# ON THE UNIQUENESS OF POLISH GROUP TOPOLOGIES

by

**Bojana Pejić**

M.A. in Mathematics, University of Pittsburgh, 2006

MMath in Mathematics, 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

UNIVERSITY OF PITTSBURGH

DEPARTMENT OF MATHEMATICS

This dissertation was presented

by

Bojana Pejić

It was defended on

August 7th 2007

and approved by

Dr. Paul Gartside, University of Pittsburgh

Dr. Vladimir Uspenskiy, Ohio University

Dr. Robert Heath, University of Pittsburgh

Dr. Christopher Lennard, University of Pittsburgh

Dissertation Director: Dr. Paul Gartside, University of Pittsburgh

# ABSTRACT

## ON THE UNIQUENESS OF POLISH GROUP TOPOLOGIES

Bojana Pejić, PhD

University of Pittsburgh, 2007

Polish groups are separable completely metrizable topological groups. A key problem in the theory of Polish groups is that of the uniqueness of a Polish group topology: under what conditions does a group admit only one Polish group topology? Closely related is the problem of automatic continuity: when is a homomorphism between Polish groups necessarily continuous? This dissertation is an investigation of these questions.

The key to unlocking these problems is to determine which sets in a Polish group are *definable* both algebraically and topologically. By *algebraically definable* one has in mind sets such as the commutators, conjugacy classes, or the squares. In the context of Polish groups, *topologically definable* means being a Borel set. A classical uniqueness result requires algebraically definable sets that are always Borel. Unfortunately its use is sometimes limited: while algebraically definable sets are often analytic (continuous images of Borel sets), it is shown here that they are not necessarily Borel. In particular, the set of squares in the homeomorphism group of the unit circle, and the set of squares in the automorphism group of the rational circle, are not Borel.

An alternative result that avoids the need for Borel sets is obtained: a Polish group with a neighborhood base at the identity consisting of sets that are always analytic has a unique Polish group topology. As a consequence of this result, compact, connected, simple Lie groups and finitely generated profinite groups have a unique Polish group topology.

# TABLE OF CONTENTS

# LIST OF FIGURES

# PREFACE

It is my pleasure to acknowledge a number of people who contributed towards the successful completion of this dissertation.

First, I would like to express my sincerest gratitude to my advisor, Professor Paul Gartside. Paul has been a great mentor and teacher, and I feel very privileged to have had the opportunity to work with him on many fun problems.

I am also indebted to the members of my dissertation committee: Professors Vladimir Uspenskiy, Bob Heath and Chris Lennard, for their insightful questions, comments and suggestions, which significantly influenced the final version of this work.

I am deeply grateful to Mr. and Mrs. Boris Vukobrat, whose generous support during my undergraduate years at Oxford University made my dream of pursuing a career in mathematics possible.

Throughout my education I received much encouragement from my family. I thank my parents for nurturing my interest and love of mathematics, and to my sister Snežana for being a wonderful friend and a champion role model. I would not be here without their support.

Finally, I would like to thank with love my husband Chris, for generously giving me his time, love and support during the months this dissertation was written — and always.

Bojana Pejić<br>
August 2007

# 1.0 INTRODUCTION

## 1.1 OVERVIEW AND STRUCTURE OF DISSERTATION

*Polish groups* are topological groups that are 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, autohomeomorphism groups, Lie groups, automorphism groups of first-order structures, profinite groups etc. are some of the examples of Polish groups.

Often, the topological structure is fundamentally important for proving results about groups. But conversely, the algebraic structure places very tight restrictions on the types of topology that can be defined on a group. In essence, my work is a part of a wider program to understand what topologies can arise in given algebraic structures.

In particular, my dissertation advisor Dr. Paul Gartside and I have been interested in the extreme case where the collection of group topologies of specified type on a group is small — of cardinality 0 or 1. When does a group admit no more than one locally compact, separable, metrizable group topology? When does a group admit a unique Polish group topology?

These questions form 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 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*, [6]). For example, every character on a Banach algebra is continuous, and also, any homomorphism onto a semisimple Banach algebra is continuous. Until recently, one of the fundamental problems in the theory of profinite (i.e., compact zero-dimensional) groups was *Serre's Conjecture* (now resolved in the positive by Nikolov and Segal [27]) which essentially asked if every finitely generated profinite group has a unique profinite group topology. Also, 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.

The starting point for much of the research in this dissertation is a classical result on the uniqueness of a Polish group topology due to G.W. Mackey [24]. According to Mackey's theorem, 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. Indeed, at first glance it seems impossible to find sets which are Borel in *all* Polish group topologies without already knowing what the Polish group topologies are — and then we would *already* know that there is only one such topology, and that the group admits a unique Polish group topology. We can avoid such circularity by considering special sets called identity sets and verbal sets.

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, and the $m$-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 [19] 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 the infinite symmetric group $S_\infty$ admits only one Polish group topology. However, the identity sets are sometimes not sufficient. For example, we will see that in the special orthogonal group $SO(3,\mathbb{R})$ no countable collection of identity sets separates points, and so the identity sets alone cannot 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.

This problem raises two natural questions: first, are all verbal sets in fact Borel, and second, can Mackey's result be extended by allowing analytic (but not necessarily Borel) sets in the countable point-separating family? Our investigation thus follows two directions, giving rise to two parts of the dissertation. In the first part (Chapters 3 and 4), we obtain alternative results on the uniqueness of a Polish group topology that allow us to use analytic sets (such as verbal sets). In the second part (Chapter 5), we examine the complexity of verbal sets and establish that not all verbal sets are Borel.

We now outline the contents in more detail.

Chapter 2 provides fundamental definitions and important results on Polish spaces and groups that will be needed in subsequent chapters.

The general theory is discussed and developed in Chapter 3. In Section 3.1 we explore the relationship between the property of having a unique Polish group topology and the property of automatic continuity of homomorphisms between Polish groups. In Sections 3.2 and 3.3 we define identity and verbal sets and make first steps in investigating their complexity. In Section 3.4 we continue by discussing the effectiveness of identity sets in proving uniqueness of topology results. In Sections 3.5, 3.6 and 3.7, we investigate different ways of utilizing verbal sets. Of special importance are Theorems 21 and 22 of Section 3.6, which say that a Polish group admits a unique Polish group topology if it has a countable network, or a neighborhood base at the identity, consisting of verbal sets. Section 3.8 introduces the *separating group*, a notion motivated by the study of automatic continuity in Banach algebras.

