) by the open sets, but they can also be generated by other families. An important result due to Mackey [18] gives sufficient conditions for a family of sets in a Polish space \( X \) to generate all of the Borel sets in \( X \).

**Theorem 6.** Let \((X, \tau)\) be a Polish space and \( A \) a countable, point–separating family of Borel sets in \( X \). Then the Borel sets in \( X \) are generated by the family \( A \): \( B(X, \tau) \subseteq \sigma(A) \). (In fact, \( B(X, \tau) = \sigma(A) \).)

Our interest in Mackey’s result comes from the important implications it has for the uniqueness of a Polish group topology, as given in the corollary below. In fact, we will refer to the corollary as Mackey’s Theorem.

**Corollary 7. Mackey’s Theorem.** Let \( G \) be a Polish group with a countable point–separating family of sets that are Borel in any Polish group topology on \( G \). Then \( G \) has a unique Polish group topology.

Note here that both in Theorem 6 and Corollary 7, the point–separating family can be
taken to be $T_0$-separating instead: if a countable $T_0$-separating family of Borel sets exists, call it $\mathcal{A}$, then $\mathcal{A}' = \mathcal{A} \cup \{A^c \mid A \in \mathcal{A}\}$ is a countable ($T_1$-)point–separating family of Borel sets, and $\sigma(\mathcal{A}) = \sigma(\mathcal{A}')$. 
3.0 GENERAL THEORY

3.1 AUTOMATIC CONTINUITY AND UNIQUENESS OF TOPOLOGY

In this section we investigate the relationship between the problems of the uniqueness of a topology and automatic continuity in the context of Polish groups.

Consider the following properties of a Polish group $G$:

(AC) Every (abstract group) homomorphism $\phi : G \to H$, where $H$ is a Polish group, is continuous.

(U) $G$ has a unique Polish group topology.

(Aut) Every automorphism of $G$ is continuous.

Lemma 8. Let $G$ be a Polish group. The following are equivalent:

(i) $G$ has the property (U),

(ii) Every isomorphism $\phi : G \to H$, where $H$ is a Polish group, is continuous.

Proof. Suppose that (U) holds and let $\tau$ be the unique Polish group topology on $G$. Let $(H, \sigma)$ be a Polish group and $\phi : G \to H$ an isomorphism. Then $\sigma' := \{\phi^{-1}(U) \mid U \in \sigma\}$ is a Polish group topology on $G$ (a ‘copy’ of the Polish group topology on $H$). By the uniqueness property (U), $\sigma' = \tau$. It follows that the inverse image under $\phi$ of every open set in $(H, \sigma)$ is open in $(G, \tau)$, so $\phi$ is continuous.

Conversely, let $\tau$ and $\tau'$ be two Polish group topologies on $G$. Then the identity isomorphism $id : (G, \tau) \to (G, \tau')$ is a homeomorphism, by applying the hypothesis twice. Thus, $\tau = \tau'$, so $G$ has a unique Polish group topology. □
Lemma 9. The following implications hold in Polish group $G$:

$$(AC) \Rightarrow (U) \Rightarrow (Aut).$$

Proof. This is immediate after replacing (U) by the equivalent condition ‘every isomorphism $\phi : G \to H$, where $H$ is a Polish group, is continuous’ given in Lemma 8. \qed

Lemma 10. Let $G$ be a Polish group. The following are equivalent:

(i) $G$ has the property (AC),
(ii) Every monomorphism $\phi : G \to H$, where $H$ is a Polish group, is continuous.

Proof. (i) $\Rightarrow$ (ii) is immediate. Suppose (ii) holds. Let $H$ a Polish group and $\phi : G \to H$ a homomorphism. Then $\psi : G \to G \times H$ given by $\psi(g) = (g, \phi(g))$ is a monomorphism from $G$ into the Polish group $G \times H$. By (ii), $\psi$ is continuous. For every open subset $U$ of $H$, $\phi^{-1}(U) = \psi^{-1}(G \times U)$ is open. Thus $\phi$ is continuous. \qed

Proposition 11. Let $G$ be a Polish group. The following are equivalent:

(i) $G$ has the property (U),
(ii) Every epimorphism $\phi : H \to G$ with closed kernel, where $H$ is a Polish group, is continuous.

Proof. Suppose $G$ has the property (U). Let $H$ be a Polish group and let $\phi : H \to G$ be an epimorphism with closed kernel. By the first isomorphism theorem, the canonical map $\phi^* : H/\ker \phi \to G$ is an algebraic isomorphism between $H/\ker \phi$ and $G$. The group $H/\ker \phi$ is Polish since $\ker \phi$ is closed. If $\sigma$ is the Polish group topology on $H/\ker \phi$, $\phi^*(\sigma)$ is a Polish group topology on $G$. By the uniqueness of the Polish group topology on $G$, $\phi^*(\sigma)$ coincides with the original Polish group topology on $G$. It follows that $\phi^*$ is continuous, and thus so is $\phi$.

Suppose now that (ii) holds. Let $\tau$ and $\tau'$ be Polish group topologies on $G$. Then the identity map from $(G, \tau') \to (G, \tau)$ must be continuous, by (ii). Thus, $\tau \subseteq \tau'$, and so $\tau = \tau'$, by Corollary 5. \qed

Proposition 12. The following are equivalent for a Polish group $G$:

(i) $G$ has the property (AC),,
(ii) Every homomorphism $\phi : G \to H$, where $H$ is a second countable topological group, is continuous.

(iii) The given (Polish) group topology is the finest second countable group topology on $G$.

Proof. Clearly (ii) $\Rightarrow$ (i). To show (i) $\Rightarrow$ (ii), recall that every second countable group $H$ embeds as a topological group into the Polish group $\text{Homeo}(\mathbb{I}^\mathbb{N})$ of homeomorphisms of the Hilbert cube [22], say, via $e : H \to \text{Homeo}(\mathbb{I}^\mathbb{N})$. Let $\phi : G \to H$, where $H$ is second countable, is a homomorphism. Then $e \circ \phi : G \to \text{Homeo}(\mathbb{I}^\mathbb{N})$ is a homomorphism from $G$ into the Polish group $\text{Homeo}(\mathbb{I}^\mathbb{N})$. By (AC), $e \circ \phi$ is continuous, and thus $\phi$ is continuous.

(ii) $\Rightarrow$ (iii): Let $\tau$ denote the given Polish group topology and let $\sigma$ be a second countable group topology on $G$. The identity map from $(G, \tau)$ into $(G, \sigma)$ is a homomorphism into a second countable group, so by (ii), it must be continuous. It follows that $\sigma \subset \tau$.

(iii) $\Rightarrow$ (ii): Let $\tau$ be the given Polish group topology on $G$. Let $H$ be an arbitrary second countable group and let $\phi : G \to H$ be a homomorphism. We may assume without loss of generality, replacing if necessary the function $\phi : G \to H$ by $\phi' : G \to G \times H$ given by $\phi'(g) = (g, \phi(g))$, that $\phi$ is injective. (Here we note that $G \times H$ is second countable since $G$ and $H$ are, and that $\phi'$ is continuous if and only if $\phi$ is continuous.) Let $\sigma$ be the topology on $G$ defined by $\sigma = \{ \phi^{-1}(V) \mid V \text{ is open in } H \}$. Then $(G, \sigma)$ is second countable, since it is homeomorphic to the subgroup $\phi(G)$ of $H$. By the assumption (iii), $\sigma \subset \tau$. Thus, the inverse image under $\phi$ of any open set in $H$ is open in $(G, \tau)$, so $\phi$ is continuous. 

**Proposition 13.** The following are equivalent for a Polish group $G$:

(i) $G$ has the property (U),

(ii) The given Polish group topology is the finest Polish group topology on $G$.

Proof. This is immediate from the fact that if two Polish group topologies are comparable, then they are equal (Lemma 5).

Recall, a topological group $H$ is said to be $\aleph_0$-bounded if for every open neighborhood $U$ of the identity, $H$ can be covered by countably many translates of $U$, i.e. if there exists a countable subset $C$ of $H$ such that $C \cdot U = H$. 

11
Proposition 14. Let $G$ be a Polish group. The following are equivalent:

(i) Every homomorphism $\phi : G \to H$, where $H$ is a second countable topological group, is continuous.

(ii) Every homomorphism $\phi : G \to H$, where $H$ is a separable topological group, is continuous.

(iii) Every homomorphism $\phi : G \to H$, where $H$ is an $\aleph_0$-bounded topological group, is continuous.

Proof. Since every second countable space is separable, and every separable topological group is $\aleph_0$-bounded, it is immediate that $(iii) \Rightarrow (ii) \Rightarrow (i)$. We show that $(i) \Rightarrow (iii)$.

Let $H$ be an $\aleph_0$-bounded topological group and $\phi : G \to H$ a homomorphism. Then $H$ embeds into a product of second countable topological groups [7]. Let $e : H \to \prod_{\lambda \in \Lambda} H_{\lambda}$, where $H_{\lambda}$ are second countable topological groups, be the embedding of $H$. For each $\lambda$, the homomorphisms $\pi_\lambda \circ e \circ \phi : H \to H_\lambda$ are continuous by hypothesis (i) (here, $\pi_\lambda$ denotes the $\lambda$-th projection of $\prod_{\mu \in \Lambda} H_\mu$ to $H_\lambda$). Thus, $\phi$ is continuous. \qed

3.2 SEPARATING GROUP

A useful concept in the theory of automatic continuity in Banach algebras [4] is that of a separating subspace. We translate this concept into the framework of metrizable groups in order to investigate the automatic continuity between Polish groups. We give a definition and prove several properties of a separating group, but at the moment we have not taken these ideas any further.

Let $G$ and $H$ be topological groups and let $\phi : G \to H$ be an (abstract group) homomorphism. We define the separating set $S(\phi)$ of $\phi$ to be

$$S(\phi) = \bigcap \{ \phi(U) : U \text{ is an open neighborhood of } 1_G \}.$$ 

For a group $G$, we will write $\mathcal{N}_G$ for the family of all open neighborhoods of the identity $1_G$ in $G$. 

12
Lemma 15. If \( G \) and \( H \) are topological groups and \( \phi : G \to H \) is a homomorphism, then \( y \in S(\phi) \) if and only if there is a net \((x_\nu)\) in \( G \) such that \( x_\nu \to 1_G \) and \( \phi(x_\nu) \to y \).

Furthermore, if \( G \) and \( H \) are metrizable, then \( y \in S(\phi) \) if and only if there is a sequence \((x_n)\) in \( G \) such that \( x_n \to 1_G \) and \( \phi(x_n) \to y \).

**Proof.** Let \( y \in S(\phi) \). Then \( y \in \overline{\phi(U)} \), for every open neighborhood \( U \) of \( 1_G \). Thus for all \( V \in \mathcal{N}_H \) and all \( U \in \mathcal{N}_G \), \( yV \cap \phi(U) \neq \emptyset \). Pick \( x_{U,V} \in U \) such that \( \phi(x_{U,V}) \in yV \). Then \((x_{U,V})\) is a net in \( G \). Here, \( \{(U,V) \mid U \in \mathcal{N}_G, V \in \mathcal{N}_H \} \) is a directed set with the partial order \( \leq \) given by \((U,V) \leq (U',V') \) if and only if \( U \supseteq U', V \supseteq V' \). Furthermore, \( x_{U,V} \to 1_G \), since for any \( W \in \mathcal{N}_G \), we have \((U,V) \geq (W,H) \Rightarrow x_{U,V} \in U \subseteq W \). Also, \( \phi(x_{U,V}) \to y \), since for any \( W \in \mathcal{N}_H \), we have \((U,V) \geq (G,W) \Rightarrow \phi(x_{U,V}) \in yV \subseteq yW \).

Conversely, let \((x_\nu)\) be a net in \( G \) with \( x_\nu \to 1_G \) and \( \phi(x_\nu) \to y \). Let \( U, V \in \mathcal{N}_G \) and \( \nu \in \mathcal{N}_H \). We need to show that \( yV \cap \phi(U) \neq \emptyset \). Since \( \phi(x_\nu) \to y \), there exists \( \lambda \) such that for all \( \nu \geq \lambda \), \( \phi(x_\nu) \in yV \). Also, since \( x_\nu \to 1_G \), there is \( \mu \) such that whenever \( \nu \geq \mu \), \( x_\nu \in U \), and consequently \( \phi(x_\nu) \in \phi(U) \). Thus, whenever \( \nu \geq \lambda \land \mu \), \( \phi(x_\nu) \in yV \cap \phi(U) \).

For the case of metrizable groups, replace in the above argument \( \mathcal{N}_G \) and \( \mathcal{N}_H \) by nested countable open neighborhood bases \((U_n)\) and \((V_m)\) of \( 1_G \) and \( 1_H \) respectively. \( \square \)

So,

\[
S(\phi) = \{ y \in H : \text{there is a net } (x_\nu) \text{ in } G \text{ with } x_\nu \to 1_G \text{ and } \phi(x_\nu) \to y \},
\]

and when the groups \( G \) and \( H \) are metrizable,

\[
S(\phi) = \{ y \in H : \text{there is a sequence } (x_n) \text{ in } G \text{ with } x_n \to 1_G \text{ and } \phi(x_n) \to y \}.
\]

Lemma 16. Let \( G \) and \( H \) be topological groups and \( \phi : G \to H \) a group homomorphism. Then the separating set \( S(\phi) \) is a closed subgroup of \( H \).

**Proof.** \( S(\phi) \) is clearly closed, since it is the intersection of a family of closed sets. Also, it is clear that \( 1_H \in S(\phi) \). Suppose \( x,y \in S(\phi) \). Then there exist nets \((x_\nu),(y_\nu)\) in \( G \) such that \( x_\nu \to 1_G, y_\nu \to 1_G, \phi(x_\nu) \to x, \phi(y_\nu) \to y \). Since \( \phi \) is a homomorphism and the group operations in \( G \) and \( H \) are continuous, we have: \( x_\nu y_\nu \to 1_G, \phi(x_\nu y_\nu) = \phi(x_\nu) \phi(y_\nu) \to xy \) and \( x_\nu^{-1} \to 1_G, \phi(x_\nu^{-1}) = \phi(x_\nu)^{-1} \to x^{-1} \), so \( xy, x^{-1} \in S(\phi) \). \( \square \)
Since $S(\phi)$ is always a subgroup of $H$, we also call it the \textit{separating subgroup} of $\phi$.

**Lemma 17.** Let $G$ and $H$ be topological groups and $\phi : G \to H$ an epimorphism. Then the separating group $S(\phi)$ is normal in $H$.

**Proof.** Let $y \in S(\phi)$ and $h \in H$. Let $(x_\nu)$ be a net in $G$ such that $x_\nu \to 1_G$ and $\phi(x_\nu) \to y$. Since $\phi$ is surjective, there exists $g \in G$ such that $\phi(g) = h$. Now the net $(gx_\nu g^{-1})$ in $G$ converges to $1_G$, while $\phi(gx_\nu g^{-1}) = \phi(g)\phi(x_\nu)\phi(g)^{-1} = h\phi(x_\nu)h^{-1} \to hyh^{-1}$. So, $y = hyh^{-1} \in S(\phi)$ and $S(\phi)$ is normal in $H$.

**Lemma 18.** Let $G$ and $H$ be metrizable groups and $\phi : G \to H$ a homomorphism. Then $\phi$ is continuous if and only if $S(\phi) = 1_H$.

**Proof.** Suppose $\phi$ is continuous. Let $y \in S(\phi)$ and let $(x_n)$ be a sequence in $G$ such that $x_n \to 1_G$ and $\phi(x_n) \to y$. By continuity of $\phi$, $\phi(x_n) \to \phi(1_G) = 1_H$, so, by the uniqueness of limits, $y = 1_H$.

Conversely, suppose $S(\phi) = 1_H$. It is sufficient to show $\phi$ is continuous at $1_G$. Let $V$ be an open neighborhood of $1_H$, and let $(U_n)$ be a nested countable open neighborhood base at $1_G$. Suppose, for a contradiction, that for all $n$, $\phi(U_n) \not\subseteq V$. Then, we can find a sequence $(x_n)$ in $G$ such that $x_n \in U_n$, but $\phi(x_n) \not\in V$. Since $U_n$'s are nested, $x_n \to 1_G$, so $\phi(x_n) \to 1_H$. On the other hand, $\phi(x_n) \in H \setminus V$, and $H \setminus V$ is closed, so $1_H \in H \setminus V$. This is a contradiction, since $1_H \in V$.

### 3.3 IDENTITY AND VERBAL SETS

As we shall see, the notion of ‘definability’ of sets plays an important role in many proofs of uniqueness of topology and automatic continuity. These proofs all depend on understanding what sets are ‘definable’, or ‘computable’, both algebraically and topologically. In this context, a set is considered to be ‘definable topologically’ if it is Borel, analytic, or has the Baire property. By ‘algebraically definable’, we have in mind sets defined using the group operation, such as conjugacy classes, commutators, centralizers, powers, etc.
Let $G$ be an arbitrary group and let $F$ be the free group on a countably infinite set \( \{x_1, x_2, \ldots \} \). If \( w = x_1^{l_1} \cdots x_r^{l_r} \in F \) and \( g_1, \ldots, g_r \) are elements of $G$, the value of the word $w$ at \( (g_1, \ldots, g_r) \) is defined to be

\[
    w(g_1, \ldots, g_r) = g_1^{l_1} \cdots g_r^{l_r}.
\]

By abuse of notation, we denote the evaluation map from $G^r$ to $G$ given by

\[
    (g_1, \ldots, g_r) \mapsto w(g_1, \ldots, g_r),
\]

also by $w$. Note that if $G$ is a topological group, the map $w$ is continuous.

Algebraically defined sets come from free words. We encounter the following types of sets defined from free words: identity sets, verbal sets, and verbal subgroups.

Subsets of $G$ of the form

\[
    \{ g \in G \mid w(g; a_1, \ldots, a_m) = 1 \},
\]

where $w$ is a free word and $a_1, \ldots, a_m$ are elements of $G$, are called identity sets. The identity sets can be thought of as the inverse images of \( \{1\} \) under the maps $w(\cdot; a_1, \ldots, a_m)$:

\[
    w(\cdot; a_1, \ldots, a_m)^{-1}\{1\}.
\]

In contrast with the identity sets, verbal sets are defined as the forward images under the maps $w$: they are the sets of the form

\[
    \{ w(g_1, \ldots, g_n; a_1, \ldots, a_m) \mid g_1, \ldots, g_n \in G \},
\]

where $w$ is a free word and $a_1, \ldots, a_m$ are elements of $G$. If no constants are used in the definition of a verbal set:

\[
    \{ w(g_1, \ldots, g_n) \mid g_1, \ldots, g_n \in G \},
\]

then we call it a full verbal set.