Chapter 4 is devoted to the applications of the general results established in the previous chapter. The uniqueness of the Polish group topology is shown for the infinite symmetric group, compact, connected, simple Lie groups (such as $SO(3, \mathbb{R})$), and finitely generated profinite groups.

Chapter 5 is devoted to resolving the question of whether all verbal sets are Borel. From the theory of Polish group actions, we know that conjugacy classes are always Borel. We show that in *Abelian* Polish groups all verbal sets are Borel (Section 5.1), and that in $S_\infty$ all full verbal sets are Borel (Section 5.2). One might anticipate that verbal sets would also be Borel in any Polish group. However, the example of the squares in the autohomeomorphism group of the circle, which, in Section 5.4, we show is not Borel, dispels this hope. In contrast with the situation in $S_\infty$, where all full verbal sets are Borel, in 5.5 we exhibit an example of a closed subgroup of $S_\infty$ in which the set of squares is not Borel.

## 2.0 BACKGROUND

In this chapter we give a summary of basic notions and facts about Polish spaces and groups. Unless a specific citation is given, all of these can be found in [20] and [1], which are our main references for descriptive set theory.

### 2.1 POLISH SPACES

A *Polish space* is a separable topological space that is metrizable by a complete metric.

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

In a topological space $(X, \tau)$, the set of *Borel sets* is the $\sigma$-algebra generated by the open sets. It is denoted by $\mathbf{B}(X, \tau)$, or simply $\mathbf{B}(X)$, when confusion is impossible. If $X$ is metrizable (so that every closed set is a $G_\delta$-set), the set $\mathbf{B}(X)$ 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. Intuitively, we think of the sets in higher levels as 'more complex', because their definition in terms of the open sets is more complex.

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

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 $A \triangle U = (A \setminus U) \cup (U \setminus A)$ is meager. The sets having the Baire property form the smallest $\sigma$-algebra containing all open sets and all meager sets.

A function $f : X \to Y$ is *Borel measurable*, or *Borel*, if the inverse image of any open set in $Y$ is Borel in $X$. We call $f$ a *Borel isomorphism* if it is a bijection and both $f$ and $f^{-1}$ are Borel. Similarly, we say that a map $f : X \to Y$ 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 a 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 $F : X \to Y$ such that $F^{-1}(B) = A$. Such a function is called a *continuous reduction* of $A$ to $B$. Kechris showed in [21] that it is sufficient for $F$ to be a *Borel reduction*, i.e., 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 $F : X \to Y$ 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]. Informally, complete analytic sets are ‘at least as complex’ as other analytic sets, and true analytic sets are ‘strictly more complex’ than Borel sets. The existence of true analytic sets implies that complete analytic sets are ‘strictly more complex’ than Borel sets.

All analytic sets have the Baire property.

We recall the following well-known result of Souslin:

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

**Theorem 2** (Lusin–Souslin)**.** *Let $X$, $Y$ be Polish spaces and $f : X \to Y$ 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 $f(A)$.*

By applying the above theorem to the identity map, we find:

**Theorem 3.** *If $(X, \mathcal{S}_1)$ and $(X, \mathcal{S}_2)$ are two standard Borel spaces, then either the two $\sigma$-algebras are equal: $\mathcal{S}_1 = \mathcal{S}_2$, or incomparable: $\mathcal{S}_1 \nsubseteq \mathcal{S}_2$ and $\mathcal{S}_2 \nsubseteq \mathcal{S}_1$.*

## 2.2 POLISH GROUPS

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

The main problem that we address in this dissertation is that of the uniqueness of a Polish group topology: under what conditions does a given Polish group admit only one Polish group topology?

Observe that the additive group $\mathbb{R}$, for example, does not have a unique Polish group topology. Group $\mathbb{R}$ is isomorphic (as an abstract group) to $\mathbb{R}^n$ for any $n \in \mathbb{N}$, because each of these groups is a vector space over $\mathbb{Q}$ of dimension $2^{\aleph_0}$. Giving $\mathbb{R}$ the topology of $\mathbb{R}^n$ for each $n$, we obtain many different Polish group topologies on $\mathbb{R}$. For more examples of Polish groups with non-unique Polish group topologies, please see Sections 4.2 and 4.3. Note that all of these examples use the Axiom of Choice.

We recall several important results that will be used in later chapters in studying the uniqueness of Polish group topologies.

**Theorem 4** (Pettis)**.** *Let $G$ be a topological group and $A \subseteq G$ a set with the Baire property which is not meager. Then $A^{-1}A$ contains an open neighborhood of the identity.*

From this we have the following easy consequence:

**Theorem 5.** *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.*

By applying Theorem 5 to the identity map, one obtains:

**Theorem 6.** *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: $\tau_1 \nsubseteq \tau_2$ and $\tau_2 \nsubseteq \tau_1$.*

We say that a family $\mathcal{A}$ of sets in a space $X$ *separates* (or $T_1$*-separates*) *points* of $X$ if for every pair of distinct points $x$ and $y$ in $X$, there is a set $A \in \mathcal{A}$ such that $x \in A$, but $y \notin A$. We say that $\mathcal{A}$ is a *point-separating*, or $T_1$*-separating family* of $X$. Similarly, we say that $\mathcal{A}$ $T_0$*-separates points* in $X$ if for any $x \neq y$ in $X$, we can find $A \in \mathcal{A}$ that contains one of the points but not the other. Call $\mathcal{A}$ 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 [24] gives sufficient conditions for a family of sets in a Polish space $X$ to generate all of the Borel sets in $X$.

**Theorem 7** (Mackey)**.** *Let $(X, \tau)$ be a Polish space and $\mathcal{A}$ a countable point-separating family of Borel sets in $X$. Then the Borel sets in $X$ are generated by the family $\mathcal{A}$: $\mathbf{B}(X, \tau) \subseteq \sigma(\mathcal{A})$. (In fact, $\mathbf{B}(X, \tau) = \sigma(\mathcal{A})$.)*

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 8** (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 7 and Corollary 8, 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 $T_1$-separating family of Borel sets, and $\sigma(\mathcal{A}) = \sigma(\mathcal{A}')$.

Finally, from the theory of Polish group actions, we recall the following well-known result (see [25]):

**Theorem 9** (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.*

## 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.

For notational simplicity, by a *homomorphism* between topological groups we will mean an *abstract group* homomorphism — and similarly for a monomorphism, epimorphism and isomorphism.

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 (abstract group) automorphism of $G$ is continuous.

We prove a series of lemmas that establish relationships and facts about these properties. In particular, we will see that (AC) $\implies$ (U) $\implies$ (Aut) (Lemma 11). Lemmas 14 and 15 reveal another parallel between properties (AC) and (U). Also, we will see that in proving (AC), one may restrict their attention to monomorphisms between Polish groups (Lemma 12). If we know that a Polish group $G$ possesses property (AC), then in fact homomorphisms from $G$ into any second-countable topological group are continuous (Lemma 14), and even into any separable group, or $\aleph_0$-bounded group (Lemma 16).

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

*(i) $G$ has 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 $\sigma$ 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 $\mathrm{id} : (G, \tau) \to (G, \tau')$ is continuous by (ii), so $\tau' \subseteq \tau$. By Theorem 6, $\tau = \tau'$, so $G$ has a unique Polish group topology. □

**Lemma 11.** *The following implications hold in a Polish group G:*

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

*Proof.* This follows immediately after replacing (U) by the equivalent condition given in Lemma 10. □

**Lemma 12.** *Let G be a Polish group. The following are equivalent:*

*(i) $G$ has property (AC),*

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

*Proof.* (i) ⇒ (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. Thus $\phi$ is continuous. □

**Lemma 13.** *Let G be a Polish group. The following are equivalent:*

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

*(ii) Every epimorphism $\phi : H \to G$ with closed kernel, where $H$ is a Polish group, is continuous.*

*Proof.* Suppose $G$ has (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 property (U) 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 $\tau$ be the given Polish group topology on $G$ and let $\tau'$ be another Polish group topology on $G$. Then the identity map $\mathrm{id} : (G, \tau') \to (G, \tau)$ must be continuous, by (ii). Thus, $\tau \subseteq \tau'$, and so $\tau = \tau'$, by Theorem 6. □

**Lemma 14.** *The following are equivalent for a Polish group $G$:*

*(i) $G$ has 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) ⇒ (i). To show (i) ⇒ (ii), recall that every second-countable group $H$ embeds as a topological group into the Polish group $Homeo(I^{\mathbb{N}})$ of homeomorphisms of the Hilbert cube [32], say, via $e : H \to Homeo(I^{\mathbb{N}})$. Let $\phi : G \to H$, where $H$ is second-countable, be a homomorphism. Then $e \circ \phi : G \to Homeo(I^{\mathbb{N}})$ is a homomorphism from $G$ into the Polish group $Homeo(I^{\mathbb{N}})$. By (AC), $e \circ \phi$ is continuous, and thus $\phi$ is continuous.

(ii) ⇒ (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 $\sigma \subseteq \tau$.

(iii) ⇒ (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), $\sigma \subseteq \tau$. Thus, the inverse image under $\phi$ of any open set in $H$ is open in $(G, \tau)$, so $\phi$ is continuous. □

**Lemma 15.** *The following are equivalent for a Polish group $G$:*

*(i) $G$ has 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 (Theorem 6). □

Recall that 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 $U$, that is, if there exists a countable subset $C$ of $H$ such that $C \cdot U = H$.

**Lemma 16.** *Let $G$ be a Polish group. The following are equivalent:*

*(i) $G$ has property (AC),*

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

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

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

*Proof.* We have already seen that (i) ⇔ (ii) in Lemma 14. Since every second-countable space is separable, and every separable topological group is $\aleph_0$-bounded, the implications (iv) ⇒ (iii) ⇒ (ii) are immediate. We show that (ii) ⇒ (iv). Let $H$ be an $\aleph_0$-bounded topological group and $\phi : G \to H$ a homomorphism. Recall that every $\aleph_0$-bounded topological group embeds into a product of second-countable topological groups [10]. Let $e : H \to \prod_{\lambda \in \Lambda} H_\lambda$, where each $H_\lambda$ is a second-countable topological group, be such an embedding of $H$. For each $\lambda$, the homomorphism $\pi_\lambda \circ e \circ \phi : H \to H_\lambda$ is continuous by hypothesis (ii) (here, $\pi_\lambda$ denotes the $\lambda$-th projection of $\prod_{\mu \in \Lambda} H_\mu$ to $H_\lambda$). Thus, $\phi$ is continuous. □

## 3.2 IDENTITY AND VERBAL SETS

As we shall see throughout this dissertation, 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 $F$ be the free group on a countably infinite set $X$. We recall several definitions and facts from group theory: A *word* $w$ in $X$ is a finite (possibly empty) sequence of symbols from $X \cup \{x^{-1} \mid x \in X\}$: written in the form $w = x_1^{\varepsilon_1} \cdots x_r^{\varepsilon_r}$, where $x_i \in X$, $\varepsilon_i = \pm 1$, $r \geq 0$. In case $r = 0$, $w$ is denoted by 1. The *product* of two words $w = x_1^{\varepsilon_1} \cdots x_r^{\varepsilon_r}$ and $v = y_1^{\eta_1} \cdots y_s^{\eta_s}$ is formed by concatenation: $wv = x_1^{\varepsilon_1} \cdots x_r^{\varepsilon_r} y_1^{\eta_1} \cdots y_s^{\eta_s}$, with the convention that $w1 = w = 1w$. The inverse of $w$ is $w^{-1} = x_r^{-\varepsilon_r} \cdots x_1^{-\varepsilon_1}$, and the inverse of 1 is 1. A word is *free* if it contains no pair of consecutive symbols of the form $xx^{-1}$ or $x^{-1}x$ ($x \in X$). Two words are *equivalent* if it is possible to pass from one to the other by means of a finite sequence of *insertions* of an $xx^{-1}$ or an $x^{-1}x$ ($x \in X$) or *deletions* of such an $xx^{-1}$ or an $x^{-1}x$. We identify each equivalence class of this equivalence relation with the unique free word it contains. Then the free group $F$ can be taken to be the set of the equivalence classes of words in $X$ (or, equivalently, the set of free words in $X$), with multiplication defined by $[w][v] = [wv]$.