For example, centralizers of an element $a \in G$,

\[
    \{ g \in G \mid gag^{-1}a^{-1} = 1 \},
\]
are identity sets, conjugacy classes:

\[ \{ gag^{-1} \mid g \in G \} \]

are (non–full) verbal sets, while the \( m \)-th powers:

\[ G^{(m)} = \{ g^m \mid g \in G \} \]

and commutators:

\[ \{ ghg^{-1}h^{-1} \mid g, h \in G \} \]

are examples of full verbal sets.

If \( W \) is a set of free words, then the verbal subgroup of \( G \) associated with \( W \) is the group

\[ W(G) = \langle \{ w(g_1, \ldots, g_n) \mid g_1, \ldots, g_n \in G, w \in W \} \rangle \]

generated by all \( w \)-values in \( G \), with \( w \in W \). If \( W = \{ w \} \), we write \( w(H) \) for \( W(H) \).

## 3.4 TOPOLOGICAL STATUS OF IDENTITY AND VERBAL SETS

A classical example that illustrates the importance of definability of sets is a theorem of Mackey [18] (Theorem 7). According to this result, in order to show that a Polish group \( G \) admits a unique Polish group topology, it is sufficient to find a countable point-separating family of sets that are Borel in any Polish group topology on \( G \). The difficulty in applying this result is deciding which sets are Borel in any Polish group topology. Good candidates for the point-separating collection would be algebraically definable sets since their definition does not depend on the choice of topology on \( G \). It is therefore important to know which algebraically definable sets are necessarily Borel (in any Polish group topology on \( G \)). We now investigate the topological status of the identity and verbal sets, and verbal subgroups.
In any topological group, identity sets are necessarily closed (and thus Borel), since they are the inverse images of the closed set $\{1\}$ under continuous maps:

$$w(\cdot; a_1, \ldots, a_m)^{-1}\{1\}.$$ 

This makes the identity sets the ideal candidates to be used in applying Mackey’s result. Indeed, the identity sets have been used to show the uniqueness of Polish group topology for a number of Polish groups. For further discussion, see Sections 3.5 and 4.1 below.

Verbal sets are continuous forward images of Polish spaces, and are therefore necessarily analytic in any Polish group. An important question that this thesis resolves is whether the verbal sets are in fact always Borel. From the theory of Polish group actions, we know that conjugacy classes are always Borel. We also show that in Abelian Polish groups and in the infinite symmetric group, the full verbal sets are Borel. One might anticipate that all verbal sets would be Borel in any Polish group. However, the example of the set of squares of the autohomeomorphism group of the circle, which we show is not Borel (Theorem 53), dispels this hope. A detailed discussion on the complexity of verbal sets is deferred to Chapter 5.

Verbal subgroups are also necessarily analytic, as we show in the lemma below:

**Lemma 19.** If $G$ is a Polish group and $W$ is a set of free words, the verbal subgroup $W(G)$ is the union of a countable collection of verbal sets, and hence analytic.

**Proof.** We may assume without loss of generality that $W$ is closed under taking inverses (otherwise, replace $W$ with $W \cup \{w^{-1} \mid w \in W\}$ — the verbal subgroup $W(G)$ remains unchanged). Then every element in $W(G)$ is a product of finitely many elements of $W$. Let $S_N$ be the set of those elements of $W(G)$ that can be written as the product of $N$ words from $W$. Then $S_N$ is the union of a countable collection of verbal sets:

$$S_N = \bigcup_{w_1, \ldots, w_N \in W} \{w_1(g^1) \cdots w_n(g^n) \mid g^j \in G^{m_j}, m_j \text{ is the number of letters in } w_j\}.$$ 

The verbal subgroup $W(G)$ is the countable union

$$W(G) = \bigcup_{N=0}^{\infty} S_N,$$

so it is itself the union of a countable collection of verbal sets. □
As we have seen, the identity sets are closed, and thus Borel, in any (Polish) group. Thus, we have the following corollary to Mackey’s theorem:

**Corollary 20.** If $G$ is a Polish group with a countable, $T_0$-separating family of identity sets (or sets from the $\sigma$-algebra generated by the identity sets), then $G$ admits a unique Polish group topology.

**Corollary 21.** Let $G$ be a Polish group with a countable subset $H$, such that for any pair of distinct points $x, y$ in $G$, there is a free word $w(X_0, X_1, \ldots, X_n)$ and $h_1, h_2, \ldots, h_n \in H$ such that

$$w(x, h_1, \ldots, h_n) = 1, \quad \text{but} \quad w(y, h_1, \ldots, h_n) \neq 1.$$ 

Then $G$ admits only one Polish group topology.

**Proof.** Let

$$C = \{w(\cdot, h_1, \ldots, h_n)^{-1}(1) : w \text{ is a free word, } h_1, \ldots, h_n \in H\}.$$ 

Then $C$ is a countable collection of identity sets. Also, if $x$ and $y$ are distinct elements of $G$, there exists a free word $w$ and $h_1, \ldots, h_n \in H$ such that

$$x \in w^{-1}(\cdot, h_1, \ldots, h_n), \quad \text{but} \quad y \notin w^{-1}(\cdot, h_1, \ldots, h_n).$$

Thus $C$ separates points and Corollary 20 applies. \hfill $\square$

The identity sets have been highly effective in proving uniqueness of Polish group topology results. In [14], Kallman shows that the autohomeomorphism group $G = Homeo(X)$, for a wide class of spaces $X$, admits a unique Polish group topology. The list of spaces $X$ for which the result holds includes: separable metric manifolds, connected countable locally finite simplicial complexes, the Hilbert cube, the Cantor set, the natural numbers. In proving this result, Kallman essentially applies Mackey’s theorem to the countable family of sets

$$C(U_r, U_j) = \bigcap_{U', V'} \{g \in G \mid g g_{U'} g^{-1} \text{ commutes with } g_{V'}\},$$

for any pair of distinct points $x, y$ in $G$. 

---

**3.5 UNIQUENESS AND IDENTITY SETS**

---
where \((U_n)\) is a countable basis for the topology of \(X\), and \(U'\) ranges over the non-empty open subsets of \(U_i\) with more than one point, and \(V'\) ranges over the nonempty open subsets of \(U_j\) with more than one point. (Here, \(g_U\) denotes a fixed element of \(G = \text{Homeo}(X)\) that is the identity on \(X \setminus U\), but not the identity on \(U\).) Even though the sets \(C(U_i, U_j)\) are not identity sets, a small modification of Kallman’s argument shows that, in fact, we can replace the family of sets \(C(U_i, U_j)\) by a countable family of identity sets that separate points. Kallman shows that the sets \(C(U_i, U_j)\) separate points. Observe that then the sets

\[
C(U_i, U_j; U', V') := \{g \in G \mid gg^{-1} \text{ commutes with } g\}
\]

must also separate points (i.e. the intersection \(\bigcap_{U', V'}\) above is redundant). Also, since \(U'\) and \(V'\) can be assumed to be basic open without loss of generality, the collection of sets \(C(U_i, U_j; U', V')\) is also countable. Finally, observe that the sets \(C(U_i, U_j; U', V')\) are identity sets:

\[
\{g \in G \mid gg^{-1}g^{-1}g^{-1}g^{-1}g^{-1}g^{-1}g^{-1}g^{-1}g^{-1}g^{-1} = 1\}.
\]

For an example of an application of identity sets, please see Section 4.1, where we give a direct proof of the uniqueness of the Polish group topology in the infinite symmetric group, \(S_\infty\).

### 3.6 DIFFICULTIES EXTENDING TO ANALYTIC SETS

In the preceding section we saw that the identity sets can be immensely useful in proving uniqueness of topology results. However, the identity sets may not always be sufficient. For example, we will see in Section 4.2, that in the special orthogonal group, \(SO(3)\), no countable collection of identity sets separates points. Therefore, in \(SO(3)\), Mackey’s theorem cannot be applied with identity sets alone.

Thus, we are forced to move beyond identity sets. Verbal sets are natural candidates. It is unfortunate that verbal sets are always analytic, and not necessarily Borel, while Mackey’s theorem requires Borel sets. A natural question then is, whether Mackey’s result can be extended to apply to analytic sets, or even the sets with the Baire property.
Recall that Mackey’s theorem follows from Theorem 6: If \( X \) is a Polish space and \( A \) a countable, point–separating family of Borel sets in \( X \), then \( B(X) \subseteq \sigma(A) \). If Theorem 6 were true with the word ‘Borel’ replaced by ‘analytic’ (or, by ‘sets with the Baire property’), we would be able to prove the analytic (respectively, the Baire property) version of Mackey’s theorem.

Lemma 22 below shows that Theorem 6 does not hold with ‘Borel’ replaced by ‘the sets having the Baire property’. We still do not know if the theorem would hold with ‘Borel’ replaced by ‘analytic’. Our example below suggests otherwise, though it does not provide a definite answer.

**Lemma 22.** Let \( C = 2^{\mathbb{N}} \) be the Cantor space. There is a countable point-separating family \( A \) of sets in \( C \), each of which is the union of an analytic and a co-analytic set, such that \( B(C) \not\subseteq \sigma(A) \).

*Proof.* Let \( U = \{ x \in C \mid x(0) = 0 \} \). Note that \( U = \{0\} \times 2^{\mathbb{N}} \) is homeomorphic to \( C \). Fix an uncountable analytic, but not Borel (in \( C \)) subset \( A \) of \( U \).

By the Perfect Set Theorem for Analytic Sets (Theorem 1), \( A \) contains a copy of the Cantor space. Thus, there exists a homeomorphic embedding \( g_1 \) of \( U \) into \( A \). (Note that since \( U \) is compact, \( g_1(U) \) is closed in \( C \).) On the other hand, \( A \subseteq U \), so the inclusion map \( h_1 : A \to U \) is a homeomorphic embedding of \( A \) into \( U \). From the injections \( g_1 \) and \( h_1 \), we construct a bijection \( f_1 : U \to A \) using a Schröder-Bernstein argument as follows. Define subsets \( K_n \) of \( U \), for \( n = 0, 1, 2, \ldots \) recursively by: \( K_0 = U \setminus h_1(A) \), \( K_n = h_1(g_1(K_{n-1})) \), for \( n = 1, 2, \ldots \). Let \( C_1 = \bigcup_n K_n \), \( B_1 = U \setminus C_1 \), \( D_1 = h_1^{-1}(B_1) = B_1 \), \( E_1 = g_1(C_1) \). Using the fact that the class of analytic sets is closed under continuous images, a simple calculation shows that each \( K_n \) is co-analytic. Then \( C_1 \) is co-analytic, as their countable union, \( B_1 \) is analytic, \( D_1 \) is analytic and \( E_1 = g_1(U) \setminus g_1(B_1) \) is co-analytic. The bijection \( f_1 : U \to A \) is now defined as

\[
  f_1(x) = \begin{cases} 
    h_1^{-1}(x) = x, & \text{if } x \in B_1, \\
    g_1(x), & \text{if } x \in C_1.
  \end{cases}
\]

Similarly, let \( g_2 : U^C \to A^C \) be the inclusion map, and let \( h_2 : C \to U^C \) be the right shift map given by \( h_2(x)(0) = 1 \) and \( h_2(x)(n) = x(n - 1) \), for \( n = 1, 2, \ldots \), where \( x \in C \).
Then $g_2$ and $h_2|A^C$ are homeomorphic embeddings, and once again we use a Schröeder-Bernstein construction; this time, to define a bijection $f_2 : U^C \to A^C$. Define subsets $L_n$ of $U^C$ recursively as follows: $L_0 = U^C \setminus h_2(A^C)$, $L_n = h_2(g_2(L_{n-1}))$, for $n = 1, 2, \ldots$

Let $B_2 = \bigcup L_n$, $C_2 = U^C \setminus B_2$, $D_2 = g_2(B_2) = B_2$, $E_2 = h_2^{-1}(C_2)$. We see that each $L_n$ is analytic, and so $B_2$ and $D_2$ are analytic too, and $C_2$ and $E_2$ are co-analytic. The bijection $f_2 : U^C \to A^C$ is given by

$$f_2(x) = \begin{cases} g_2(x) = x, & \text{if } x \in B_2, \\ h_2^{-1}(x), & \text{if } x \in C_2. \end{cases}$$

Let $f = f_1 \cup f_2$, $B = B_1 \cup B_2$, $C = C_1 \cup C_2$, $D = D_1 \cup D_2$ and $E = E_1 \cup E_2$. Then

$$f(x) = \begin{cases} x, & \text{if } x \in B, \\ g_1(x), & \text{if } x \in C_1, \\ h_2^{-1}(x), & \text{if } x \in C_2. \end{cases}$$

Let $U_n = \{x \in C \mid x(n) = 0\}$ and $U'_n = \{x \in C \mid x(n) = 1\}$ for $n = 0, 1, 2, \ldots$ Further, define $A_n = f(U_n)$, $A'_n = f(U'_n)$, and let $\mathcal{A} = \{A_n \mid n \in \mathbb{N}\} \cup \{A'_n \mid n \in \mathbb{N}\}$. We claim that the family $\mathcal{A}$ has the desired properties.

To show that $\mathcal{A}$ is point–separating, let $x$ and $y$ be distinct points in $C$. Then there exists $n \in \mathbb{N}$ such that $f^{-1}(x)(n) \neq f^{-1}(y)(n)$. If $f^{-1}(x)(n) = 0$ and $f^{-1}(y)(n) = 1$, then $f^{-1}(x) \in U_n$ and $f^{-1}(y) \notin U_n$, so $x \in A_n$ and $y \notin A_n$. Similarly, if $f^{-1}(x)(n) = 1$ and $f^{-1}(y)(n) = 0$, we find that $A'_n$ contains $x$, but does not contain $y$.

Each $A_n$ (and similarly, each $A'_n$) is the union of an analytic set and a co-analytic set. To see this, write:

$$A_n = f(U_n) = f(U_n \cap B) \cup f(U_n \cap C_1) \cup f(U_n \cap C_2) = (U_n \cap B) \cup g_1(U_n \cap C_1) \cup h_2^{-1}(U_n \cap C_2).$$

Then, $U_n \cap B$ is analytic. Further, $g_1(U_n \cap C_1) = g_1(U) \setminus g_1(U \setminus (U_n \cap C_1))$ co-analytic, since it equals the set difference between a closed and an analytic set. Also, $h_2^{-1}(U_n \cap C_2) = C \setminus h_2^{-1}(U^C \setminus (U_n \cap C_2))$ is co-analytic.
Lastly, we need to show that $B(C) \nsubseteq \sigma(A)$. Since $(C, \sigma(U)) = (C, B(C))$ is a standard Borel space, and $f : (C, \sigma(U)) \to (C, \sigma(A))$ is a Borel isomorphism, it follows that $(C, \sigma(A))$ is also a standard Borel space. The two standard Borel spaces are different, since $A \in \sigma(A)$, but $A \notin B(C)$. By Corollary 4, the two $\sigma$-algebras are incomparable, so $B(C) \nsubseteq \sigma(A)$. 

### 3.7 UNIQUENESS AND VERBAL SETS

While it is unclear if Mackey’s theorem can be extended directly to apply to analytic sets, we have obtained other Mackey-type results that work with analytic sets. These theorems work even with the sets that only have the Baire property.

These results now allow us to use verbal sets and verbal subgroups. We give two applications: in Sections 4.2 and 4.3 we show that certain compact Lie groups (such as $SO(3)$) and all finitely generated profinite groups have a unique Polish group topology.

Recall that a collection $\mathcal{N}$ of subsets of a topological space $X$ is called a network for $X$ if whenever $x \in V$, with $V$ open in $X$, we have $x \in N \subset V$ for some $N$ in $\mathcal{N}$.

**Theorem 23.** If a Polish group $G$ has a countable network of sets that have the Baire property in any Polish group topology on $G$, then $G$ has a unique Polish group topology.

In particular, if a Polish group $G$ has a countable network of sets from the $\sigma$-algebra generated by identity and verbal sets, then $G$ has a unique Polish group topology.

**Proof.** Let $\tau$ be a Polish group topology and $\mathcal{N}$ a countable network as in the statement of the theorem. Let $\sigma$ be a Polish group on $G$, potentially different form $\tau$. Consider the identity map

$$\text{id : (G, \sigma) \to (G, \tau).}$$

We will show that $\text{id}$ is continuous, so that $\tau \subseteq \sigma$. Then by Corollary 5, $\tau = \sigma$. By Theorem 3, it is sufficient to show that $\text{id}$ is Baire measurable. Let $V$ be an open set in $(G, \tau)$. Then
$V$ can be written as the union of a countable collection of sets from the network $\mathcal{N}$:

$$V = \bigcup_{n \in \omega} A_n,$$

with $A_n \in \mathcal{N}$ for $n = 1, 2, \ldots$ Since each $A_n$ has the Baire property in $(G, \sigma)$, it follows that their (countable) union also has the Baire property. So, $\text{id}(V) = V$ has the Baire property. So $\text{id}$ is Baire measurable.

**Theorem 24.** Let $G$ be a Polish group with a neighborhood base at the identity of sets that have the Baire property in every Polish group topology on $G$. Then $G$ has a unique Polish group topology.

In particular, if $G$ is a Polish group with a neighborhood base at the identity of sets from the $\sigma$-algebra generated by identity and verbal sets, then $G$ has a unique Polish group topology.

**Proof.** Let $B$ be a neighborhood base at the identity as in the statement of the theorem. We may assume without loss of generality that $B$ is countable, since $G$ is first countable. Let $D$ be a countable dense subset of $G$. Consider the collection

$$\mathcal{N} = \{dB \mid d \in D, B \in B\}.$$

Clearly, $\mathcal{N}$ is countable and the sets in $\mathcal{N}$ have the Baire property in any Polish group topology on $G$. We will show that $\mathcal{N}$ is a network in $G$. Let $x \in U$, with $U$ open in $G$. Then $x^{-1}U$ is an open neighborhood of $1$, so there exists an open neighborhood $V$ of $1$ such that $V^2 \subseteq x^{-1}U$. Let $B \in B$ be such that $1 \in B \subseteq V$, and let $W$ be an open neighborhood of $1$ such that $W^{-1}W \subseteq B$. Since $xW$ is open, it meets the dense set $D$. Let $d \in xW \cap D$. We show that $x \in dB \subseteq U$. Since $d \in xW \subseteq xW^{-1}W$,

$$x^{-1}d \in W^{-1}W,$$

so

$$d^{-1}x \in W^{-1}W \subseteq B,$$

so

$$x \in dB.$$
Also,
\[ dB \subseteq (xB) \subseteq xV^2 \subseteq x(x^{-1}U) = U. \]

This shows that \( \mathcal{N} \) is a countable network for \( G \) of sets that have the Baire property in any Polish group topology on \( G \). By theorem 23, \( G \) has a unique Polish group topology. \( \square \)

3.8 LOCALLY COMPACT SEPARABLE METRIZABLE GROUP TOPOLOGY

In this section, we prove another Mackey-type result. It gives the conditions on the uniqueness of locally compact separable metrizable group topology.