Let $w = w(x_1, \ldots, x_r) \in F$ be a free word in $X$ involving symbols $x_1, \ldots, x_r \in X$, or their inverses. If $G$ is an arbitrary group and $g_1, \ldots, g_r \in G$, the *value* of the word $w$ at $(g_1, \ldots, g_r)$, denoted by $w(g_1, \ldots, g_r)$, is the element of $G$ obtained by replacing each $x_i$ by $g_i$, and the operations in $F$ by the operations in $G$. 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*. Identity sets can be seen 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 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, the centralizer of an element $a \in G$: $\{g \in G \mid gag^{-1}a^{-1} = 1\}$ is an identity set, the conjugacy class: $\{gag^{-1} \mid g \in G\}$ is a (non-full) verbal set, 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 $W(G)$ generated by all $w$-values in $G$, for all $w \in W$, i.e.,

$$W(G) = \langle \bigcup_{w \in W} \{w(g_1, \ldots, g_{n(w)}) \mid g_1, \ldots, g_{n(w)} \in G\} \rangle,$$

where $n(w)$ is the number of letters in $w$. If $W = \{w\}$, we write $w(H)$ for $W(H)$.

## 3.3 TOPOLOGICAL STATUS OF IDENTITY AND VERBAL SETS

A classical example that illustrates the importance of definability of sets is a theorem of Mackey [24] (Corollary 8). 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 identity sets, 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 identity sets ideal candidates to be used in applying Mackey's result. Indeed, identity sets have been used to show the uniqueness of a Polish group topology for a number of Polish groups. For further discussion, see Sections 3.4 and 4.1 below.

Verbal sets, on the other hand, are continuous *forward* images of Polish spaces, and therefore necessarily analytic in any Polish group. An important question that this dissertation resolves is whether verbal sets are in fact always Borel. It is known that in a general Polish group all conjugacy classes are Borel (this follows from the fact that all orbits of a Polish group acting continuously on a Polish space are Borel (Theorem 9): apply this to the conjugation action of the Polish group on itself). We also show that in Abelian Polish groups all verbal sets are Borel, and in the infinite symmetric group $S_\infty$ all 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 54), dispels this hope. A detailed discussion on the complexity of verbal sets is deferred to Chapter 5.

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

**Lemma 17.** *If $G$ is a Polish group and $W$ is a set of free words, then 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 the product of a finite list of values of words from $W$. Let $S_N$ be the set of those elements of $W(G)$ that can be written as the product of $N$ values of words from $W$. Then $S_N$ is the union of a countable collection of verbal sets:

$$S_N = \bigcup_{w_1,\ldots,w_N \in W} \{w_1(\mathbf{g_1}) \cdots w_N(\mathbf{g_N}) \mid \mathbf{g_j} \in G^{m_j}, \text{ where } m_j \text{ is the number of letters in } w_j\}.$$

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. □

## 3.4 UNIQUENESS AND IDENTITY SETS

As we have seen, identity sets are closed, and thus Borel, in any (Polish) group. Thus, we have the following corollaries to Mackey's theorem:

**Corollary 18.** *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 19.** *Let $G$ be a Polish group with a countable subset $H$, such that for any pair of distinct points $a, b$ in $G$, there is a free word $w(x_0, x_1, \ldots, x_n)$ and $h_1, \ldots, h_n \in H$ such that*

$$w(a, h_1, \ldots, h_n) = 1, \quad \textit{but} \quad w(b, h_1, \ldots, h_n) \neq 1.$$

*Then $G$ admits only one Polish group topology.*

*Proof.* Let

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

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

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

Thus $\mathcal{C}$ separates points and Corollary 18 applies. □

Identity sets have been highly effective in proving uniqueness of Polish group topology results. In [19], Kallman shows that, for a wide class of spaces $X$, the autohomeomorphism group $G = Homeo(X)$ admits a unique Polish group topology. The list of spaces $X$ for which the result holds includes: separable metrizable manifolds, connected, countable, locally finite simplicial complexes, the Hilbert cube, the Cantor set, and the natural numbers. In proving this result, Kallman essentially applies Mackey's theorem to the countable family of sets

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

where $(U_n)$ is a countable basis for the topology of $X$, and $U'$ ranges over the nonempty 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 $G = Homeo(X)$ 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

$$S(U', V') := \{g \in G \mid g g_{U'} g^{-1} \text{ commutes with } g_{V'}\}$$

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 the sets $S(U',V')$ is also countable. Finally, observe that the sets $S(U',V')$ are identity sets:

$$S(U',V') = \{g \in G \mid gg_{U'}g^{-1}g_{V'}gg_{U'}^{-1}g^{-1}g_{V'}^{-1} = 1\}.$$

For another 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 $S_\infty$.

### 3.5 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, identity sets may not always be sufficient. For example, we will see in Section 4.2, that in the special orthogonal group, $SO(3,\mathbb{R})$, *no* countable collection of identity sets separates points. Therefore, in $SO(3,\mathbb{R})$, 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 sets with the Baire property.

Recall that Mackey's theorem follows from Theorem 7: If $X$ is a Polish space and $\mathcal{A}$ a countable point-separating family of *Borel* sets in $X$, then $\mathbf{B}(X) \subseteq \sigma(\mathcal{A})$. If Theorem 7 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.

**Remark.** Recall that in Mackey's theorem the $T_1$-separating family of Borel sets can be replaced by a $T_0$-separating family. In the analytic version of Mackey's theorem (if it were true), one could not readily replace '$T_1$-separating' by '$T_0$-separating', since the complement of an analytic set is not necessarily analytic.

Lemma 20 below shows that Theorem 7 does not hold with 'Borel' replaced by '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 20.** *Let $\mathcal{C} = 2^{\mathbb{N}}$ be the Cantor space. There is a countable point-separating family $\mathcal{A}$ of sets in $\mathcal{C}$, each of which is the (disjoint) union of an analytic and a co-analytic set, such that*

$$\mathbf{B}(\mathcal{C}) \not\subseteq \sigma(\mathcal{A}).$$

*Proof.* Let $U = \{x \in \mathcal{C} \mid x(0) = 0\}$. Note that $U = \{0\} \times 2^{\mathbb{N}}$ is homeomorphic to $\mathcal{C}$. Fix an uncountable analytic, but not Borel (in $\mathcal{C}$) 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 $\mathcal{C}$.) On the other hand, $A \subsetneq U$, 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 Schröeder-Bernstein argument as follows. Define subsets $K_n$ of $U$, for $n \geq 0$ recursively by: $K_0 = U \setminus h_1(A)$, $\quad K_n = h_1(g_1(K_{n-1}))$, for $n \geq 1$. Let $C_1 = \bigcup_n K_n$, $B_1 = U \setminus C_1$, $D_1 = h_1^{-1}(B_1) = B_1$, $E_1 = g_1(C_1)$. See Figure 1.

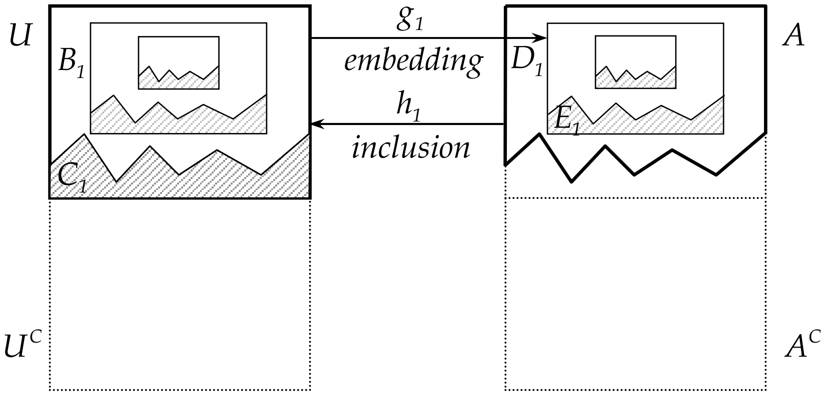

Figure 1: Constructing the first bijection: Homeomorphic embeddings $g_1$ and $h_1$.

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 $h_2 : \mathcal{C} \to U^C$ 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 $x \in \mathcal{C}$. Then $g_2$ and $h_2 \restriction A^C$ 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: $L_0 = U^C \setminus h_2(A^C)$, $\quad L_n = h_2(g_2(L_{n-1}))$, for $n \geq 1$. Let $B_2 = \bigcup_n L_n$, $C_2 = U^C \setminus B_2$, $D_2 = g_2(B_2) = B_2$, $E_2 = h_2^{-1}(C_2)$. See Figure 2.

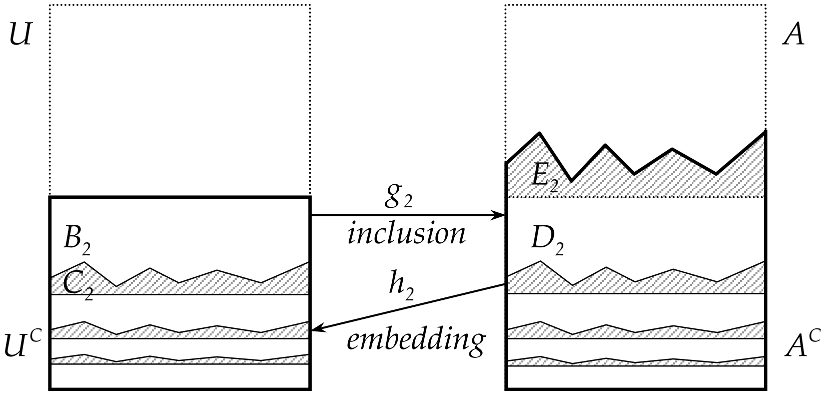

Figure 2: Constructing the second bijection: Homeomorphic embeddings $g_2$ and $h_2$.

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 $U_n = \{x \in \mathcal{C} \mid x(n) = 0\}$ and $A_n = f(U_n)$ for $n \geq 0$, and let $\mathcal{U} = \{U_n \mid n \geq 0\}$ and $\mathcal{A} = \{A_n \mid n \geq 0\} \cup \{A_n^C \mid n \geq 0\}$. 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 $\mathcal{C}$. 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 $f^{-1}(y)(n) = 0$, then $x \in A_n^C$ and $y \notin A_n^C$.

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

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

Clearly, $U_n \cap B$ 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 and analytic set. Also, $h_2^{-1}(U_n \cap C_2) = \mathcal{C} \setminus h_2^{-1}(U^C \setminus (U_n \cap C_2))$ is co-analytic.

Lastly, we need to show that $\mathbf{B}(\mathcal{C}) \nsubseteq \sigma(\mathcal{A})$. Since $(\mathcal{C}, \sigma(\mathcal{U})) = (\mathcal{C}, \mathbf{B}(\mathcal{C}))$ is a standard Borel space, and $f : (\mathcal{C}, \sigma(\mathcal{U})) \to (\mathcal{C}, \sigma(\mathcal{A}))$ is a Borel isomorphism, it follows that $(\mathcal{C}, \sigma(\mathcal{A}))$ is also a standard Borel space. The two standard Borel spaces are different, since $A \in \sigma(\mathcal{A})$, but $A \notin \mathbf{B}(\mathcal{C})$. By Theorem 3, the two $\sigma$-algebras are incomparable, so $\mathbf{B}(\mathcal{C}) \nsubseteq \sigma(\mathcal{A})$. □

## 3.6 UNIQUENESS AND VERBAL SETS

While it is unclear if Mackey's theorem can be extended to apply to analytic sets, we prove other Mackey-type results that work with analytic sets. These theorems work even with 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 compact, connected, simple Lie groups (such as $SO(3, \mathbb{R})$) 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 $x \in N \subseteq V$ for some $N \in \mathcal{N}$.

**Theorem 21.** *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 topology on $G$, potentially different from $\tau$. Consider the identity map $\mathrm{id} : (G, \sigma) \to (G, \tau)$. We will show that id is continuous, so that $\tau \subseteq \sigma$. Then by Theorem 6, the topologies $\tau$ and $\sigma$ are equal. By Theorem 5, it is sufficient to show that the map 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 $\mathcal{N}$:

$$V = \bigcup_{n=1}^{\infty} A_n,$$

with $A_n \in \mathcal{N}$ for $n \geq 1$. Since each $A_n$ has the Baire property in $(G, \sigma)$, it follows that their (countable) union also has the Baire property. So, $\mathrm{id}^{-1}(V) = V$ has the Baire property in $(G, \sigma)$. So id is Baire measurable, as required. □

**Theorem 22.** *Let $G$ be a Polish group with a neighborhood base at the identity consisting 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 consisting of sets from the $\sigma$-algebra generated by identity and verbal sets, then $G$ has a unique Polish group topology.*

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

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

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 $B \in \mathcal{B}$ 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 $x \in dB \subseteq U$. First,

$$\begin{aligned} d \in xW \subseteq xW^{-1}W &\implies x^{-1}d \in W^{-1}W \\ &\implies d^{-1}x \in W^{-1}W \subseteq B \\ &\implies x \in dB. \end{aligned}$$