It is known that a topological group is locally compact separable metrizable if and only if it is \( \sigma \)-compact Polish.

**Theorem 25.** If \( G \) is a topological group with a countable point–separating family of sets from the \( \sigma \)-algebra generated by identity and verbal sets, then \( G \) has at most one locally compact separable metric group topology.

**Proof.** Suppose \( G \) has a locally compact separable metric group topology \( \tau \). Then \( (G, \tau) \) is a \( \sigma \)-compact Polish group. All identity and verbal sets in \( G \) are Borel in \( (G, \tau) \). We already know that identity sets are always Borel (closed). Let \( V = \{ w(g_1, \ldots, g_n; a_1, \ldots, a_m) \mid g_1, \ldots, g_n \in G \} \), where \( a_1, \ldots, a_m \in G \) and \( w \) is a word in \( G \), be a verbal set in \( G \). Then \( V = w(G^n) \) is \( \sigma \)-compact, and thus \( F_{\sigma} \) in \( (G, \tau) \). Let \( C \) be a countable point–separating family of sets from the \( \sigma \)-algebra of identity and verbal sets. Then by Theorem 6, \( \mathcal{B}(G, \tau) = \sigma(C) \). Suppose \( \tau' \) is another locally compact separable metric group topology on \( G \). Then, by repeating the same argument, \( \mathcal{B}(G, \tau') = \sigma(C) \). It follows that \( \mathcal{B}(G, \tau) = \mathcal{B}(G, \tau') \). Thus the identity group isomorphism \( \text{id} \) between the Polish groups \( (G, \tau) \) and \( (G, \tau') \) is a Borel map. By Theorem 3, \( \text{id} \) is a homeomorphism. So \( \tau = \tau' \). \( \square \)

Note that in applying this result it is sufficient to find a \( T_0 \)-separating family \( C \), since then the sets in \( C \) together with their complements form a \( T_1 \)-separating family.

Theorem 25 applies to show uniqueness of the locally compact separable metrizable topology in compact connected simple Lie groups. This result was obtained indepen-
dently by Kallman [11]. (Note that Kallman’s result also refers to locally compact topolo-
gies, despite the fact that the MathSciNet review of the article omits this requirement.) We
will see in Section 4.2 that, in fact, compact connected simple Lie groups have a unique
Polish group topology.
4.0 APPLICATIONS

4.1 INFINITE SYMMETRIC GROUP

The infinite symmetric group $S_\infty$ is the group of permutations of the set of the natural numbers $\mathbb{N}$. With the relative topology as a subset of $\mathbb{N}^\mathbb{N}$, it is a Polish group. Note that we can also think of $S_\infty$ as being the group of all autohomeomorphisms of the natural numbers.

It is known that the natural topology on $S_\infty$ described above is the only topology on it in which it is a Polish group [12, 14]. The uniqueness of the Polish group topology on $S_\infty$ also follows from the stronger property that homomorphisms from $S_\infty$ into arbitrary separable groups are automatically continuous [17].

In this section we give an independent direct proof of the uniqueness of the Polish group topology on $S_\infty$. Our purpose is to provide a proof which uses Mackey’s theorem with identity sets (Corollary 20).

**Notation.** For $a_1, \ldots, a_n$ ($n \geq 1$), distinct points in $\mathbb{N}$,

$$(a_1 \ a_2 \cdots \ a_n)$$

is the permutation that maps $a_i$ to $a_{i+1}$ for $i = 1, 2, \ldots, n - 1$, and $a_n$ to $a_1$, and is otherwise the identity. Such a permutation is called an $n$-cycle. Similarly, for a sequence $(a_i)_{i \in \mathbb{Z}}$ of distinct elements of $\mathbb{N}$,

$$(\cdots \ a_{-1} \ a_0 \ a_1 \ a_2 \cdots)$$

26
denotes the permutation that maps each \(a_i\) to \(a_{i+1}\) and is otherwise the identity. We call such a permutation an \textit{infinite cycle}. Any permutation in \(S_\infty\) can be represented by an unordered formal composition of disjoint cycles in a unique way. We say that a permutation \(\pi\) contains cycles \(\sigma_1, \ldots, \sigma_k\), and write \(\pi \supset \sigma_1 \cdots \sigma_k\), if \(\sigma_1, \ldots, \sigma_k\) are (some of the) cycles in the unique disjoint cycle representation of \(\pi\). Finally, for \(\text{finitely many distinct points} a_1, \ldots, a_k\), it will be convenient to write \(\pi \supset (a_1 a_2 \cdots a_k \cdots)\), to mean \(\pi(a_i) = a_{i+1}\), for each \(i = 1, \ldots, k-1\). Note that by this notation we do not imply that the cycle is of infinite length.

For \(a \neq b\) in \(\mathbb{N}\), let \(C(a\ b)\) be the centralizer of \((a\ b)\) in \(S_\infty\):

\[ C(a\ b) = \{ \pi \in S_\infty \mid \pi(a\ b) = (a\ b)\pi \} \]

Note that \(C(a\ b)\) is an identity set, since:

\[ C(a\ b) = \{ \pi \in S_\infty \mid \pi(a\ b)\pi^{-1}(a\ b)^{-1} = 1 \} \]

Also, for any \(\tau \in S_\infty\), \(\tau C(a\ b)\) is an identity set, because:

\[ \tau C(a\ b) = \{ \pi \in S_\infty \mid \tau^{-1}\pi(a\ b)\tau^{-1}\pi(a\ b)^{-1} = 1 \} \]

\textbf{Lemma 26.} If \(a \neq b\), a permutation \(\pi\) is in \(C(a\ b)\) if and only if either \(\pi(a) = a\) and \(\pi(b) = b\) or \(\pi(a) = b\) and \(\pi(b) = a\), i.e. \(\pi\) either fixes or switches \(a\) and \(b\).

\textit{Proof.} Clearly \(\pi(a)\) is either \(a\) or \(b\), for otherwise, \(\pi(a) = (a\ b)\pi(a) = \pi(a\ b)(a) = \pi(b)\).

If \(\pi(a) = a\), then \(\pi(b) = \pi(a\ b)(a) = (a\ b)\pi(a) = (a\ b)(a) = b\), and if \(\pi(a) = b\), a similar computation shows that \(\pi(b) = a\). The converse is immediate. \qed

\textbf{Lemma 27.} The family

\[ C = \{ \tau C(a\ b) : \tau \text{ is a 2-cycle or a 3-cycle}, a, b \in \mathbb{N} \} \]

\(T_0\)-separates points in \(S_\infty\).
Proof. Take any $\pi \neq \sigma$ in $S_\infty$. At some point $\pi$ and $\sigma$ disagree: without loss of generality, suppose $\pi(1) \neq \sigma(1)$. We cannot have both $\pi(1) = 1$ and $\sigma(1) = 1$. Without loss of generality, assume $\pi(1) \neq 1$, say $\pi(1) = 2$.

Suppose first that $\pi(2) \neq 1$, say $\pi(2) = 3$. So,

$$\pi \supset (\cdots 1 2 3 \cdots).$$

We consider the following (exhaustive) list of cases:

(a) $\sigma(1) = 1$: $\sigma \supset (1)$;
(b) $\sigma(1) = 3, \sigma(3) = 1$: $\sigma \supset (1 3)$;
(c) $\sigma(1) = 3, \sigma(3) = 2$: $\sigma \supset (\cdots 1 3 2 \cdots)$;
(d) $\sigma(1) = 3, \sigma(3) \neq 1, 3$, say, $\sigma(3) = 4$: $\sigma \supset (\cdots 1 3 4 \cdots)$;
(e) $\sigma(1) \neq 1, 3$, say $\sigma(1) = 4$: $\sigma \supset (\cdots 1 4 \cdots)$.

In each of the cases, we find an element of the family $C$ that $T_0$-separates $\pi$ and $\sigma$:

(a) $(1 3)C(1 2)$, because $(1 3)\pi \supset (1 2)$, while $(1 3)\sigma \supset (\cdots 1 3 \cdots)$;
(b) $C(1 3)$, because $\pi \supset (\cdots 1 2 3 \cdots)$, while $\sigma \supset (1 3)$;
(c) $(1 3)C(1 2)$, because $(1 3)\pi \supset (1 2)$, while $(1 3)\sigma \supset (1)(\cdots 3 2 \cdots)$;
(d) $(1 4)C(1 3)$, because $(1 4)\pi \supset (\cdots 1 2 3 \cdots)$, while $(1 4)\sigma \supset (1 3)$;
(e) $(1 3)C(1 2)$, because $(1 3)\pi \supset (1 2)$, while $(1 3)\sigma \supset (\cdots 1 4 \cdots)$.

Now consider the case when $\pi(2) = 1$:

$$\pi \supset (1 2).$$

If $\sigma(1) \neq 1$ or $\sigma(2) \neq 2$, then $\pi$ and $\sigma$ are $T_0$-separated by $C(1 2)$. So suppose $\sigma(1) = 1$ and $\sigma(2) = 2$:

$$\sigma \supset (1)(2).$$

Case $\pi(3) \neq \sigma(3)$: If $\pi(3) \neq 3$, say $\pi(3) = 4$, by repeating the above argument, we can $T_0$-separate $\pi$ and $\sigma$ in all of the cases, except possibly when

$$\pi \supset (1 2)(3 4),$$
$$\sigma \supset (1)(2)(3)(4).$$
But then, $\pi$ and $\sigma$ are $T_0$-separated by $C(1\ 3)$. If $\sigma(3) \neq 3$, say $\sigma(3) = 4$, we can $T_0$-separate $\pi$ and $\sigma$ as before, in all of the cases, except possibly when

$$\pi \supset (1\ 2)(3)(4),$$

$$\sigma \supset (1)(2)(3\ 4).$$

But then, $\pi$ and $\sigma$ are $T_0$-separated by $(1\ 3\ 2)C(1\ 3)$: since $(1\ 2\ 3)\pi \supset (1\ 3)(2)(4)$, and $(1\ 2\ 3)\sigma \supset (1\ 2\ 3\ 4)$.

Case $\pi(3) = \sigma(3)$: If $\pi(3) = \sigma(3) = 3$, then $\pi \supset (1\ 2)(3)$, and $\sigma \supset (1)(2)(3)$, so $\pi$ and $\sigma$ are $T_0$-separated by $C(1\ 3)$. Otherwise, we may take $\pi(3) = \sigma(3) = 4$. In this case, $(3\ 4)\pi \supset (1\ 2)(3)$, and $(3\ 4)\sigma \supset (1)(2)(3)$, so $\pi$ and $\sigma$ are $T_0$-separated by $(3\ 4)C(1\ 3)$. □

**Theorem 28.** $S_\infty$ admits a unique Polish group topology.

*Proof.* The family $\mathcal{C}$ from Lemma 27 is a countable $T_0$-separating family of identity sets. By Corollary 20 the Polish group topology on $S_\infty$ is unique. □

### 4.2 COMPACT LIE GROUPS

In this section we give an application of Theorem 24 to show that compact, connected, simple Lie groups have a unique Polish group topology. An example of such a group is the special orthogonal group $SO(3, \mathbb{R})$.

Only last week we discovered a paper by Kallman [13] in which he proves a stronger result that all compact connected metric groups with totally disconnected center have a unique Polish group topology. We still include our proof here as it was obtained independently and uses our general theorem.

Recall that a topological group is a *Lie group* if and only if its topology is locally Euclidean [20]. A Lie group is *semisimple* if and only if it has no non-trivial connected normal Abelian subgroups; a compact, connected, Lie group is semisimple if and only if its center is finite [8]. A semisimple Lie group $G$ is a *simple Lie group* if there are no infinite connected Lie groups $E$ and $F$ such that $G$ is locally isomorphic to $E \times F$. 29
For a group $G$ and $a \in G$ we denote by $M_G(a)$, or $M(a)$ when confusion is impossible, the set

$$M_G(a) = \{ cbab^{-1}a^{-1}c^{-1} \mid b, c \in G \}.$$

We take this definition from [3], where this set is studied and used to prove van der Waerden’s Continuity Theorem [23]: Every homomorphism from a compact, connected, simple Lie group with trivial center into a compact topological group is continuous. Lemmas 29 and 30 below, which state important properties of the set $M(a)$, are taken from the same source.

**Lemma 29.** Let $K$ be a compact metrizable topological group and let $(a_n)$ be a sequence in $K$ such that $a_n \to 1$. Then for every (open) neighborhood $V$ of the identity, there is $n$ such that $M(a_n) \subseteq V$.

**Lemma 30.** Let $G$ be an $m$-dimensional compact, connected, simple Lie group and let $a \in G$ be a non-central element of $G$. Then the set

$$N(a) = \{ \prod_{i=1}^{m} h_i \mid h_i \in M(a) \}$$

is a neighborhood of the identity.

Proofs of both lemmas can be found in [3], as a part of the proof of van der Waerden’s theorem. While Lemma 29 is elementary, Lemma 30 is crucial to our argument, and we give here a proof in the special case when $G = SO(3, \mathbb{R})$.

Recall that $SO(3, \mathbb{R})$ is the group of the special orthogonal matrices

$$SO(3, \mathbb{R}) = \{ A \in M_3(\mathbb{R}) \mid A^{-1} = A^T, \det A = 1 \}.$$

With the relative topology as a subset of $\mathbb{R}^9$, it is a Polish group. The elements of $SO(3, \mathbb{R})$ are routinely identified with the rotations of the unit sphere $S^2$ via $T \mapsto [T]_B$, where $T \in \mathcal{L}(\mathbb{R}^3)$ is a rotation of $S^2$, $B$ is a fixed orthonormal basis of $\mathbb{R}^3$ and $[T]_B$ denotes the matrix of $T$ with respect to the basis $B$. Then, for $A_n, A \in SO(3, \mathbb{R})$, $A_n \to A$ if and only if the angle of rotation of $A_n$ approaches the angle of rotation of $A$ and the axis of rotation of $A_n$ approaches the axis of rotation of $A$. The identity matrix will be denoted by $E$. Also, we will write $R_{a, \alpha}$, where $a \in S^2$ and $\alpha \in [0, \pi]$, for the rotation with the axis $a$ and angle $\alpha$.  
Lemma 31. (a) Matrices $A, B \in SO(3, \mathbb{R})$ belong to the same conjugacy class in $SO(3, \mathbb{R})$ if and only if $A$ and $B$ represent rotations by the same angle.

(b) If $E \neq A \in SO(3, \mathbb{R})$, there exists $B \in SO(3, \mathbb{R})$ such that $AB \neq BA$.

(c) $SO(3, \mathbb{R})$ is path-connected.

Proof. (a) If distinct matrices $A$ and $B$ represent rotations by the same angle with respect to the standard basis in $\mathbb{R}^3$, we can think of $A$ and $B$ as representing the same linear transformation, but with respect to two different (positively oriented) orthonormal bases of $\mathbb{R}^3$. If $P$ is the change of bases matrix between the two (positively oriented) orthonormal bases, then $P \in SO(3, \mathbb{R})$ and $P^{-1}AP = B$. So $A$ and $B$ belong to the same conjugacy class. Conversely, if $B = P^{-1}AP$ for some $P \in SO(3, \mathbb{R})$, thinking of $P$ as a change of bases matrix, we see that $A$ and $B$ must represent rotations by the same angle.

(b) Suppose for a contradiction that $A$ commutes with all elements of $SO(3, \mathbb{R})$. Let $C$ be a rotation by the same angle as the angle of $A$, but with a different axis. Then, by part (a), $C = P^{-1}AP$ for some $P \in SO(3, \mathbb{R})$. But then $A$ commutes with $P$, so $C = P^{-1}AP = P^{-1}PA = A$, a contradiction.

(c) Let $A = R_{a, \alpha} \in SO(3, \mathbb{R})$. Then $f : [0, 1] \to SO(3, \mathbb{R})$, given by $f(t) = R_{a, t\alpha}$, is a continuous path connecting $E$ and $A$.

We denote by $Rot(\theta)$, $\theta \in [0, \pi]$ the conjugacy class of rotations by angle $\theta$.

Proof of Lemma 30 in case $G = SO(3, \mathbb{R})$. By Lemma 31 (b), the center of $SO(3, \mathbb{R})$ is trivial. Let $A$ be a non-central element of $SO(3, \mathbb{R})$, i.e. $A \neq E$. We will show that $M(A)$ is a neighborhood of $E$ (and thus, so is $N(A) \supseteq M(A)$). Choose $B \in SO(3, \mathbb{R})$ such that $BAB^{-1}A^{-1} \neq E$. Let $\gamma > 0$ be the angle of rotation of $BAB^{-1}A^{-1}$. Define

$$U = \{X \in SO(3, \mathbb{R}) \mid \text{the angle of rotation of } X \text{ is } < \gamma\} = \bigcup_{\theta \in [0, \gamma)} \{X \in SO(3, \mathbb{R}) \mid \text{the angle of rotation of } X \text{ is } \theta\} = \bigcup_{\theta \in [0, \gamma)} Rot(\theta).$$

31
Set $U$ is clearly an open neighborhood of $E$. We will show that it is a subset of $M(A)$.

Since $SO(3, \mathbb{R})$ is path-connected (Lemma 31 (c)), there exists a continuous map $f : [0, 1] \to SO(3, \mathbb{R})$ such that $f(0) = E$ and $f(1) = B$. Define

$$B_t = f(t) \quad \text{and} \quad P_t = B_t A B_t^{-1} A^{-1}.$$ 

The function $g : [0, 1] \to [0, \pi]$ that maps $t$ to the angle of $P_t$, is a continuous function with $g(0) = 0$ and $g(1) = \gamma$. By the Intermediate Value Theorem, for each $\theta \in [0, \gamma]$, there exists $t_{\theta}$ such that $g(t_{\theta}) = \theta$. So the angle of $P_{t_{\theta}}$ is $\theta$. By the part (a) of Lemma 31, it follows that $\text{Rot}(\theta)$ is the conjugacy class of $P_{t_{\theta}}$. So,

$$U = \bigcup_{\theta \in [0, \gamma]} \text{Rot}(\theta) = \bigcup_{\theta \in [0, \gamma]} \{ CP_{t_{\theta}} C^{-1} | C \in SO(3, \mathbb{R}) \} = \{ CB_{t_{\theta}} A B_{t_{\theta}}^{-1} A^{-1} C^{-1} | \theta \in [0, \gamma], C \in SO(3, \mathbb{R}) \},$$

so $U \subseteq M(A)$. \hfill \qed

**Theorem 32.** If $G$ is a compact, connected, simple Lie group (for example, the special orthogonal group $SO(3, \mathbb{R})$), then $G$ has a unique Polish group topology.

**Proof.** We show that the family

$$\{ N(a) \mid a \text{ is a non-central element of } G \}$$

forms a neighborhood base at the identity for the topology on $G$. Indeed, the members of the family are neighborhoods of 1, by Lemma 30. Also, given an open neighborhood $U$ of 1, we find a non-central element $a$ such that $N(a) \subseteq U$. First, choose an open neighborhood $V$ of 1 such that $V^m \subseteq U$. Since $G$ is connected, 1 is not isolated, and by the separation property $T_2$ we can find a sequence of distinct points $a_n$ in $G$ such that $a_n \to 1$. Since the center of $G$ is finite, we may assume without loss of generality that all $a_n$'s are non-central. By Lemma 29, there exists $n$ such that $M(a_n) \subseteq V$. Write $a = a_n$. Then $N(a) \subseteq V^n \subseteq U$.

Observe that each of the sets $N(a)$, for $a \in G$, is a verbal set. The uniqueness of the Polish group topology now follows from Theorem 24. \hfill \qed
It is worth noting here that this uniqueness result could not be obtained by applying Mackey’s theorem with identity sets, since, as we show in Corollary 34 below, it is not possible to find a countable point-separating family of identity sets.

**Lemma 33.** If $G$ is a connected Lie group, then the identity sets in $G$ are either closed nowhere dense or equal to $G$.

**Proof.** Let $A$ be an identity set in $G$. Then $A = f^{-1}\{1\}$, where $f : G \to G$ is given by $f(x) = w(x; c_1, \ldots, c_m)$, for some free word $w$ and some fixed elements $c_1, \ldots, c_m$ in $G$. Suppose that $A$ is not nowhere dense. Then $A$ contains a non-empty open subset $U$. Because the maps $(x, y) \mapsto xy$ and $x \mapsto x^{-1}$ are analytic, and the composition of analytic functions is analytic, $f$ is analytic. Let $g : G \to G$ be the constant function 1. Then the analytic functions $f$ and $g$ coincide on $U$, so by the identity theorem for analytic functions, $f$ and $g$ agree on the connected component of $U$. Since $G$ is connected, $f = g$. It follows that $A = G$. \hfill \Box

**Corollary 34.** If $G$ is a connected Lie group, no countable family of identity sets separates points in $G$.

**Proof.** Suppose $A$ is a countable family of identity sets that separate points in $G$. Assume, without loss of generality, that $G \notin A$. Then $A$ is a countable cover of $G$ by closed nowhere dense sets, which contradicts the Baire category theorem. \hfill \Box

### 4.3 PROFINITE GROUPS

In this section we give an application of Theorem 24 to finitely generated profinite groups.

A **profinite group** is a zero-dimensional compact Hausdorff topological group, or equivalently a compact Hausdorff group whose open normal subgroups form a base for the neighborhoods of the identity.

Note that if $G$ is a profinite group and $U$ is an open normal subgroup, then $G/U$ is a finite group.
A profinite group, $G$, such that for every open normal subgroup $U$, the group $G/U$ is a $p$-group is called a pro-$p$ group. A topological group $G$ is said to have the finite index property if every subgroup of $G$ of finite index is necessarily open.

Serre (see [10]) proved that every (topologically) finitely generated pro-$p$ group has the finite index property. Serre went on to conjecture that every finitely generated profinite group has the finite index property. Serre’s conjecture has recently been proved by Nikolov and Segal [21].

A group word $w$ is said to be $d$-locally finite if every $d$-generator (abstract) group $H$ satisfying $w(H) = 1$ is necessarily finite. Lemmas 35 and 36 below are key results from [21], we include the proof of the latter as it is not explicitly stated.

**Lemma 35.** Let $w$ be a $d$-locally finite group word and let $G$ be a $d$-generator profinite group. Then the verbal subgroup $w(G)$ is open in $G$.

**Lemma 36.** If $G$ is a finitely generated profinite group, then every open normal subgroup of $G$ contains an open verbal subgroup.

**Proof.** Let $G$ be a $d$-generator profinite group and $N$ an open normal subgroup of $G$ (so $G/N$ is finite). Let $F$ be the free group on free generators $x_1, \ldots, x_d$ and let

$$D = \bigcap \{ \ker \theta \mid \theta : F \to G/N \text{ is a homomorphism} \}.$$ 

Then $D$ is the intersection of finitely many subgroups of finite index, and thus itself has finite index in $F$. It follows that $D$ is a free group of finite rank $m$ given by the Schreier index formula:

$$D = \langle w_1(x_1, \ldots, x_d), \ldots, w_m(x_1, \ldots, x_d) \rangle.$$ 

From the definition of $D$, it follows that $w_i(u) \in D$ for each $i$ and any $u \in F^d$. Thus, setting

$$w(y_1, \ldots, y_m) = w_1(y_1)w_2(y_2)\cdots w_m(y_m),$$ 

where $y_1, \ldots, y_m$ are disjoint $d$-tuples of variables, we have $w(F) = D$. We show that this implies that the word $w$ is $d$-locally finite. For if $H$ is a $d$-generator abstract group, then $H = F/K$ for some normal subgroup $K$ of the free group on $d$ generators. If $w(H) = 1$, then...
then $w(F) \subseteq K$. But now $K$ has finite index in $F$ because it contains $w(F) = D$ which has finite index in $F$, and so $H = F/K$ is finite, as required. Also, $w(G) \subseteq N$, since $w_i(g) \in N$ for each $i$ and any $g \in G^d$. By Lemma 35, $w(G)$ is an open verbal subgroup of $G$ contained in $N$.

**Theorem 37.** Let $G$ be a finitely generated profinite group. Then $G$ has a unique Polish group topology.

**Proof.** By definition, $G$ has a neighborhood base at the identity of open subgroups. Each open subgroup in a profinite group contains a normal open subgroup, and by Lemma 36, each open normal subgroup contains an open verbal subgroup. Thus, $G$ has a neighborhood base at the identity of verbal subgroups, which are analytic (Lemma 19). By Theorem 24, $G$ has a unique Polish group topology. \qed

---

35
PART II

COMPLEXITY OF VERBAL SETS
5.0 COMPLEXITY OF VERBAL SETS

As we have seen in Chapters 3 and 4, the notion of definability of sets plays an important role in many proofs of the uniqueness of topology. In particular, it is important to understand which algebraically definable sets are Borel.

In this chapter we investigate the complexity of verbal sets in various Polish groups. While in many situations we will be able to show that verbal sets are Borel, the most interesting result for us is the example of a verbal set that is completely analytic, and hence not Borel (see Theorem 53). This result establishes that not all verbal sets are Borel.

Definitions and Notation. Let $X$ be any set. For $a_1, \ldots, a_n$ ($n \geq 1$), distinct elements of $X$,

$$(a_1 \ a_2 \ \cdots \ a_n)$$

denotes the permutation of $X$ that maps $a_i$ to $a_{i+1}$ for $i = 1, 2, \ldots, n-1$, and $a_n$ to $a_1$, leaving the the other elements of $X$ fixed. We call such a permutation a finite cycle or, more specifically, an $n$-cycle or a cycle of length $n$. Similarly, for a sequence $(a_i)_{i \in \mathbb{Z}}$ of distinct elements of $X$,

$$(\cdots \ a_{-1} \ a_0 \ a_1 \ a_2 \ \cdots)$$

denotes the permutation of $X$ that maps each $a_i$ to $a_{i+1}$ and leaves the other elements of $X$ fixed. We call such a permutation an infinite cycle or a cycle of infinite length.

Any permutation of $X$ can be represented by an unordered formal composition of disjoint cycles in a unique way. We say that a permutation $f$ contains a cycle $\sigma$ if $\sigma$ is one of the cycles in the unique disjoint cycle representation of $f$. If $f$ contains disjoint cycles $\sigma_1, \ldots, \sigma_k, \ldots$, we also say that $f$ contains the product $\sigma_1 \cdots \sigma_k [\cdots]$. 

37
If $G$ is a group, $G^{(n)}$ will denote the set of all $n$-th powers in $G$:

$$G^{(n)} = \{g^n \mid g \in G\}.$$

### 5.1 ABELIAN GROUPS

We will show that in Abelian Polish groups full verbal sets are necessarily Borel. For this we will use the following well known result from the theory of Polish group actions, see [19], or [15] p. 93:

**Theorem 38.** (Miller) Let $G$ be a Polish group, $X$ a standard Borel space, and $(g, x) \mapsto g.x$ a Borel action of $G$ on $X$. Then every orbit $\{g.x \mid g \in G\}$ is Borel.

**Theorem 39.** Let $(G, +)$ be an Abelian Polish group and $w(x_1, \ldots, x_n)$ a free word on $n$ letters. Then the verbal set $V = \{w(g_1, \ldots, g_n) \mid g_1, \ldots, g_n \in G\}$, is Borel in $G$.

**Proof.** Consider the map $\phi : G^n \to G$, defined by $\phi(g_1, \ldots, g_n) = w(g_1, \ldots, g_n)$. It is continuous by the continuity of the group operations and it is a homomorphism since the group $G$ is Abelian. Let the Polish group $G^n$ act on $G$ by $(g, h) \mapsto g.h := \phi(g) + h$, for $g \in G^n, h \in G$. By the properties of $\phi$, this is a well defined continuous (and thus, Borel) action of $G^n$ on $G$. By Theorem 38, the orbits of this action are Borel. In particular, the orbit of the zero element: $\{g.0 \mid g \in G^n\} = \{\phi(g) \mid g \in G^n\} = V$, is Borel.

### 5.2 INFINITE SYMMETRIC GROUP

Recall that $S_\infty$ denotes the group of permutations of $\mathbb{N}$ with the topology inherited from the Tychonoff product $\mathbb{N}^\mathbb{N}$.

**Theorem 40.** Full verbal sets in $S_\infty$ are Borel.
To prove this, we first appeal to [5] where it is shown that if \( w(x_1, \ldots, x_n) \) is a free word that is not a proper power, then the verbal set \( w(S_{\infty}^n) \) is the whole of \( S_{\infty} \), in which case it is certainly Borel. Thus it remains to show that for each \( m \geq 1 \), the set
\[
S_{\infty}^{(m)} = \{ \pi^m \mid \pi \in S_{\infty} \}
\]
of all \( m \)-th powers in \( S_{\infty} \), is Borel.

We first show that the set of squares \( S_{\infty}^{(2)} \) is Borel. The ideas of this proof are then extended to show that for any \( m \geq 1 \), the set of \( m \)-th powers \( S_{\infty}^{(m)} \) is Borel.

### 5.2.1 Set of Squares

In Theorem 41 we give necessary and sufficient conditions for a permutation in \( S_{\infty} \) to be a square. We use this characterization in Theorem 43 to prove that \( S_{\infty}^{(2)} \) is Borel.

**Theorem 41 (Characterization of Squares).** For a permutation \( \pi \in S_{\infty} \) the following are equivalent:

(i) \( \pi \in S_{\infty}^{(2)} \),

(ii) For every \( 1 \leq n \leq \infty \), the number of \( 2n \)-cycles in the cycle representation of \( \pi \) is even. (Here, \( 2 \cdot \infty = \infty \) and \( \infty \) is considered to be even).

**Proof.** We investigate the cycle structure of the disjoint cycle decomposition of a square permutation. We note the following:

(a) The square of an infinite cycle is a product of two infinite cycles:
\[
(\cdots a_{-1} a_0 a_1 a_2 \cdots)^2 = (\cdots a_{-2} a_0 a_2 \cdots)(\cdots a_{-1} a_1 a_3 \cdots);
\]

(b) The square of a finite cycle of length \( 4n \) is a product of two \( 2n \)-cycles:
\[
(a_1 a_2 \cdots a_{4n})^2 = (a_1 a_3 \cdots a_{4n-1})(a_2 a_4 \cdots a_{4n});
\]

(c) The square of a \( (4n + 2) \)-cycle is a product of two \( (2n + 1) \)-cycles:
\[
(a_1 a_2 \cdots a_{4n+2})^2 = (a_1 a_3 \cdots a_{4n+1})(a_2 a_4 \cdots a_{4n+2});
\]
(d) The square of a finite cycle of length \(2n + 1\) is another \((2n + 1)\)-cycle:

\[
(a_1 \ a_2 \ \cdots \ a_{2n+1})^2 = (a_1 \ a_3 \ \cdots \ a_{2n+1} \ a_2 \ a_4 \ \cdots \ a_{2n}).
\]

From these observations we see that in a disjoint cycle representation of a square permutation, the infinite cycles occur in pairs (see (a)). Also, for any \(n \in \mathbb{N}\), the \(2n\)-cycles appear in pairs (b), while the \((2n + 1)\)-cycles may occur either in pairs (c) or alone (d). Thus, if \(\pi \in S_\infty^{(2)}\), then the number of \(2n\)-cycles in \(\pi\) for \(1 \leq n \leq \infty\) is even (including, possibly, infinite).

Conversely, suppose that (ii) holds. Construct a permutation \(\rho\) from \(\pi\) as follows:

(a) If \((\cdots \ a_0 \ a_1 \ \cdots)(\cdots \ b_0 \ b_1 \ \cdots)\) is in the disjoint cycle decomposition of \(\pi\), let \((\cdots \ a_0 \ b_0 \ a_1 \ b_1 \ \cdots)\) be a cycle of \(\rho\);
(b) If \((a_1 \ a_2 \ \cdots \ a_{2n})(b_1 \ b_2 \ \cdots \ b_{2n})\) is in \(\pi\), let \((a_1 \ b_1 \ \cdots \ a_{2n} \ b_{2n})\) be a cycle of \(\rho\);
(c) If \((a_1 \ a_2 \ \cdots \ a_{2n+1})\) is a cycle of \(\pi\), let \((a_1 \ a_{n+2} \ a_2 \ a_{n+3} \ a_3 \ \cdots \ a_{2n+1} \ a_{n+1})\) be a cycle of \(\rho\).

Of course such a permutation \(\rho\) is not uniquely determined. It is clear from the construction that \(\pi = \rho^2\), so \(\pi \in S_\infty^{(2)}\).

**Lemma 42.** For all \(k = 1, 2, \ldots\) and \(n = 1, 2, \ldots\) or \(n = \infty\), the set

\[
B(k; n) := \{\pi \in S_\infty \mid \pi \text{ contains (at least) } k \text{ cycles of length } n\}
\]

is Borel \((F_\sigma)\).

**Proof.** For \(b_1, b_2, \ldots, b_n \in \mathbb{N}\), where \(n \geq 1\), let

\[
U(b_1, \ldots, b_n) := \{\pi \in S_\infty \mid \pi(b_1) = b_2, \ldots, \pi(b_{n-1}) = b_n\}.
\]

This set is clopen in \(S_\infty\), since it is the intersection of the basic clopen subset \(\{f \in \mathbb{N}\mathbb{N} \mid f(b_1) = b_2, \ldots, f(b_{n-1}) = b_n\}\) of \(\mathbb{N}\mathbb{N}\) with \(S_\infty\).

For \(a, b \in \mathbb{N}\) and \(m \geq 1\), let

\[
V(a, b; m) := \{\pi \in S_\infty \mid \pi^m(a) = b\}.
\]
Then $V(a, b; 1) = U(a, b)$ and for $m = 2, 3, \ldots$

$$V(a, b; m) = \{ \pi \mid \exists b_2, \ldots, b_m \in \mathbb{N}, \pi(a) = b_2, \pi(b_2) = b_3, \ldots, \pi(b_m) = b \}$$

$$= \bigcup_{b_2, \ldots, b_m \in \mathbb{N}} U(a, b_2, \ldots, b_m, b).$$

So $V(a, b; m)$ is open for all $m \geq 1$.