Also,

$$dB \subseteq (xB)B \subseteq xV^2 \subseteq x(x^{-1}U) = U.$$

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 21, $G$ has a unique Polish group topology. □

### 3.7 LOCALLY COMPACT SEPARABLE METRIZABLE GROUP TOPOLOGY

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

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

**Theorem 23.** *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, metrizable group topology.*

*Proof.* Suppose $G$ has a locally compact, separable, metrizable group topology $\tau$. Then $(G, \tau)$ is a $\sigma$-compact Polish group. Then all identity and verbal sets in $G$ are Borel in $(G, \tau)$. We already know that identity sets are always Borel. Let $V = \{w(\mathbf{g}; \mathbf{a}) \mid \mathbf{g} \in G^n\}$, where $\mathbf{a} \in G^m$ 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 $(G, \tau)$, so verbal sets are indeed Borel. Let $\mathcal{C}$ be a countable point-separating family of sets from the $\sigma$-algebra of identity and verbal sets. Then by Theorem 7, $\mathbf{B}(G, \tau) = \sigma(\mathcal{C})$. Suppose $\tau'$ is another locally compact, separable, metrizable group topology on $G$. Then, by repeating the same argument, $\mathbf{B}(G, \tau') = \sigma(\mathcal{C})$. It follows that $\mathbf{B}(G, \tau) = \mathbf{B}(G, \tau')$. Thus the identity group isomorphism id between the Polish groups $(G, \tau)$ and $(G, \tau')$ is Borel. By Theorem 5, id is a homeomorphism. So $\tau = \tau'$. □

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

Theorem 23 applies to show the uniqueness of the locally compact, separable, metrizable group topology in compact, connected, simple Lie groups. This result was obtained independently by Kallman [16]. (Note that Kallman's result also refers to locally compact topologies, 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.

## 3.8 SEPARATING GROUP

A useful concept in the theory of automatic continuity in Banach algebras [6] is that of a *separating space*, which measures the discontinuity of a linear map. In [15] Johnson shows that the separating space of an epimorphism of Banach algebras is always contained in the radical of the codomain (see also [6], p. 599). As a consequence, if the codomain is semisimple, the epimorphism is automatically continuous. A further consequence is Johnson's famous Uniqueness-of-Norm Theorem: every semisimple Banach algebra has a unique complete norm.

We translate the notion of the separating space into the framework of metrizable groups in order to study the automatic continuity between Polish groups and the uniqueness of the Polish group topology. We give a definition and prove several properties of the *separating group* of a group homomorphism, but at the moment we do not pursue these ideas 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

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

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

**Lemma 24.** *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 $U \in \mathcal{N}_G$ and $V \in \mathcal{N}_H$. 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 $\nu \geq \lambda, \mu$, we have $\phi(x_\nu) \in yV \cap \phi(U)$.

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. □

**Lemma 25.** *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 $xy, x^{-1} \in S(\phi)$. □

Since $S(\phi)$ is always a subgroup of $H$, we also call it the *separating group* of $\phi$.

**Lemma 26.** *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, $hyh^{-1} \in S(\phi)$, and $S(\phi)$ is normal in $H$. □

**Lemma 27.** *Let $G$ and $H$ be Polish 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 $\phi$, $\phi(x_n) \to \phi(1_G) = 1_H$, and so by the uniqueness of limits, $y = 1_H$.

Conversely, suppose $S(\phi) = \{1_H\}$. Then the graph $\Gamma = \{(g, \phi(g)) \mid g \in G\}$ is a closed subgroup of $G \times H$, and hence a Polish group. The restriction $p_G : \Gamma \to G$ of the projection $\pi_G : G \times H \to G$ is a continuous abstract group isomorphism of $\Gamma$ and $G$. By Theorem 5, $p_G$ is a homeomorphism. To see that $\phi$ is continuous, note that for every open set $V$ in $H$, $\phi^{-1}(V) = p_G((G \times V) \cap \Gamma)$ is open in $G$. □

# 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 $\mathbb{N}$.

It is known that the natural topology on $S_\infty$ described above is the only Polish group topology on it [17, 19]. The uniqueness of the Polish group topology on $S_\infty$ also follows from the stronger property (AC) that homomorphisms from $S_\infty$ into arbitrary Polish groups are automatically continuous [22].

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 18).

**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 $\mathbb{N}$,

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

denotes the permutation that maps each $a_i$ to $a_{i+1}$ and is otherwise the identity. We call such a permutation an *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 *finitely many* distinct points $a_1, \ldots, a_k$, it will be convenient to write $\pi \supset (\cdots a_1\, a_2 \cdots a_k \cdots)$, to mean $\pi(a_i) = a_{i+1}$, for each $i = 1, \ldots, k-1$. We emphasize 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:

$$\tau C(a\, b) = \{\pi \in S_\infty \mid \tau^{-1}\pi(a\, b)\pi^{-1}\tau(a\, b)^{-1} = 1\}.$$

**Lemma 28.** *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 $b$.*

*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. □

**Lemma 29.** *The family*

$$\mathcal{C} = \{\tau C(a\, b) \mid \tau \textit{ is a } 2\textit{-cycle or a } 3\textit{-cycle}, a, b \in \mathbb{N}\}$$

*$T_0$-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 $\pi(1) = 2$.

(a) 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:

(i) $\sigma(1) = 1$: $\quad \sigma \supset (1)$;

(ii) $\sigma(1) = 3, \sigma(3) = 1$: $\quad \sigma \supset (1\,3)$;

(iii) $\sigma(1) = 3, \sigma(3) = 2$: $\quad \sigma \supset (\cdots 1\,3\,2 \cdots)$;

(iv) $\sigma(1) = 3, \sigma(3) \neq 1, 3$, say, $\sigma(3) = 4$: $\quad \sigma \supset (\cdots 1\,3\,4 \cdots)$;

(v) $\sigma(1) \neq 1, 3$, say $\sigma(1) = 4$: $\quad \sigma \supset (\cdots 1\,4 \cdots)$.