For $a_1 \in \mathbb{N}$ and $1 \leq n \leq \infty$, the set

$$W(a_1; n) := \{ \pi \in S_\infty \mid \pi \text{ contains } (\underbrace{a_1 \ldots}_n) \}$$

is Borel (closed or open) in $S_\infty$. Indeed, $W(a_1; 1) = U(a_1, a_1)$, and for $n = 2, 3, \ldots$

$$W(a_1; n) = \{ \pi \mid \exists b_2, \ldots, b_n \in \mathbb{N} \text{ such that } \pi \text{ contains } (a_1 b_2 \ldots b_n) \}$$

$$= \bigcup_{b_2, \ldots, b_n \in \mathbb{N}} U(a_1, b_2, \ldots, b_n, a_1),$$

so $W(a_1; n)$ is open for $n = 1, 2, \ldots$. For $n = \infty$, $W(a_1; n)$ is closed, since:

$$W(a_1; \infty) = \{ \pi \mid \pi \text{ contains a cycle } (\underbrace{a_1 \ldots}_n) \text{ of infinite length} \}$$

$$= \{ \pi \mid \forall m = 1, 2, \ldots, \pi \text{ does not contain } (\underbrace{a_1 \ldots}_m) \}$$

$$= \bigcap_{m \geq 1} (S_\infty \setminus W(a_1; m)).$$

For $a_1, a_2, \ldots, a_k \in \mathbb{N}$ ($k \geq 1$) pairwise distinct and $1 \leq n \leq \infty$, the set

$$W(a_1, \ldots, a_k; n) := \{ \pi \in S_\infty \mid \pi \text{ contains } (\underbrace{a_1 \ldots}_n) \ldots (\underbrace{a_k \ldots}_n) \},$$
is Borel in $S_\infty$. We have already shown this set is Borel in the case $k = 1$. For $k > 1$ and $1 \leq n \leq \infty$, $W(a_1, \ldots, a_k; n)$ is Borel ($F_\sigma$ and $G_\delta$) because

$$W(a_1, \ldots, a_k; n) = \{\pi \mid \forall i = 1, \ldots, k, \pi \text{ contains } (\cdot \cdot \cdot a_i \cdot \cdot \cdot) \text{ and }$$

$$\forall i \neq j \in \{1, \ldots, k\}, \text{ the cycles containing } a_i \text{ and } a_j \text{ are distinct}\}$$

$$= \bigcap_{1 \leq i \leq k} \{\pi \mid \pi \text{ contains } (\cdot \cdot \cdot a_i \cdot \cdot \cdot)\} \cap \bigcap_{1 \leq i \leq j \leq k} \{\pi \mid \forall m = 1, 2, \ldots \pi^m(a_i) \neq a_j \text{ and } \pi^m(a_j) \neq a_i\}$$

$$= \bigcap_{1 \leq i \leq k} W(a_i; n) \cap \bigcap_{1 \leq i \leq j \leq k} (S_\infty \setminus (V(a_i, a_j; m) \cup V(a_j, a_i; m))].$$

Finally, for $k = 1, 2, \ldots$ and $1 \leq n \leq \infty,$

$$B(k; n) = \{\pi \mid \exists a_1, \ldots, a_k \in \mathbb{N} \text{ such that } \pi \text{ contains } (\cdot \cdot \cdot a_1 \cdot \cdot \cdot) \ldots (\cdot \cdot \cdot a_k \cdot \cdot \cdot)\}$$

$$= \bigcup_{a_1, \ldots, a_k \in \mathbb{N}} W(a_1, \ldots, a_k; n).$$

Thus $B(k; n)$ is Borel ($F_\sigma$).

\[\square\]

**Theorem 43.** $S_\infty^{(2)}$ is Borel ($F_\sigma \delta$) in $S_\infty$.

**Proof.** Using the characterization of the square permutations given in Lemma 41, we express $S_\infty^{(2)}$ as a Boolean combination of sets previously shown to be Borel:

$$S_\infty^{(2)} = \{\pi \in S_\infty \mid \text{for all } 1 \leq n \leq \infty \text{ and for all } k \geq 1, \text{ if } \pi \text{ has } 2k - 1 \text{ cycles of length } 2n, \text{ then it has } 2k \text{ cycles of length } 2n\}$$

$$= \bigcap_{n,k} \left(\{\pi \mid \pi \text{ does not have } 2k - 1 \ 2n\text{-cycles}\} \cup \{\pi \mid \pi \text{ has } 2k \ 2n\text{-cycles}\}\right)$$

$$= \bigcap_{n,k} (S_\infty \setminus B(2k - 1; 2n)) \cup B(2k; 2n)).$$

So by Lemma 42, the set $S_\infty^{(2)}$ is Borel ($F_\sigma \delta$).

\[\square\]
5.2.2 Set of m-th Powers

Consider now the set $S^{(m)}$ of all $m$-th powers in $S_\infty$, where $m \geq 1$. We will characterize the elements of this set (Theorem 45), and then show it is Borel (Theorem 46).

**Lemma 44.** (a) The unique disjoint cycle representation of the $m$-th power of a cycle of length $N$ consists of $d$ cycles, each of length $l := \frac{N}{d}$, where $d = (N, m)$;
(b) The unique disjoint cycle representation of the $m$-th power of an infinite cycle consists of $m$ infinite cycles.

**Proof.** (a) Let $\sigma = (a_1 \cdots a_N)$. By symmetry, $\sigma^m$ consists of finite cycles of equal length. The elements in the cycle that contains $a_1$ are all $a_k$'s with $k = (1 + jm) \mod N$, for some $j = 0, 1, 2, \ldots$ (Here, $s \mod N$ denotes the remainder in the integer division of $s$ by $N$.) Let $x$ be the smallest positive integer solution of the equation

$$1 + xm \equiv 1 \pmod{N}.$$ 

Then there are exactly $x$ indices $k$ of the form $(1 + jm) \mod N$. In other words, the length of the cycle containing $a_1$ is precisely $x$. Now, $1 + xm \equiv 1 \pmod{N}$ if and only if $xm = yN$ for some integer $y$. The smallest positive solution to this equation is $x = \frac{N}{d}$. It follows that the length of each cycle in $\sigma^m$ is $\frac{N}{d}$, and the number of the cycles clearly must be $d$.

(b) It is clear that

$$(\cdots a_1 a_2 \cdots)^m = (\cdots a_1 a_{m+1} \cdots)(\cdots a_2 a_{m+2} \cdots) \cdots (\cdots a_m a_{2m} \cdots),$$

so the statement follows. $\square$

**Theorem 45** (Characterization of m-th Powers). Let $m = \prod_{i=1}^{s} p_i^{\alpha_i}$, where for each $i$, $p_i$ is prime and $\alpha_i > 0$, be the unique prime factorization of $m \geq 1$. For a permutation $\pi \in S_\infty$ the following are equivalent:

(i) $\pi \in S^{(m)}_\infty$,
(ii) For every $1 \leq n \leq \infty$ the number of $p_in$-cycles is divisible by $p_i^{\alpha_i}$. (Here, $\infty \cdot n = \infty$ and $\infty$ is considered to be divisible by any finite number. Note that in particular, the number of infinite cycles is divisible by $m$.)
Proof. Suppose that $π ∈ S^{(m)}_∞$ and let $ρ ∈ S_∞$ be such that $π = ρ^m$.

Let $n ∈ \{1, 2, \cdots\}$. By Lemma 44 (a), cycles of a given length in $π$ appear in groupings of equal size, more precisely: if $π$ contains a cycle of length $p_i^n$, then there exist $k ≥ 1$, disjoint $p_i^n$-cycles $σ_2, \ldots, σ_k$ in $π$, and a $p_i^n k$-cycle $σ$ in $ρ$ such that

$$σ^m = σ_1σ_2 \cdots σ_k$$

and

$$(m, p_i nk) = k.$$ Writing $m = p_i^{α_i} m_1$, $n = p_i^{β_i} n_1$, and $k = p_i^{γ_i} k_1$, where $(m_1, p_i) = (n_1, p_i) = (k_1, p_i) = 1$, we get

$$(p_i^{α_i} m_1, p_i^{1 + β_i + γ_i} n_1 k_1) = p_i^{γ_i} k_1.$$ It follows that $γ_i = \min(α_i, 1 + β_i + γ_i)$, so $γ_i = α_i$. Thus, $k$ is divisible by $p_i^{α_i}$. We conclude that the number of $p_i^n$-cycles in $π$ is divisible by $p_i^{α_i}$ (possibly infinite).

If $n = ∞$, and $σ_1$ is an infinite cycle in $π$, then by Lemma 44 (b), there exist disjoint infinite cycles $σ_2, \ldots, σ_m$ in $π$ and an infinite cycle $σ$ in $ρ$ such that

$$ρ^m = σ_1σ_2 \cdots σ_m.$$ Thus, the number of infinite cycles in $π$ is divisible by $m$.

Conversely, let $π$ be a permutation in $S_∞$ satisfying (ii). We will construct a permutation $ρ$ such that $ρ^m = π$.

Fix $1 ≤ l ≤ ∞$. By (ii), the number of cycles in $π$ of length $l$ is divisible by $p_i^{α_i}$, for each $i$ with $p_i|l$. Thus, the number of $l$-cycles in $π$ is divisible by

$$d := \prod_{p_i|l} p_i^{α_i}$$

(possibly infinite). Let

$$N := dl \quad (N = ∞ \text{ if } l = ∞).$$ Note that for finite $l$, $d = (N, m)$. For $l = ∞$, $d = \prod_{i=1}^{∞} p_i^{α_i} = m$. 

44
Divide the cycles of length \( l \) in \( \pi \) into pairwise disjoint groupings of \( d \)-many. Let \( \sigma_1, \sigma_2, \ldots, \sigma_d \) be a grouping of \( l \)-cycles in \( \pi \). By Lemma 44, the product \( \sigma_1\sigma_2\cdots\sigma_d \) can be written as the \( m \)-th power of a cycle \( \sigma \) of length \( N \). Put the cycle \( \sigma \) into the permutation \( \rho \).

Doing this for each length \( l \), \( 1 \leq l \leq \infty \), and each grouping of \( l \)-cycles in \( \pi \), we complete the construction of \( \rho \). It is clear by design that \( \rho^m = \pi \).

**Theorem 46.** \( S^{(m)}_{\infty} \) \( (m \geq 1) \) is Borel \( (F_{0\delta}) \) in \( S_{\infty} \).

**Proof.** Let \( m = \prod_{i=1}^{s} p_i^{\alpha_i} \), \( \alpha_i > 0 \), be the unique prime factorization of \( m \). By Lemma 45, a permutation \( \pi \) is in \( S^{(m)}_{\infty} \) if and only if for all prime factors \( p_i \) of \( m \), for all \( n \in \{1, 2, \ldots\} \cup \{\infty\} \) and for all \( k \in \{1, 2, \ldots\} \), if \( \pi \) has \( p_i^{\alpha_i}(k-1)+1 \) \( p_i n \)-cycles, then \( \pi \) has \( p_i^{\alpha_i} k \) \( p_i n \)-cycles. Thus,

\[
S^{(m)}_{\infty} = \bigcap_{p_i, n, k} ((S_{\infty} \setminus B(p_i^{\alpha_i}(k-1)+1; p_i n)) \cup B(p_i^{\alpha_i} k; p_i n)),
\]

where \( B(k; n) \) denotes the set of permutations that have (at least) \( k \) cycles of length \( n \). By Lemma 42, it follows that \( S^{(m)}_{\infty} \) is Borel \( (F_{0\delta}) \). \( \Box \)

### 5.3 AUTOHOMEOMORPHISM GROUP OF THE UNIT INTERVAL

Let \( \text{Homeo}(I) \) denote the group of autohomeomorphisms of the (closed) unit interval \( I \). With the topology induced by the supremum metric, \( \text{Homeo}(I) \) is a Polish group. We will show that the set of squares

\[
\text{Homeo}(I)^{(2)} = \{ f^2 = f \circ f \mid f \in \text{Homeo}(I) \}
\]

is Borel (clopen).

Let \( \text{Homeo}^+(I) \) be set of the order preserving (increasing) homeomorphisms of \( I \):

\[
\text{Homeo}^+(I) = \{ f \in \text{Homeo}(I) \mid \forall x, y \in I, \ x < y \Rightarrow f(x) < f(y) \}
\]

and \( \text{Homeo}^-(I) \) the set of the order reversing ones. Then \( \text{Homeo}^+(I) \) is a clopen subgroup of \( \text{Homeo}(I) \) of index 2 whose other coset is \( \text{Homeo}^-(I) \).
We will show that $\text{Homeo}(I)^{(2)} = \text{Homeo}^+(I)$, and therefore the set of squares is clopen. It is clear that the squares preserve the order. The rest of this section is devoted to proving the converse: every order preserving homeomorphism is a square.

This result is probably folklore; it is mentioned without proof in [6]. We present here our own proof in detail because the ideas and notation will be used in the more involved arguments of the next section.

For $J$, a closed and bounded interval in $\mathbb{R}$, let $\text{Homeo}(J)$ and $\text{Homeo}^+(J)$ denote the homeomorphisms and the order preserving homeomorphisms of $J$, respectively. Further, let

\[
K(J) = \{ f \in \text{Homeo}^+(J) | \forall x \in J^0, f(x) > x \},
\]

\[
L(J) = \{ f \in \text{Homeo}^+(J) | \forall x \in J^0, f(x) < x \}.
\]

**Lemma 47.** (a) For all $f \in K(J)$, there exists $g \in K(J)$ such that $f = g^2$.

(b) Similarly, for all $f \in L(J)$, there exists $g \in L(J)$ such that $f = g^2$.

**Proof.** Without loss of generality assume $J = I$. We give a proof of the part (a); the proof of the part (b) is analogous.

Define for each $n \in \mathbb{Z}$ and each $r \in [0,1)$ points $a_{n,r}$ in $(0,1)$ as follows (see Figure 1):

\[
a_{0,0} := \frac{1}{2},
\]

\[
a_{n,0} := f^n(a_{0,0}),
\]

\[
a_{0,r} := a_{0,0} + r(a_{1,0} - a_{0,0}),
\]

\[
a_{n,r} := f^n(a_{0,r}).
\]

Then:

(i) $0 < \cdots < a_{-1,0} < a_{0,0} < a_{1,0} < a_{2,0} < \cdots < 1$,

(ii) $a_{n,0} \to 0$ as $n \to -\infty$ and $a_{n,0} \to 1$ as $n \to \infty$,

(iii) $a_{n,r} < a_{m,s}$ if and only if $n + r < m + s$,

(iv) For all $x \in (0,1)$, there are $n \in \mathbb{Z}$ and $r \in [0,1)$ such that $x = a_{n,r}$.
The first claim follows by induction from the fact that \( a_{0,0} < f(a_{0,0}) = a_{1,0} \) (since \( f \in K(I) \)). For part (ii), let \( a = \lim_{n \to \infty} a_{n,0} \in (\frac{1}{2}, 1] \). Then \( f(a) = \lim_{n \to \infty} f(a_{n,0}) = \lim_{n \to \infty} a_{n+1,0} = a \). Since \( \forall x \in (0,1), f(x) \neq x \), it follows that \( a = 1 \). Similarly, \( \lim_{n \to -\infty} a_{n,0} = 0 \). To see (iii), notice that for \( r < s \), \( a_{0,0} < a_{0,r} < a_{0,s} < a_{1,0} \), and since \( f \) is order preserving, \( a_{n,0} < a_{n,r} < a_{n,s} < a_{n+1,0} \). Using this fact and (i) we see: if \( n < m \), then \( a_{n,r} < a_{n+1,0} \leq a_{m,0} \leq a_{m,s}, \) and if \( n = m \) and \( r < s \), then \( a_{n,r} < a_{n,s} = a_{m,s} \). Similarly, if \( n > m \) or \( n = m, r > s \) then \( a_{n,r} > a_{m,s} \). For claim (iv), suppose \( x \in (0,1) \). Then (i) and (ii) imply that there is an \( n \) such that \( x \in [a_{n,0}, a_{n+1,0}] \). Then \( f^{-n}(x) \in [a_{0,0}, a_{1,0}] \). We can of course find \( r \) such that \( f^{-n}(x) = a_{0,r} \), and so \( x = a_{n,r} \).

We claim that the unique disjoint cycle decomposition of \( f \) is

\[
\prod_{r \in [0,1)} (\cdot \cdot \cdot a_{-1,r} \; a_{0,r} \; a_{1,r} \; a_{2,r} \; \cdot \cdot \cdot).
\]
It is clear that $f$ and this formal composition agree on the set $\{a_{n,r} \mid n \in \mathbb{Z}, r \in [0, 1)\}$. But, by (iv), $\{a_{n,r} \mid n \in \mathbb{Z}, r \in [0, 1)\} = (0, 1)$.

Let $g$ be the permutation of $I$ given by the following disjoint cycle decomposition:

$$g := \prod_{r \in [0, \frac{1}{2})} (\cdots a_{-1,r} \ a_{-1,r+\frac{1}{2}} \ a_{0,r} \ a_{0,r+\frac{1}{2}} \ a_{1,r} \ a_{1,r+\frac{1}{2}} \ \cdots).$$

It is immediate that $f = g^2$. That $g$ is order preserving follows from (iii). Further, $g$ is continuous because the preimages of the open intervals in $I$ are open intervals in $I$, by the fact that $g$ is a bijection that preserves the order. For each $x \in (0, 1)$, $g(x) > x$, by (iv) and (iii). So $g \in K(I)$.

**Proposition 48.** For every $f \in \text{Homeo}^+(I)$, there exists $g \in \text{Homeo}^+(I)$ such that $f = g^2$.

**Proof.** Given $f \in \text{Homeo}^+(I)$, let $\{I_\lambda\}$ be the set of all maximal subintervals of $I$ on which the function $f(x) - x$ does not change sign. Let $I_\lambda$ be the closure of $I_\lambda$: $I_\lambda = \overline{I_\lambda}$. Then by Lemma 47, for each $\lambda$ there exists $g_\lambda \in \text{Homeo}(I_\lambda)$ such that $f|I_\lambda = g_\lambda^2$. Define $g : I \to I$ by

$$g(x) = \begin{cases} g_\lambda(x), & \text{if } x \in I_\lambda, \\ x, & \text{if } x \text{ is such that } f(x) = x. \end{cases}$$

It is clear that $g \in \text{Homeo}^+(I)$ and $f = g^2$. □

As discussed at the beginning of this section, we have proved the following:

**Theorem 49.** The set $\text{Homeo}(I)^{(2)}$ of the squares in $\text{Homeo}(I)$ is Borel.

### 5.4 AUTOHOMEOHOMOMORPHISM GROUP OF THE UNIT CIRCLE

Let $\text{Homeo}(S^1)$ be the group of the autohomeomorphisms of the unit circle $S^1$. Equipped with the topology of the supremum metric, it is a Polish group. In this section we investigate the complexity of the set

$$\text{Homeo}(S^1)^{(2)} = \{f^2 = f \circ f \mid f \in \text{Homeo}(S^1)\}$$
of the squares in \( \text{Homeo}(S^1) \).

We have seen in Section 5.3 that the set of squares in the autohomeomorphism group \( \text{Homeo}(I) \) of the unit interval, is Borel, and, indeed, it is of low Borel complexity. Remarkably, we will see that if the endpoints of the unit interval are identified to form the circle, \( S^1 \), then the set of squares in its autohomeomorphism group \( \text{Homeo}(S^1) \) is (analytic but) not Borel. In fact, it is complete analytic.

The result that the squares in \( \text{Homeo}(I) \) are Borel is in contrast to the situation in the space \( C(I, I) \) of all continuous maps from the unit interval into itself. By studying the properties of the set of points where a function is locally constant, Humke & Laczkovich showed in [9] that the squares in \( C(I, I) \) are (analytic but) not Borel. Later Beleznay improved this result by showing that the squares are complete analytic [2]. Of course, autohomeomorphisms are nowhere locally constant. Instead, in proving that the squares in \( \text{Homeo}(S^1) \) are complete analytic, we focus on the structure of the set of fixed points.