In each of the cases, using Lemma 28, we find an element of the family $\mathcal{C}$ that $T_0$-separates $\pi$ and $\sigma$:

(i) $(1\,3)C(1\,2)$, because $(1\,3)\pi \supset (1\,2)$, while $(1\,3)\sigma \supset (\cdots 1\,3 \cdots)$;

(ii) $C(1\,3)$, because $\pi \supset (\cdots 1\,2\,3 \cdots)$, while $\sigma \supset (1\,3)$;

(iii) $(1\,3)C(1\,2)$, because $(1\,3)\pi \supset (1\,2)$, while $(1\,3)\sigma \supset (1)(\cdots 3\,2 \cdots)$;

(iv) $(1\,4)C(1\,3)$, because $(1\,4)\pi \supset (\cdots 1\,2\,3 \cdots)$, while $(1\,4)\sigma \supset (1\,3)$;

(v) $(1\,3)C(1\,2)$, because $(1\,3)\pi \supset (1\,2)$, while $(1\,3)\sigma \supset (\cdots 1\,4 \cdots)$.

(b) 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 $\sigma(2) = 2$:

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

(i) Case $\pi(3) \neq \sigma(3)$: Either $\pi(3) \neq 3$, or $\sigma(3) \neq 3$. If $\pi(3) \neq 3$, say $\pi(3) = 4$, by repeating the above argument with 3 and 4 in place of 1 and 2 respectively, 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 $(1\,2\,3)\sigma \supset (1\,2\,3\,4)$.

(ii) 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 30.** *$S_\infty$ admits a unique Polish group topology.*

*Proof.* The family $\mathcal{C}$ from Lemma 29 is a countable $T_0$-separating family of identity sets. By Corollary 18 the Polish group topology on $S_\infty$ is unique. □

## 4.2 COMPACT LIE GROUPS

In this section we give an application of Theorem 22 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 I discovered a paper by Kallman [18] in which he proves a stronger result that all compact, connected metrizable 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 [26]. 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 [12]. 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 $E \times F$.

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 [5], p. 1234, where this set is studied and used to prove van der Waerden's Continuity Theorem [33]: Every homomorphism from a compact, connected, simple Lie group with trivial center into a compact topological group is continuous. Lemmas 31 and 32 below, which state important properties of the set $M(a)$, are taken from the same source.

**Lemma 31.** *Let $K$ be a compact metrizable topological group and let $(a_n)$ be a sequence in $K$ such that $a_n \longrightarrow 1$. Then for every (open) neighborhood $V$ of the identity, there is $n$ such that $M(a_n) \subseteq V$.*

**Lemma 32.** *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 [5], as a part of the proof of van der Waerden's theorem. While Lemma 31 is elementary, Lemma 32 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 $T \leftrightarrow [T]_{\mathcal{B}}$, where $T \in \mathcal{L}(\mathbb{R}^3)$ is a rotation of $S^2$, $\mathcal{B}$ is a fixed orthonormal basis of $\mathbb{R}^3$ and $[T]_{\mathcal{B}}$ denotes the matrix of $T$ with respect to the basis $\mathcal{B}$. Then, for $A_n, A \in SO(3, \mathbb{R})$, $A_n \longrightarrow A$ 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 axis $a$ and angle $\alpha$.

**Lemma 33.** *(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 $P \in SO(3, \mathbb{R})$, by 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

$$C = P^{-1}AP = P^{-1}PA = A,$$

which is 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 $\mathrm{Rot}(\theta)$, $\theta \in [0, \pi]$, the conjugacy class of rotations by angle $\theta$.

*Proof of Lemma 32 in case $G = SO(3, \mathbb{R})$.* By Lemma 33 (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

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

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 33 (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 part (a) of Lemma 33, it follows that $\mathrm{Rot}(\theta)$ is the conjugacy class of $P_{t_\theta}$. So,

$$\begin{aligned} U &= \bigcup_{\theta\in[0,\gamma)} \mathrm{Rot}(\theta) \\ &= \bigcup_{\theta\in[0,\gamma)} \{CP_{t_\theta}C^{-1} \mid C \in SO(3,\mathbb{R})\} \\ &= \{CB_{t_\theta}AB_{t_\theta}^{-1}A^{-1}C^{-1} \mid \theta \in [0,\gamma), C \in SO(3,\mathbb{R})\}, \end{aligned}$$

so $U \subseteq M(A)$. □

**Theorem 34.** *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 32. 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 31, there exists $n$ such that $M(a_n) \subseteq V$. Write $a = a_n$. Then $N(a) \subseteq V^m \subseteq U$.

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 22. □

**Remark 1.** The requirement that $G$ be simple in Theorem 34 is necessary. For example, the circle group $\mathbb{T} = \mathbb{R}/\mathbb{Z}$ is a compact, connected Lie group, which is not simple, and it does not have a unique Polish group topology. To see this, we construct a discontinuous automorphism of $\mathbb{T}$ and appeal to Lemma 11. Consider $\mathbb{R}$ as a vector space over $\mathbb{Q}$. Extend the set $\{1, \pi\}$ to a Hamel basis $B$ and define a linear map $g$ on the basis by letting $g(1) = 1$, $g(\pi) = 2\pi$, and $g(b) = b$ for all other $b \in B$. Define $f : \mathbb{T} \to \mathbb{T}$ by $f(x\mathbb{Z}) = g(x)\mathbb{Z}$. Then $f$ is a (well-defined) discontinuous automorphism of $\mathbb{T}$.

**Remark 2.** It is worth noting here that the uniqueness result of Theorem 34 could not be obtained by applying Mackey's theorem with identity sets: we show in Corollary 36 below that it is not possible to find a countable point-separating family of identity sets.

**Lemma 35.** *If $G$ is a connected Lie group, then 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 $f(x) = w(x; a_1, \ldots, a_m)$, for some free word $w$ and some fixed elements $a_1, \ldots, a_m$ in $G$. Suppose that $A$ is not nowhere dense. Then $A$ contains a nonempty 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 [30], $f$ 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 $G$ containing $U$. Since $G$ is connected, $f = g$. It follows that $A = G$. □

**Corollary 36.** *If $G$ is a connected Lie group, no countable family of identity sets separates points in $G$.*

*Proof.* Suppose $\mathcal{A}$ is a countable family of identity sets that separate points in $G$. Assume, without loss of generality, that $G \notin \mathcal{A}$. Then $\mathcal{A}$ is a countable cover of $G$ by closed nowhere dense sets, which contradicts the Baire Category Theorem. □

### 4.3 PROFINITE GROUPS

In this section we give an application of Theorem 22 to finitely generated profinite groups.

A *profinite group* is a compact, Hausdorff, zero-dimensional topological group, or equivalently a compact Hausdorff group whose open 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 proved that every (topologically) finitely generated pro-$p$ group has the finite index property , see [31], or [14], p. 25. 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 [27].