![Figure 2: Showing completeness of an analytic set.](image)

A standard technique for showing completeness of an analytic set is to reduce an already known complete analytic set to the given set. Beleznay in [2] showed that the set \( \text{LO}2 \) of linear orders of type \( I + I \) (precise definition follows) is complete analytic. To show that \( \text{Homeo}(S^1)^{(2)} \) is complete, we construct in Lemma 52 a continuous reduction \( F \) of \( \text{LO}2 \) to \( \text{Homeo}(S^1)^{(2)} \). Since \( \text{LO}2 \) is complete, an arbitrary analytic set \( A \) can be reduced to it via a continuous map \( G \). Composing this reduction map \( G \) with \( F \) gives a continuous
reduction of $A$ to $\text{Homeo}(S^1)^{(2)}$. This proves that $\text{Homeo}(S^1)^{(2)}$ is complete.

We first give in Lemma 51 a necessary and sufficient condition for a homeomorphism of $S^1$ of a certain type to be a square. Then we use this characterization to construct a continuous reduction of $LO_2$ to $\text{Homeo}(S^1)^{(2)}$ in Lemma 52.

5.4.1 Definitions and Notation

First, we give a definition of the set $LO_2$, as given in [2]. Let $\alpha \in 2^{\mathbb{N} \times \mathbb{N}}$ code the relation $R$ on $\mathbb{N}$ the following way: $(n, m) \in R$ if and only if $\alpha(n, m) = 1$. Then $LO_2$ is defined to be the set of those codes $\alpha \in 2^{\mathbb{N} \times \mathbb{N}}$ that code a linear order. $LO_2$ is a $G_\delta$ subset of the Polish space $2^{\mathbb{N} \times \mathbb{N}}$, and thus a Polish space itself. For codes $\alpha$ from $LO_2$, we write $n <_\alpha m$ instead of $\alpha(n, m) = 1$. The set $LO_2$ is the collection of codes from $LO_2$ which code a linear order of the form $I + I$:

$$LO_2 = \{\alpha \in LO \mid \exists f \in 2^{\mathbb{N}}, g \in \mathbb{N}^{\mathbb{N}} \text{ such that } g : \mathbb{N} \to \mathbb{N} \text{ is a bijection, and}$$

$$\forall n, m \in \mathbb{N}, \ f(n) = 0 \text{ and } f(m) = 1 \text{ imply } n <_\alpha m,$$

$$\forall n \in \mathbb{N}, \ f(n) = 0 \text{ if and only if } f(g(n)) = 1,$$

$$\forall n \in \mathbb{N}, \ g(g(n)) = n,$$

$$\forall n, m \in \mathbb{N}, \text{ if } f(n) = f(m) = 0 \text{ then } n <_\alpha m \text{ iff } g(n) <_\alpha g(m)\}. \]$$

In other words, $f$ determines two classes of $\mathbb{N}$ such that every element of $f^{-1}(\{0\})$ is $\alpha$-less than every element of $f^{-1}(\{1\})$, and $g$ gives an $\alpha$-order preserving bijection of these two classes. As mentioned previously, $LO_2$ is a complete analytic set.

While we visualize the topological space $S^1$ as the unit circle, formally, we consider $S^1$ to be the quotient space obtained from the unit interval $I$ by identifying its endpoints 0 and 1. For distinct points $x_1, x_2, \ldots, x_n$ ($n \geq 3$) in $S^1$, we write $x_1 < x_2 < \cdots < x_n$ $(< x_1)$ if, when traveling anticlockwise along the circle $S^1$ starting from $x_1$, we reach points $x_2, x_3, \ldots, x_n$ in that order (before reaching $x_1$ again). For $x, y \in S^1$ we define the open interval $(x, y) = \{z \mid x < z < y\}$. In the obvious way we also define ‘$\leq$’ and the closed and semi-closed intervals in $S^1$. 

50
Let $\text{Homeo}^+(S^1)$ denote the set of order preserving homeomorphisms of $S^1$:

$$\text{Homeo}^+(S^1) = \{ f \in \text{Homeo}(S^1) \mid \forall x, y, z \in S^1, \ x < y < z \Rightarrow f(x) < f(y) < f(z) \}.$$ 

Similarly, let $\text{Homeo}^-(S^1)$ be the collection of the order reversing homeomorphisms of $S^1$. Clearly, $\text{Homeo}^+(S^1)$ is a subgroup of $\text{Homeo}(S^1)$ of index 2, with $\text{Homeo}^-(S^1)$ as its other coset.

For $f \in \text{Homeo}^+(S^1)$ and $a, b \in S^1$ define $D(f|\lbrack a, b \rbrack)$ to be the set of those points in $[a, b]$ that are not fixed by $f \circ f$:

$$D(f|\lbrack a, b \rbrack) = \{ x \in [a, b] \mid f^2(x) \neq x \}.$$ 

Finally, we define a collection $\mathcal{M}$ of a special kind of homeomorphisms of $S^1$:

$$\mathcal{M} = \{ f \in \text{Homeo}^+(S^1) \mid f(0) = \frac{1}{2}, f\left(\frac{1}{2}\right) = 1 = 0, \forall x \in (0, \frac{1}{2}), \ 0 < x \leq f^2(x) < \frac{1}{2} \text{ and } \forall x \in \left(\frac{1}{2}, 1\right), \ \frac{1}{2} < x \leq f^2(x) < 1 \}.$$ 

The last two conditions can be rewritten as

$$\forall x \in (0, \frac{1}{2}), \ \frac{1}{2} < f^{-1}(x) \leq f(x) < 1 \text{ and } \forall x \in \left(\frac{1}{2}, 1\right), \ 0 < f^{-1}(x) \leq f(x) < \frac{1}{2}.$$ 

A typical function in $\mathcal{M}$, together with its inverse, is shown in Figure 3.
5.4.2 The Proof

**Lemma 50.** Let \( f \in \mathcal{M} \). Suppose \( 0 < a < a' < c < c' < \frac{1}{2} < b < b' < d < d' < 1 \) are points in \( S^1 \) such that \( f \) contains

\[(a \ b)(c \ d)(a' \ b')(c' \ d')\]

in its disjoint cycle representation and for all \( x \in (a, a') \cup (c, c') \cup (b, b') \cup (d, d') \), \( f^2(x) \neq x \).

Let \( A = [a, a'] \cup [c, c'] \cup [b, b'] \cup [d, d'] \). Then there exists an order preserving homeomorphism \( g \) of \( A \) such that \( g \) contains

\[(a \ c \ b \ d')(a' \ c' \ b' \ d')\]

and \( f|A = g^2 \).
Proof. Fix an arbitrary point \( a_{0,0} \in (a, a') \) and for \( n \in \mathbb{Z} \), let

\[
a_{n,0} := f^{2n}(a_{0,0}) \in (a, a'),
\]
\[
b_{n,0} := f^{2n+1}(a_{0,0}) \in (b, b').
\]

For \( r \in (0, 1) \) and \( n \in \mathbb{Z} \) let

\[
a_{0,r} := a_{0,0} + r(a_{1,0} - a_{0,0}),
\]
\[
a_{n,r} := f^{2n}(a_{0,r}) \in (a, a'),
\]
\[
b_{n,r} := f^{2n+1}(a_{0,r}) \in (b, b').
\]

Starting with an arbitrary point \( c_{0,0} \) in \((c, c')\), construct analogous sequences \((c_{n,r})\) and \((d_{n,r})\) in \((c, c')\) and \((d, d')\) respectively. Then the following are true for the sequence \((a_{n,r})\):

(i) \( a < \cdots < a_{-1,0} < a_{0,0} < a_{1,0} < a_{2,0} < \cdots < a' \),

(ii) \( a_{n,0} \to a \) as \( n \to -\infty \) and \( a_{n,0} \to a' \) as \( n \to \infty \),

(iii) \( a < a_{n,r} < a_{m,s} < a' \) if and only if \( n + r < m + s \),

(iv) For all \( x \in (a, a') \), there are \( n \in \mathbb{Z} \) and \( r \in [0, 1) \) such that \( x = a_{n,r} \).
and analogous statements hold for the sequences \((b_{n,r}), (c_{n,r})\) and \((d_{n,r})\). We omit the proof as it is similar to the proof of Lemma 47. Note that in (i) we use the assumption that \(f \in \mathcal{M}\) (see Figure 4).

The disjoint cycle decomposition of \(f\restriction A\) is then

\[
(a \ b)(c \ d)(a' \ b')(c' \ d') \cdot \prod_{r \in \{0,1\}} (\cdots a_{0,r} \ b_{0,r} \ a_{1,r} \ b_{1,r} \cdots)(\cdots c_{0,r} \ d_{0,r} \ c_{1,r} \ d_{1,r} \cdots).
\]

It is clear from the construction that every cycle in this composition is a cycle of \(f\restriction A\). But (iv) implies that also, every cycle of \(f\restriction A\) is included in this representation.

![Figure 5: A square root of \(f\restriction A\).](image_url)
Define $g$ to be the permutation of $A$ given by the following disjoint cycle representation:

$$g := (a \ c \ b \ d)(a' \ c' \ b' \ d') \cdot \prod_{r \in [0,1)} (\cdots \cdot a_{0,r} \ c_{0,r} \ b_{0,r} \ d_{0,r} \ a_{1,r} \ c_{1,r} \ b_{1,r} \ d_{1,r} \cdots).$$

Then clearly $g^2 = f | A$. That $g$ is order preserving follows from (iii). The inverse images under $g$ of the open intervals in $S^1$ are open intervals because $g$ is an order preserving bijection. Thus $g$ is continuous. □

**Lemma 51** (Characterization of Squares in $\mathcal{M}$). For a homeomorphism $f \in \mathcal{M}$, the following are equivalent:

(i) $f \in \text{Homeo}(S^1)^{(2)}$,

(ii) There exist $c \in (0, \frac{1}{2})$ and an order preserving homeomorphism $\phi : [0, c) \to [c, \frac{1}{2})$ such that

$$\phi(D(f| [0, c))) = D(f| [c, \frac{1}{2}]).$$

**Proof.** Suppose that $f \in \text{Homeo}(S^1)^{(2)}$ and let $g \in \text{Homeo}(S^1)$ be such that $f = g^2$. Note that $g(0) \neq 0$, otherwise $f(0) = g^2(0) = 0$. Also, $g(0) \neq \frac{1}{2}$, for otherwise $f(\frac{1}{2}) = f(g(0)) = g^3(0) = g(f(0)) = g(\frac{1}{2}) = g(g(0)) = f(0) = \frac{1}{2}$. We claim that $g \in \text{Homeo}^+(S^1)$. Suppose, for a contradiction, $g \in \text{Homeo}^-(S^1)$. If $0 < g(0) < \frac{1}{2} < 0$, then applying $g$ to each of these points, the order of their images reverses, i.e. $g(0) > \frac{1}{2} > g(\frac{1}{2}) > g(0)$. In particular, $g(\frac{1}{2}) \in (0, \frac{1}{2})$. Now applying $g$ again, we find $\frac{1}{2} < g(\frac{1}{2}) < 0 < \frac{1}{2}$. However, this gives $g(\frac{1}{2}) \in (\frac{1}{2}, 1)$ — a contradiction! Case $0 < \frac{1}{2} < g(0) < 0$ yields a contradiction in a similar way. So $g$ indeed must be order preserving. Now, either $g(0) \in (0, \frac{1}{2})$ or $g^{-1}(0) \in (0, \frac{1}{2})$. In case $g(0) \in (0, \frac{1}{2})$, let $c = g(0)$ and let $\phi = g| [0, c]$. 55
Then \( \phi \) is an order preserving homeomorphism of \([0, c]\) with \([c, \frac{1}{2}]\) and for \( x \in [c, \frac{1}{2}] \) we have

\[
\begin{align*}
x \in \phi(D(f| [0, c])) & \iff g^{-1}(x) \in D(f| [0, c]) \\
& \iff f^2(g^{-1}(x)) \neq g^{-1}(x) \\
& \iff g^3(x) \neq g^{-1}(x) \\
& \iff g^4(x) \neq x \\
& \iff f^2(x) \neq x \\
& \iff x \in D(f| [c, \frac{1}{2}])
\end{align*}
\]

so \( \phi(D(f| [0, c])) = D(f| [c, \frac{1}{2}]) \). In case \( g^{-1}(0) \in (0, \frac{1}{2}) \), the proof is similar, only with \( c = g^{-1}(0) \) and \( \phi = g^{-1}|[0, c] \).

Conversely, suppose that (ii) holds. Let \( K = \{ x \in [0, c] \mid f^2(x) = x \} \). Note that \( 0, c \in K \). Define \( g_K \) on \( K' = K \cup \phi(K) \cup f(K) \cup f(\phi(K)) \) by the following disjoint cycle representation:

\[
\prod_{x \in K} (x \ \phi(x) \ f(x) \ f(\phi(x))).
\]

Then \( g_K \) is an order preserving homeomorphism of \( K' \) and \( g_K^2 = f|K' \). Set \( D(f| [0, c]) \) consists of disjoint open intervals. Let \( L \) be a component of \( D(f| [0, c]) \). Let \( g_L \) be the order preserving homeomorphism of \( L' = L \cup \phi(L) \cup f(L) \cup f(\phi(L)) \) such that \( f|L' = g_L^2 \), constructed in Lemma 50. Define

\[
g = g_K \cup \bigcup \{ g_L \mid L \text{ is a component of } D(f| [0, c]) \}.
\]

It is not hard to check that then \( g \) is a well defined order preserving homeomorphism of \( S^1 \) with \( f = g^2 \).

**Lemma 52.** There is a continuous function \( F : LO \to M \) such that

\[
F(\alpha) \in \text{Homeo}(S^1)^{(2)} \quad \text{if and only if} \quad \alpha \in LO2.
\]

**Proof. Construction.** Fix \( \alpha \in LO \). We want to define \( F(\alpha) \in M \). We start by constructing a discrete collection of open intervals \( \{(p_n, q_n) \mid n \in \mathbb{N}\} \) with endpoints in \((0, \frac{1}{2})\) and with the following properties:
(a) The order of \( \{ p_n \mid n \in \mathbb{N} \} \) is isomorphic to the order coded by \( \alpha \),

(b) \( \inf \{ p_n \mid n \in \mathbb{N} \} = 0 \) if and only if the order has no smallest element,

(c) \( \sup \{ q_n \mid n \in \mathbb{N} \} = \frac{1}{2} \) if and only if the order has no largest element,

(d) For any \( x \notin \bigcup_{n \in \mathbb{N}} (p_n, q_n) \), \( \sup \{ q_n \mid q_n \leq x \} = \inf \{ p_n \mid p_n \geq x \} \) if and only if there is no biggest \( q_n \) below \( x \) and no smallest \( p_n \) above \( x \),

(e) \( |q_n - p_n| < \frac{1}{n} \).

To do this, we follow the construction of Beleznay in [2]. Let \( \mathcal{O} = \{ (a_m, b_m) \mid m \in \mathbb{N} \} \) be an enumeration of the rational open subintervals with endpoints in \((0, \frac{1}{2})\). Choose a pairwise disjoint subsystem of \( \mathcal{O} \) as follows. Let \( (s_1, t_1) = (a_1, b_1) \), \( t_0 = 0 \) and \( s_0 = \frac{1}{2} \). Assume that we have already chosen \( (s_k, t_k) \) for \( k = 1, 2, \ldots, n - 1 \) such that if \( k < \alpha \) then \( t_k < s_i \) (i.e. \( (s_k, t_k) \) precedes \( (s_i, t_i) \)). Let \( i \) be the \( \alpha \)-biggest among \( 1, 2, \ldots, n - 1 \) that is \( \alpha \)-less than \( n \), if such \( i \) exists. Otherwise let \( i = 0 \). Let \( j \) be the \( \alpha \)-smallest among \( 1, 2, \ldots, n - 1 \) that is \( \alpha \)-bigger than \( n \), and if no such \( j \) exists, let \( j = 0 \). By the choice of \( s_k, t_k \) for \( k = 0, 1, \ldots, n - 1 \), \( t_i < s_j \). Let \( (s_n, t_n) \) be the first \( (a_m, b_m) \) such that it is

(i) strictly inside \( (t_i, s_j) \),

(ii) contains \( \frac{t_i + s_j}{2} \), and

(iii) \( |b_m - a_m| < \frac{1}{n} \).

For an example of the first few steps of this construction, see Figure 6.

![Figure 6: Intervals \((s_n, t_n)\) for \( n = 0, 1, \ldots, 4 \), when \( 2 <_\alpha 3 <_\alpha 1 <_\alpha 4 \).](image)

It is clear that this process can be continued and yields a pairwise disjoint system of intervals \( \{ (s_n, t_n) \mid n \in \mathbb{N} \} \) such that the order of \( \{ s_n \mid n \in \mathbb{N} \} \) is isomorphic to the order coded by \( \alpha \). We now let \( (p_n, q_n) \) be the middle third of the interval \( (s_n, t_n) \). The collection \( \{ (p_n, q_n) \mid n \in \mathbb{N} \} \) constructed this way has all of the aforementioned properties: (b),(c),(d) are ensured by (ii), and (e) is implied by (iii).
Let \( U = \bigcup_{n \in \mathbb{N}} (p_n, q_n) \). We now define \( F(\alpha) \) as follows: for \( x \in S^1 = [0, 1]/\sim, \)

\[
F(\alpha)(x) = \begin{cases} 
\frac{1}{2} + x, & \text{if } x \in [0, \frac{1}{2}) \setminus U, \\
\frac{1}{2} + x + \frac{q_n - p_n}{\pi} \sin(\frac{\pi}{q_n - p_n} (x - p_n)), & \text{if } x \in (p_n, q_n), \\
-\frac{1}{2} + x, & \text{if } x \in [\frac{1}{2}, 1) \setminus (\frac{1}{2} + U), \\
-\frac{1}{2} + x + \frac{q_n - p_n}{\pi} \sin(\frac{\pi}{q_n - p_n} (x - \frac{1}{2} - p_n)), & \text{if } x \in \frac{1}{2} + (p_n, q_n).
\end{cases}
\]

If we visualize \( S^1 \) as the unit circle, then \( F(\alpha) \) acts on the points outside \( U \) and \( \frac{1}{2} + U \) as the rotation by \( \pi \), while each point in \( U \) and \( \frac{1}{2} + U \) is rotated by ‘a little over’ \( \pi \). More precisely, a point \( x \) in \( (p_n, q_n) \) is taken to a point in \( \frac{1}{2} + (p_n, q_n) \), between its diametrically opposite point \( \frac{1}{2} + x \) and \( \frac{1}{2} + q_n \), and points in \( \frac{1}{2} + (p_n, q_n) \) are mapped similarly. See Figure 7. One readily verifies that \( F(\alpha) \in \mathcal{M} \).

**Continuity.** We show that \( F : LO \to \mathcal{M} \) is continuous. For \( \alpha \in LO \), let \( \{(p_n^\alpha, q_n^\alpha) \mid n \in \mathbb{N}\} \) denote the discrete collection of open intervals constructed from \( \alpha \). Fix \( \alpha \in LO \). We show that \( F \) is continuous at \( \alpha \). Specifically, we prove that for all \( \varepsilon > 0 \), there is an open neighborhood \( N_\alpha \) of \( \alpha \) such that for all \( \beta \in N_\alpha \), \( d(F(\alpha), F(\beta)) < \varepsilon \).

Fix \( \varepsilon > 0 \) and let \( n_\varepsilon = \lceil \frac{1}{\varepsilon} \rceil \). Then, by (e), for all \( \beta \in LO \), \( n \geq n_\varepsilon \Rightarrow |q_n^\beta - p_n^\beta| < \varepsilon \). Let

\[
N_\alpha = \{ \beta \in LO \mid \beta \text{ and } \alpha \text{ agree on the order of } 1, 2, \ldots, n_\varepsilon - 1 \}.
\]

This is a basic open neighborhood of \( \alpha \). If \( \beta \in N_\alpha \), then the intervals \( (p_n^\alpha, q_n^\alpha) \) and \( (p_n^\beta, q_n^\beta) \) coincide for \( n < n_\varepsilon \), so \( F(\alpha) \) and \( F(\beta) \) may differ only on the set

\[
A = \bigcup_{n \geq n_\varepsilon} (p_n^\alpha, q_n^\alpha) \cup \bigcup_{n \geq n_\varepsilon} (p_n^\beta, q_n^\beta).
\]

Thus,

\[
d(F(\alpha), F(\beta)) = \sup \{|F(\alpha)(x) - F(\beta)(x)| \mid x \in S^1\}
= \sup \{|F(\alpha)(x) - F(\beta)(x)| \mid x \in A\}.
\]
If \( x \in A \), then \( x \in (p_n^\alpha, q_n^\alpha) \) for some \( n \geq n_\sigma \) or \( x \in (p_m^\beta, q_m^\beta) \) for some \( m \geq \varepsilon \), or both. If \( x \) belongs to \((p_n^\alpha, q_n^\alpha)\) and no other component of \( A \), then

\[
|F(\alpha)(x) - F(\beta)(x)| \leq |q_n^\alpha - p_n^\alpha| < \varepsilon.
\]

Similarly, if \( x \) belongs to \((p_m^\beta, q_m^\beta)\) only, then

\[
|F(\alpha)(x) - F(\beta)(x)| \leq |q_m^\beta - p_m^\beta| < \varepsilon.
\]

Finally, if \( x \in (p_n^\alpha, q_n^\alpha) \cap (p_m^\beta, q_m^\beta) \), then

\[
|F(\alpha)(x) - F(\beta)(x)| \leq \max(|q_n^\alpha - p_n^\alpha|, |q_m^\beta - p_m^\beta|) < \varepsilon.
\]

Thus, \( d(F(\alpha), F(\beta)) < \varepsilon \). This proves the continuity of \( F \).
To be square is to be even. We now turn to proving $F(\alpha) \in \text{Homeo}(S^1)^{(2)} \iff \alpha \in LO2$.

Suppose $F(\alpha) \in \text{Homeo}(S^1)^{(2)}$. Then by Lemma 51, there exist $c \in (0, \frac{1}{2})$ and an order preserving homeomorphism $\phi : [0, c] \to [c, \frac{1}{2}]$ such that

$$\phi(D(F(\alpha)[[0, c]]) = D(F(\alpha)[[c, \frac{1}{2}]]).$$

Then $c \notin U$. For, otherwise, $c \in D(F(\alpha)[[0, c]])$, and so $\phi(c) \in D(F(\alpha)[[c, \frac{1}{2}]])$, which further implies that $\phi(c) \in U \cup (\frac{1}{2} + U)$. But, $\phi(c) = \frac{1}{2} \notin U \cup (\frac{1}{2} + U)$.

Since $D(F(\alpha)[[0, \frac{1}{2}]] = U$, we find that

$$\phi \left( \bigcup_{p_n \in (0, c)} (p_n, q_n) \right) = \bigcup_{p_n \in (c, \frac{1}{2})} (p_n, q_n).$$

Since $\phi$ is a homeomorphism, if $p_n \in (0, c)$, then $\phi((p_n, q_n))$ is equal to $(p_m, q_m)$ for some $m$ with $p_m \in (c, \frac{1}{2})$. This further means that for $p_n \in (0, c), \phi(p_n) = p_m$ for some $p_m \in (c, \frac{1}{2})$.

Let $J = \{ n \mid p_n \in (0, c) \}$ and $K = \{ n \mid p_n \in (c, \frac{1}{2}) \}$. Then, in $(0, \frac{1}{2})$, every element of $J$ precedes every element of $K$ and $\tau : J \to K$ defined by

$$\tau(n) \text{ is the unique } m \text{ such that } \phi(p_n) = p_m$$

is an order preserving bijection between $J$ and $K$. Thus, the order of $\{ p_n \mid n \in \mathbb{N} \}$ is of the form $I + I$. Since this order is isomorphic to the order coded by $\alpha$, we find $\alpha \in LO2$.

Conversely, suppose $\alpha \in LO2$. According to Lemma 51, we need to find $c \in (0, \frac{1}{2})$ and an order preserving homeomorphism $\phi : [0, c] \to [c, \frac{1}{2}]$ with the property $\phi(D(F(\alpha)[[0, c]]) = D(F(\alpha)[[c, \frac{1}{2}]]).$

Write $\mathbb{N}$ as the disjoint union of sets $J$ and $K$ such that each element of $J$ is $\alpha$-less than each element of $K$ and there is an $\alpha$-order preserving bijection $\tau : J \leftrightarrow K$. Let $c_1 = \sup\{ q_n \mid n \in J \}$ and $c_2 = \inf\{ p_n \mid n \in K \}$. If $J$ has no biggest element, let $c = c_1$. If $K$ has no smallest element, let $c = c_2$. (This definition of $c$ is not ambiguous, since in the case that both $J$ has no biggest element and $K$ has no smallest element, $c_1 = c_2$ by (d)). Otherwise, let $c = \frac{c_1 + c_2}{2}$. Notice that if $J$ has a biggest element, then $c_1 < c$ and if $K$ has a smallest element then $c < c_2$.  

60
Define \( \phi(p_n) = p_{\tau(n)} \) and \( \phi(q_n) = q_{\tau(n)} \). Then \( \phi \) is strictly order preserving on the set \( S = \{ p_n, q_n \mid n \in J \} \).

Extend \( \phi \) to the closure of \( S \) as follows. First note that if \( x \in \overline{S} \), then either \( x = \sup \{ q_n \mid q_n \leq x \} \) or \( x = \inf \{ p_n \mid p_n \geq x \} \) (or both). In case \( x = \sup \{ q_n \mid q_n \leq x \} \), define \( \phi(x) = \sup \{ q_{\tau(n)} \mid q_n \leq x \} \). In case \( x = \inf \{ p_n \mid p_n \geq x \} \), define \( \phi(x) = \inf \{ p_{\tau(n)} \mid p_n \geq x \} \). This is well defined (non-ambiguous): Suppose \( x = \sup \{ q_n \mid q_n \leq x \} = \inf \{ p_n \mid p_n \geq x \} \). We need to show that \( y := \sup \{ q_{\tau(n)} \mid q_n \leq x \} \) and \( z := \inf \{ p_{\tau(n)} \mid p_n \geq x \} \) are equal. Clearly \( y \leq z \), and if \( y < z \), there can be no intervals \((p_n, q_n)\) between \( y \) and \( z \). Thus, \( y = \sup \{ q_m \mid q_m \leq y \} = \sup \{ q_m \mid q_m \leq z \} \) and \( z = \inf \{ p_m \mid p_m \geq z \} \). By the property (d), there is no biggest \( q_n \) below \( x \) and there is no smallest \( p_n \) above \( x \). Since \( \tau \) is an order preserving bijection, it follows that there is no biggest \( q_m \) below \( y \), and thus no biggest \( q_m \) below \( z \), and also, there is no smallest \( p_m \) above \( z \). This, by (d) again, implies \( \sup \{ q_m \mid q_m \leq z \} = \inf \{ p_m \mid p_m \geq z \} \), i.e. \( y = z \). Clearly \( \phi \) is continuous and order preserving on \( \overline{S} \).

Note that

\[
\inf S = 0 \iff J \text{ has no smallest element (by (b))}

\iff K \text{ has no smallest element}

\iff \inf \tau(S) = c \text{ (by the definition of } c \text{).}
\]

and

\[
\sup S = c \iff J \text{ has no biggest element (definition of } c \text{)}

\iff K \text{ has no biggest element}

\iff \inf \tau(S) = \frac{1}{2} \text{ (by (c)).}
\]

Next we define \( \phi(0) = c \) and \( \phi(c) = \frac{1}{2} \). By the above remarks, \( \phi \) is well defined (i.e. if \( \phi \) has already been defined at 0 and/or \( c \), this new definition agrees with the previous one) and \( \phi \) is order preserving and continuous on \( \overline{S} \cup \{0, c\} \).

The complement of \( \overline{S} \cup \{0, c\} \) in \([0, c]\) is a disjoint union of open intervals. We define \( \phi \) to be linear on each of these components and continuous on \([0, c]\).
By construction, $\phi$ is an order preserving homeomorphism between $[0,c]$ and $[c, \frac{1}{2}]$, and

$$\phi(D(F(\alpha) \mid [0,c])) = \phi(\bigcup_{n \in J} (p_n, q_n)) = \bigcup_{m \in K} (p_m, q_m) = D(F(\alpha) \mid [c, \frac{1}{2}]).$$

\[\square\]

**Theorem 53.** The set of squares $\text{Homeo}(S^1)^{(2)}$ in $\text{Homeo}(S^1)$ is complete analytic.

**Proof.** The set $\text{Homeo}(S^1)^{(2)}$ is obviously analytic, since $f \mapsto f \circ f$ is continuous. Lemma 52 gives a continuous reduction of $LO2$, a complete analytic set, to $\text{Homeo}(S^1)^{(2)}$. By the discussion from the beginning of this section, $\text{Homeo}(S^1)^{(2)}$ is complete. \[\square\]

### 5.5 Automorphism Group of the Rational Circle

In Section 5.2, we saw that the full verbal sets in $S_\infty$ are Borel. An important class of Polish groups are the automorphism groups of countable first order structures, which are all closed subgroups of $S_\infty$. It is a natural question to ask if in these Polish groups, the full verbal sets are also necessarily Borel. The answer turns out to be negative: we exhibit here an automorphism group of a countable first order structure in which the set of squares is complete analytic.

Recall that $S^1$ denotes the quotient space obtained by identifying the endpoints of the unit interval $I$. Of course, $S^1$ is homeomorphic to the unit circle via the map $t \mapsto e^{2\pi it}$. We define a three place relation `$<$' on $S^1$ by: $x < y < z$ if and only if, when starting from $x$ and moving along the circle in the anticlockwise direction, we first arrive at $y$, and then at $z$ (before returning to $x$). We define the *rational circle* $Q$ to be the subset of $S^1$ consisting of the rational points, equipped with the relation $<$ restricted to $Q$. Consider the group of automorphisms of the countable first order structure $(Q, <)$:

$$\text{Aut}(Q, <) = \{ \pi \in \text{Sym}(Q) \mid \forall x, y, z \in Q, \ x < y < z \Rightarrow \pi(x) < \pi(y) < \pi(z) \}.$$
We give $\text{Aut}(Q, <)$ the relative topology as a subspace of the group $\text{Sym}(Q)$ of permutations of $Q$ (which is homeomorphic to $S_\infty$). $\text{Aut}(Q, <)$ is then a closed subgroup of the Polish group $S_\infty$, and thus a Polish group itself.

We show below that $\text{Aut}(Q, <)$ naturally embeds as an abstract subgroup into the Polish group $\text{Homeo}(S^1)$. Thus, another natural way to topologize $\text{Aut}(Q, <)$ would be to give it the topology as a subset of $\text{Homeo}(S^1)$. However, we will see that this topology is not Polish.

The fact that $\text{Aut}(Q, <)$ embeds as a subgroup into $\text{Homeo}(S^1)$ is nevertheless useful to us as we consider the question of the complexity of the set of squares in $\text{Aut}(Q, <)$. The proof that $\text{Homeo}(S^1)^{(2)}$ is complete analytic relies a great deal on the ordering on the circle $S^1$. Here, we will extend the ideas of Section 5.4 to prove that $\text{Aut}(Q, <)^{(2)}$ is also complete analytic.

Let $\pi \in \text{Aut}(Q, <)$. We define an extension $\hat{\pi}$ of $\pi$ to $S^1$ as follows. For $x \in S^1$, write $\{x\} = \bigcap_{n=0}^{\infty} [p_n, q_n]$, for some $p_n, q_n \in Q$ with $p_0 < p_1 < \cdots < x < \cdots < q_1 < q_0$. Then $\pi(p_0) < \pi(p_1) < \cdots < \pi(q_1) < \pi(q_0)$. Define $\hat{\pi}(x)$ to be the unique point of the intersection $\bigcap_{n=0}^{\infty} [\pi(p_n), \pi(q_n)]$. One can show that $\hat{\pi}$ is a well-defined order preserving homeomorphism of $S^1$, and that it extends $\pi$: $\hat{\pi} \in \text{Homeo}^+(S^1)$ and $\hat{\pi} \mid Q = \pi$. Also, if $f \in \text{Homeo}^+(S^1)$ and $f(Q) = Q$, then $f \mid Q \in \text{Aut}(Q, <)$ and $\hat{f} \mid Q = f$.

Define $\psi : \text{Aut}(Q, <) \to \text{Homeo}(S^1)$ by $\psi(\pi) = \hat{\pi}$. One can show that $\psi$ is an abstract group embedding, so $\text{Aut}(Q, <) \cong \psi(\text{Aut}(Q, <))$ is a subgroup of $\text{Homeo}(S^1)$. Observe that $\psi(\text{Aut}(Q, <))$ is a $G_{\delta\sigma}$ subset of $\text{Homeo}(S^1)$, since

$$\psi(\text{Aut}(Q, <)) = \{ f \in \text{Homeo}^+(S^1) \mid f(Q) = Q \} = \{ f \in \text{Homeo}^+(S^1) \mid \forall x \in Q, \exists y \in Q, f(x) = y \text{ and } \forall y \in Q, \exists x \in Q, f(x) = y \}.$$  

Let $\tau$ be the usual Polish group topology on $\text{Aut}(Q, <)$, that is, the relative topology as a subset of $\text{Sym}(Q)$. Let $\tau'$ denote the topology on $\text{Aut}(Q, <)$ inherited from $\text{Homeo}(S^1)$: $\tau' = \{ \psi^{-1}(U) \mid U \text{ is open in } \text{Homeo}(S^1) \}$. We show that the topologies $\tau$ and $\tau'$ are comparable, but not equal. Thus, by Theorem 5, $\tau'$ cannot be Polish. To show that $\tau$ is finer
than \( \tau' \), it is enough to see that every basic open set of \( \tau' \) contains a basic open set of \( \tau \). Consider the basic open set \( U(\pi, \varepsilon) := \{ \sigma \in Aut(Q, <) \mid \sup_{x \in S^1} |\hat{\sigma}(x) - \pi(x)| < \varepsilon \} \) of \( \tau' \), where \( \pi \in Aut(Q, <) \) and \( \varepsilon > 0 \). Let \( n = \lceil \frac{1}{\varepsilon} \rceil + 1 \), so that \( \frac{1}{n} < \varepsilon \). Let \( x_i = \pi^{-1}(\frac{i}{n}) \), for \( i = 1, \ldots, n \). Then \( V(\pi, \{ x_1, \ldots, x_n \}) := \{ \sigma \in Aut(Q, <) \mid \sigma(x_i) = \pi(x_i), i = 1, \ldots, n \} \) is a basic open set of \( \tau \) contained in \( U(\pi, \varepsilon) \). To see that \( \tau \) is strictly finer than \( \tau' \), observe that \( V(id, \{ 0 \}) = \{ \sigma \in Aut(Q, <) \mid \sigma(0) = 0 \} \) is an open set in \( \tau \), but not open in \( \tau' \).

As discussed in Section 5.4, to show completeness of an analytic set, it is sufficient to find a continuous reduction of an already known complete analytic set to the given set. In fact, recall that according to a result by Kechris [16], it is sufficient to find a Borel reduction. To show that \( Aut(Q, <)^{(2)} \) is complete, we construct in Lemma 57 a Borel reduction \( G \) of the complete analytic set \( LO2 \) to \( Aut(Q, <)^{(2)} \). But before constructing this Borel reduction, we will need a characterization of the squares, which we give in Lemma 55.

### 5.5.1 Definitions and Notation

Throughout this section we fix \( A = \sqrt{2} \frac{100}{100} \) and \( B = \frac{1}{2} + \sqrt{2} \frac{100}{100} \) in \( S^1 \). They will play the role of 0 and \( \frac{1}{2} \) from the previous section, but they have an additional quality highly important for this argument to work: they are irrational.

Define

\[
\mathcal{M}(A, B) = \{ f \in Homeo^+(S^1) \mid f(A) = B, f(B) = A, \\
\forall x \in (A, B), \ A < x < f^2(x) < B, \text{ and} \\
\forall x \in (B, A), \ B < x < f^2(x) < A \}.
\]

and

\[
\mathcal{M}_Q(A, B) = \{ \pi \in Aut(Q, <) \mid \hat{\pi}(A) = B, \hat{\pi}(B) = A, \\
\forall x \in (A, B) \cap Q, \ A < x < \pi^2(x) < B, \text{ and} \\
\forall x \in (B, A) \cap Q, \ B < x < \pi^2(x) < A \}.
\]

Note that if \( \pi \in \mathcal{M}_Q(A, B) \), then \( \hat{\pi} \in \mathcal{M}(A, B) \), and if \( f \in \mathcal{M}(A, B) \) with \( f(Q) = Q \), then \( f|Q \in \mathcal{M}_Q(A, B) \).
5.5.2 The Proof

**Lemma 54.** Let \( \pi \in \mathcal{M}_Q(A, B) \). Then \( f := \hat{\pi} \in \mathcal{M}(A, B) \). Suppose \( A < a < a' < c < c' < B < b < b' < d < d' < A \) are points in \( S^1 \) such that \( f \) contains
\[
(ab)(cd)(a'b')(c'd')
\]
in its disjoint cycle representation and for all \( x \in (a, a') \cup (c, c') \cup (b, b') \cup (d, d') \), \( f^2(x) \neq x \).

Let \( S = [a, a'] \cup [c, c'] \cup [b, b'] \cup [d, d'] \). Then there exists an order preserving homeomorphism \( g \) of \( S \) such that \( g(S \cap Q) = S \cap Q \), \( g \) contains
\[
(abc'd')(a'b'c'd')
\]
and \( f|S = g^2 \). Then, \( \sigma := g|S \cap Q \) is an automorphism of \((S \cap Q, <)\) and \( \pi|S \cap Q = \sigma^2 \).

**Proof.** The proof is the same as that of Lemma 50, only with \( A \) and \( B \) in place of 0 and \( \frac{1}{2} \), and with \( a_{0,0} \in (a, a') \cap Q \) and \( r \in [0, 1) \cap Q \). □

**Lemma 55** (Characterization of Squares in \( \mathcal{M}_Q(A, B) \)). For an automorphism \( \pi \in \mathcal{M}_Q(A, B) \), the following are equivalent:

(i) \( \pi \in \text{Aut}(Q, <)^{(2)} \),

(ii) There exist an irrational point \( c \in (A, B) \) and an order preserving homeomorphism \( \phi : [A, c] \rightarrow [c, B] \) such that \( \phi([A, c] \cap Q) = [c, B] \cap Q \), and
\[
\phi(D(\hat{\pi}|[A, c])) = D(\hat{\pi}|[c, B])
\]

**Proof.** Suppose that \( \pi \in \text{Aut}(Q, <)^{(2)} \) and let \( \sigma \in \text{Aut}(Q, <) \) be such that \( \pi = \sigma^2 \). Let \( f = \hat{\pi} \) and \( g = \hat{\sigma} \). Then \( f \in \mathcal{M}(A, B) \) and \( f = g^2 \). As in the proof of Lemma 51, let \( c = g(A) \) and \( \phi = g|[A, c] \) if \( g(A) \in (A, B) \), or, let \( c = g^{-1}(A) \) and \( \phi = g^{-1}|[A, c] \) if \( g^{-1}(A) \in (A, B) \). As before, \( \phi \) is an order preserving homeomorphism of \([A, c]\) with \([c, B]\). But also, \( \phi([A, c] \cap Q) = [c, B] \cap Q \), since \( g(Q) = Q \).

Suppose now (ii) holds. We construct \( g_K, g_L \) and \( g \) as in the proof of Lemma 51, except, we replace 0 and \( \frac{1}{2} \) by \( A \) and \( B \) respectively, and we use Lemma 54 to obtain \( g_L \). Then \( g \) is, as before, a well defined order preserving homeomorphism of \( S^1 \) with \( f = g^2 \). In addition, since both \( g_K \) and \( g_L \) map rational points to rational points, and irrationals to irrationals, \( g(Q) = Q \). Let \( \sigma = g|Q \). Then \( \sigma \in \text{Aut}(Q, <) \) and \( \pi = \sigma^2 \). So \( \pi \in \text{Aut}(Q, <)^{(2)} \). □
Lemma 56. For each linear order $\alpha \in \text{LO}$, there exists a discrete collection of open intervals \{(p_n, q_n) \mid n \in \mathbb{N}\} with rational endpoints in $(A, B)$ satisfying the following properties:

(a) The order of \{p_n \mid n \in \mathbb{N}\} is isomorphic to the order (coded by) $\alpha$,  
(b) $\inf\{p_n \mid n \in \mathbb{N}\} = A$ if and only if the order $\alpha$ has no smallest element,  
(c) $\sup\{q_n \mid n \in \mathbb{N}\} = B$ if and only if the order $\alpha$ has no largest element,  
(d) For any $x \notin \bigcup_{n \in \mathbb{N}}(p_n, q_n)$, $\sup\{q_n \mid q_n \leq x\} = \inf\{p_n \mid p_n \geq x\}$ if and only if there is no biggest $q_n$ below $x$ and no smallest $p_n$ above $x$,  
(e) All accumulation points of \{p_n, q_n \mid n \in \mathbb{N}\}, if there are any, are irrational.

Further, it is possible to assign such a collection of intervals \{(p_n^\alpha, q_n^\alpha) \mid n \in \mathbb{N}\} to each linear order $\alpha \in \text{LO}$ in such a way that if linear orders $\alpha$ and $\beta$ agree on the order of $1, 2, \ldots, N$, then $(p_n^\alpha, q_n^\alpha) = (p_n^\beta, q_n^\beta)$ for $n = 1, \ldots, N$.

Proof. Enumerate the rational numbers in $(A, B)$: $r_1, r_2, r_3, \ldots$ Fix a countable dense subset $P$ of $(A, B)$ consisting of irrational points (e.g. $P = (\mathbb{Q} + \sqrt{2}) \cap (A, B)$). Let $\mathcal{P} = \{I_k \mid k \in \mathbb{N}\}$ be an enumeration of the intervals with endpoints from $P$. Choose a pairwise disjoint subsystem \{(s_n, t_n) \mid n \in \mathbb{N}\} of $\mathcal{P}$ as follows. Let $(s_1, t_1)$ be the first interval in $\mathcal{P}$. Let $t_0 = A, s_0 = B$. Assume we have already chosen $(s_k, t_k)$ for $k = 1, 2, \ldots, n - 1$ such that if $k <_\alpha l$, then $t_k < s_l$ (i.e. $(s_k, t_k)$ precedes $(s_l, t_l)$). Let $i$ be the $\alpha$-biggest among $1, 2, \ldots, n - 1$ that is $\alpha$-less than $n$, if such $i$ exists. Otherwise, let $i = 0$. Let $j$ be the $\alpha$-smallest among $1, 2, \ldots, n - 1$ that is $\alpha$-bigger than $n$, and if no such $j$ exists, let $j = 0$. By the choice of $s_k, t_k$ for $k = 0, 1, \ldots, n - 1$, $t_i < s_j$. Let $(s_n, t_n)$ be the first interval in $\mathcal{P}$ such that it is

(i) strictly inside $(t_i, s_j)$,  
(ii) contains $\frac{t_i + s_j}{2}$, and  
(iii) contains the first $r_m$ in $(t_i, s_j)$.

It is clear that this process can be continued for all $n \in \mathbb{N}$ and yields a pairwise disjoint system of intervals \{(s_n, t_n) \mid n \in \mathbb{N}\} such that the order of \{s_n \mid n \in \mathbb{N}\} is isomorphic to the order coded by $\alpha$. Let $\mathcal{Q} = \{J_k \mid k \in \mathbb{N}\}$ be an enumeration of the intervals with rational endpoints in $(A, B)$. We now let $(p_n, q_n)$ be the first interval in $\mathcal{Q}$ that is contained in $(s_n, t_n)$.

66
The collection \{ (p_n, q_n) \mid n \in \mathbb{N} \} constructed this way has all of the desired properties. Requirement (ii) of the construction ensures (b),(c) and (d). Property (e) follows from (iii): we will show that for any \( m, r_m \) is not an accumulation point of \( S = \{ p_n, q_n \mid n \in \mathbb{N} \} \). If \( r_m \in (s_N, t_N) \) for some \( N \), then there are only two points from \( S \), namely \( p_N \) and \( q_N \) inside \( (s_N, t_N) \) and so \( r_m \) cannot be an accumulation point of \( S \). Suppose \( r_m \notin (s_n, t_n) \) for all \( n \in \mathbb{N} \). Without loss of generality, assume \( r_m \in (t_1, B) \). Then there are at most \( m - 1 \) intervals \( (s_i, t_i) \) in \( (t_1, B) \), for otherwise, \( r_m \) would have been picked up by one of intervals \( (s_i, t_i) \) (the only reason it was not picked up is because an ‘earlier’ rational point was picked up instead; but there are only \( m - 1 \) rational points preceding \( r_m \)). Thus, there are only finitely many points from \( S \) in \( (t_1, B) \), and so \( r_m \) cannot be an accumulation point of \( S \).

It is clear from the construction that if \( \alpha \) and \( \beta \) in \( LO \) agree on the order of \( 1, 2, \ldots, N \), then \( (p_n^\alpha, q_n^\alpha) = (p_n^\beta, q_n^\beta) \) for \( n = 1, \ldots, N \). \( \square \)

**Lemma 57.** There is a Borel function \( G : LO \to \mathcal{M}_Q(A, B) \subseteq \text{Aut}(Q, <) \) such that

\[
G(\alpha) \in \text{Aut}(Q, <)^{(2)} \quad \text{if and only if} \quad \alpha \in LO2.
\]

**Proof. Construction.** Let \( \alpha \in LO \). We define an automorphism \( G(\alpha) \) of \( (Q, <) \). Let \( \{ (p_n^\alpha, q_n^\alpha) \mid n \in \mathbb{N} \} \) be a discrete collection of open intervals assigned to \( \alpha \) as in Lemma 56. Let \( U_\alpha = \bigcup_{n \in \mathbb{N}} (p_n^\alpha, q_n^\alpha) \subseteq (A, B) \).

Let \( h : [0, 1] \to [0, \frac{1}{4}] \) be the map

\[
h(x) = \begin{cases} 
\frac{1}{2} x, & \text{if } x \in [0, \frac{1}{2}] \\
\frac{1}{2} - \frac{1}{2} x, & \text{if } x \in [\frac{1}{2}, 1].
\end{cases}
\]

Define \( F(\alpha) : S^1 \to S^1 \) as follows: for \( x \in S^1 \),

\[
F(\alpha)(x) = \begin{cases} 
\frac{1}{2} + x, & \text{if } x \notin U_\alpha \cup (\frac{1}{2} + U_\alpha), \\
\frac{1}{2} + x + (q_n^\alpha - p_n^\alpha) h(\frac{x - p_n^\alpha}{q_n^\alpha - p_n^\alpha}), & \text{if } x \in (p_n^\alpha, q_n^\alpha) \cup (\frac{1}{2} + (p_n^\alpha, q_n^\alpha))
\end{cases}
\]

see Figure 8. (It is understood here that points greater than 1 are identified with their decimal parts, i.e. \( S^1 \) is seen as the quotient space obtained from \( \mathbb{R} \) by identifying points
$x$ and $y$ if and only if $x - y \in \mathbb{Z}$.) Then $F(\alpha)$ is a homeomorphism of $S^1$ in $\mathcal{M}(A, B)$.

Define $G(\alpha)$ to be the restriction of $F(\alpha)$ to the rational circle $Q$:

$$G(\alpha) = F(\alpha) \restriction Q.$$

Then $G(\alpha) \in \mathcal{M}_Q(A, B)$ and $\hat{G}(\alpha) = F(\alpha)$.

\[\text{Figure 8: Map } F(\alpha).\]

**Borel measurability.** The sets

$$B(\pi, x_1) = \{ \sigma \in Aut(Q, <) \mid \pi(x_1) = \sigma(x_1) \},$$

where $\pi \in Aut(Q, <)$ and $x_1 \in Q$, form a countable subbasis for the topology on $Aut(Q, <)$. To show that $G(\alpha)$ is Borel, it suffices to show that the inverse image under $G$ of any subbasic open set is Borel. Let

$$S = G^{-1}(B(\pi, x_1)) = \{ a \in LO \mid G(\alpha)(x_1) = \pi(x_1) \}.$$
Fix $\beta \in S$ (case $S = \emptyset$ is trivial). Then $G(\beta)(x_1) = \pi(x_1)$, so

$$S = \{ \alpha \in LO \mid G(\alpha)(x_1) = G(\beta)(x_1) \}.$$ 

Case $x_1 \in U_\beta \cup (\frac{1}{2} + U_\beta)$: We will show that $S$ is open. Fix $\alpha \in S$. Notice that

$$x_1 \in U_\beta \cup (\frac{1}{2} + U_\beta) \iff G(\beta)(x_1) \neq \frac{1}{2} + x_1 \iff G(\alpha)(x_1) \neq \frac{1}{2} + x_1 \iff x_1 \in U_\alpha \cup (\frac{1}{2} + U_\alpha).$$

Thus, $x_1 \in (p^a_N, q^a_N) \cup (\frac{1}{2} + (p^a_N, q^a_N))$ from some $N$. Then

$$N(\alpha, \{1, \ldots, N\} \times \{1, \ldots, N\}) = \{ \gamma \in LO \mid \alpha \text{ and } \gamma \text{ agree on the order of } 1, \ldots, N \}$$

is a basic open neighborhood of $\alpha$ contained in $S$, and so $S$ is open.

Case $x_1 \notin U_\beta \cup \frac{1}{2} + U_\beta$: We show that $S$ is closed. In this case, $G(\beta)(x_1) = \frac{1}{2} + x_1$, so

$$S = \{ \alpha \in LO \mid G(\alpha)(x_1) = \frac{1}{2} + x_1 \} = \{ \alpha \in LO \mid x_1 \notin U_\alpha \cup (\frac{1}{2} + U_\alpha) \}. $$

Fix $\alpha \in S^C = \{ \alpha \in LO \mid x_1 \in U_\alpha \cup (\frac{1}{2} + U_\alpha) \}$. Let $N$ be such that $x_1 \in (p^a_N, q^a_N) \cup (\frac{1}{2} + (p^a_N, q^a_N))$. Then $N(\alpha, \{1, \ldots, N\} \times \{1, \ldots, N\})$ is an open neighborhood of $\alpha$ contained in $S^C$, so $S^C$ is open, and $S$ is closed.

**To be square is to be even.** We now show that $G(\alpha)$ is a square if and only if $\alpha \in LO(2)$.

Suppose $G(\alpha) \in Aut(Q, <)^{(2)}$. Let $c$ be an irrational point in $(A, B)$ and $\phi : [A, c] \to [c, B]$ an order preserving homeomorphism as in Lemma 55. Continuing as in the proof of Lemma 52, we see that $\alpha \in LO(2)$.

Conversely, suppose $\alpha \in LO(2)$. According to Lemma 55, to see that $G(\alpha)$ is a square, we need to find an irrational point $c \in (A, B)$ and an order preserving homeomorphism $\phi : [A, c] \to [c, B]$ such that $\phi([A, c] \cap Q) = [c, B] \cap Q$, and

$$\phi(D(\hat{\pi}([A, c]))) = D(\hat{\pi}([c, B])).$$
As before, write \( \mathbb{N} \) as the disjoint union of sets \( J \) and \( K \) such that each element of \( J \) is \( \alpha \)-less than each element of \( K \) and there is an \( \alpha \)-order preserving bijection \( \tau : J \leftrightarrow K \). Let \( c_1 = \sup \{ q_n \mid n \in J \} \) and \( c_2 = \inf \{ p_n \mid n \in K \} \). If \( J \) has no biggest element, let \( c = c_1 \). Note that \( c_1 \) is irrational, since it is an accumulation point of \( \{ q_n \mid n \in \mathbb{N} \} \). If \( K \) has no smallest element, let \( c = c_2 \). Again, \( c_2 \) is irrational, as an accumulation point of \( \{ p_n \mid n \in \mathbb{N} \} \). Otherwise, let \( c \) be any irrational point between \( c_1 \) and \( c_2 \). Define \( \phi(p_n) = p_{\tau(n)} \) and \( \phi(q_n) = q_{\tau(n)} \). As before, \( \phi \) can be extended to the closure of \( \{ p_n, q_n \mid n \in \mathbb{N} \} \) by

\[
\phi(x) = \begin{cases} 
\sup \{ \phi(q_n) \mid q_n \leq x \}, & \text{if } x = \sup \{ q_n \mid q_n \leq x \}, \\
\inf \{ \phi(p_n) \mid p_n \geq x \}, & \text{if } x = \inf \{ p_n \mid p_n \geq x \}.
\end{cases}
\]

Next, define \( \phi(A) = c \) and \( \phi(c) = B \). As we have seen before, these definitions are non-ambiguous, and define an order preserving map \( \phi \) on \( S = \{ p_n, q_n \mid n \in \mathbb{N} \} \cup \{ A, c \} \). Note that \( \phi \) takes rational points to rational points, and irrationals to irrationals.

Next we extend \( \phi \) to the complement of \( S \) in \( [A, c] \). The complement consists of pairwise disjoint open intervals. Let \((a, b)\) be a component of the complement. Note that \( a, b \in S \). If the points \( a \) and \( b \) are both rational, define \( \phi \) on \((a, b)\) simply to be the linear function \( \phi(x) = \phi(a) + \frac{\phi(b) - \phi(a)}{b - a} (x - a) \), ‘connecting’ the points \((a, \phi(a))\) and \((b, \phi(b))\) of the graph of \( \phi \). If one of the endpoints \( a \) and \( b \) is irrational, to ensure that \( \phi \) preserves rationality, proceed as follows: Fix two sequences \((a_n)\) and \((b_n)\) of rational points in \((a, b)\) such that \( a < \cdots < a_3 < a_2 < a_1 < b_1 < b_2 < b_3 < \cdots < b \), and \( a_n \to a \), \( b_n \to b \). Also, pick sequences \((c_n)\) and \((d_n)\) of rational points in \((\phi(a), \phi(b))\) such that \( \phi(a) < \cdots < c_3 < c_2 < c_1 < d_1 < d_2 < d_3 < \cdots < \phi(b) \), and \( c_n \to \phi(a) \), \( d_n \to \phi(b) \). Define \( \phi(a_n) = c_n \) and \( \phi(b_n) = d_n \) for each \( n \), and on each subinterval \((a_{n+1}, a_n), (a_1, b_1)\) \((b_n, b_{n+1})\) define \( \phi \) to be the linear function ‘connecting’ the existing points of the graph of \( \phi \).

This construction ensures that \( \phi \) has all of the properties required by Lemma 55, so \( G(a) \in \text{Aut}(Q, <)\).

\[\blacksquare\]

**Theorem 58.** The set of squares \( \text{Aut}(Q, <)^{(2)} \) in \( \text{Aut}(Q, <) \) is complete analytic.
Proof. The set $\text{Aut}(Q, <)^{(2)}$ is analytic, since $\pi \mapsto \pi^2$ is continuous. Map $G$ from Lemma 57 is a Borel reduction of the complete analytic set $LO2$ to $\text{Aut}(Q, <)^{(2)}$. By the remarks made earlier, this proves that $\text{Aut}(Q, <)^{(2)}$ is complete analytic. \qed
BIBLIOGRAPHY