A free word $w$ is said to be *$d$-locally finite* if every $d$-generator (abstract) group $H$ satisfying $w(H) = \{1\}$ is necessarily finite. Lemmas 37 and 38 below are key results from [27], we include the proof of the latter as it is not explicitly stated.

**Lemma 37.** *Let $w$ be a $d$-locally finite free word and let $G$ be a $d$-generator profinite group. Then the verbal subgroup $w(G)$ is open in $G$.*

**Lemma 38.** *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 $w_i(\mathbf{u}) \in D$ for each $i$ and any $\mathbf{u} \in F^d$. Thus, setting

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

where $\mathbf{y_1}, \ldots, \mathbf{y_m}$ are disjoint $d$-tuples of variables, we have $w(F) = D$. We show that the free word $w$ is $d$-locally finite. 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 $w(F) \subseteq K$. But now $K$ has finite index in $F$ because it contains $w(F) = D$ which has finite index in $F$. So $H = F/K$ is finite, as required. Also, $w(G) \subseteq N$, since $w_i(\mathbf{g}) \in N$ for each $i$ and any $\mathbf{g} \in G^d$. By Lemma 37, $w(G)$ is an open verbal subgroup of $G$ contained in $N$. □

**Theorem 39.** *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 38, each open normal subgroup contains an open verbal subgroup. Thus, $G$ has a neighborhood base at the identity of verbal subgroups, which are analytic in any Polish group topology on $G$, by Lemma 17. By Theorem 22, $G$ has a unique Polish group topology. □

**Remark.** The requirement that $G$ be finitely generated is indispensable. An example of a profinite group that does not have a unique Polish group topology is $G = \mathbb{Z}_2^\omega$. Of course, $\mathbb{Z}_2^\omega$ is not finitely generated. One Polish group topology on $G$ is the usual product topology, where each $\mathbb{Z}_2$ is given the discrete topology. We now construct a different Polish group topology on $G$. Let $p$ be a non-principal ultra-filter on $\omega$. Then $H := \{\chi_{A^C} \mid A \in p\}$ is a subgroup of $G$ of index 2. Further, since $p$ is non-principal, $H$ is dense in $G$, and so it is not closed. Group $H$ is isomorphic (as an abstract group) to $\mathbb{Z}_2^\omega$, since both groups are the unique free Boolean group with $2^{\aleph_0}$ elements. Give $H$ the product topology of $\mathbb{Z}_2^\omega$. Now $G$ is isomorphic (as an abstract group) to $H \times \mathbb{Z}_2$ via the map $\phi : G = H \cup (a + H) \to H \times \mathbb{Z}_2$, given by $\phi(h) = (h, 0)$, $\phi(a + h) = (h, 1)$, for $h \in H$, where $a$ is some fixed element of the coset $G \setminus H$. Give $G$ the topology of the Polish group $H \times \mathbb{Z}_2$. This new Polish group topology on $G$ is different from the first one because in the new topology $H$ is closed in $G$.

# 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 understanding the problem of the uniqueness of a topology of a given type on a topological group. In particular, it is important to understand which algebraically definable sets are Borel.

Identity sets are of course always closed. On the other hand, all that one can say about a general verbal set (in a Polish group) with certainty is that it is necessarily analytic. It is not clear if verbal sets might always be Borel.

In this chapter we investigate the complexity of verbal sets in various Polish groups. In many situations we will be able to show that verbal sets are Borel. However, the most interesting results for us are those of Sections 5.4 and 5.5, where we exhibit examples of verbal sets that are complete analytic, and hence not Borel. These results establish that not all verbal sets are Borel.

**Definitions and Notation.** For reader's convenience, we repeat some of the definitions from Section 4.1. 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 $\sigma_1, \dots, \sigma_k$, we also say that $f$ *contains* the product $\sigma_1 \cdots \sigma_k$.

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

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

not be confused with $G^n$, which, as usual, will stand for the Cartesian product $\underbrace{G \times \cdots \times G}_{n}$.

## 5.1 ABELIAN GROUPS

We show that in Abelian Polish groups verbal sets are necessarily Borel.

**Theorem 40.** *Let $(G, +)$ be an Abelian Polish group, $w(x_1, \dots, x_n, y_1, \dots, y_m)$ a free word, and $c_1, \dots, c_m$ constants in $G$. Then the verbal set $V = \{w(g_1, \dots, g_n; c_1, \dots, c_m) \mid g_1, \dots, g_n \in G\}$ is Borel in $G$.*

*Proof.* Since $G$ is Abelian, $w(g_1, \dots, g_n; c_1, \dots, c_m)$ can be written in the form

$$w(g_1, \dots, g_n; c_1, \dots, c_m) = \alpha_1 g_1 + \cdots + \alpha_n g_n + \beta_1 c_1 + \cdots + \beta_m c_m,$$

for some $\alpha_i, \beta_j \in \mathbb{Z}$. Let $c$ be the constant $c := \beta_1 c_1 + \cdots + \beta_m c_m \in G$, so that

$$w(g_1, \dots, g_n; c_1, \dots, c_m) = \alpha_1 g_1 + \cdots + \alpha_n g_n + c.$$

Consider the map $\phi : G^n \to G$, defined by $\phi(g_1, \dots, g_n) = \alpha_1 g_1 + \cdots + \alpha_n g_n$. 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 $(\mathbf{g}, h) \mapsto \mathbf{g}.h := \phi(\mathbf{g}) + h$, for $\mathbf{g} \in G^n, h \in G$. By the properties of $\phi$, this is a well-defined continuous action of $G^n$ on $G$. By Theorem 9, the orbits of this action are Borel. In particular, the orbit of the element $c$: $\{\mathbf{g}.c \mid \mathbf{g} \in G^n\} = \{\phi(\mathbf{g}) + c \mid \mathbf{g} \in G^n\} = V$, 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 41.** *Full verbal sets in $S_\infty$ are Borel.*

To prove this, we first appeal to [7] where it is shown that if $w(x_1, \ldots, x_n)$ is a free word that is not a proper power, then the full 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 42 we give a necessary and sufficient condition for a permutation in $S_\infty$ to be a square. We use this characterization in Theorem 44 to prove that $S_\infty^{(2)}$ is Borel.

**Theorem 42** (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 analyze 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 $n$, the $2n$-cycles appear in pairs (as in (b)), while the $(2n+1)$-cycles may occur either in pairs (as in (c)) or alone (as in (d)). Thus, if $\pi \in S_\infty^{(2)}$, then the number of $2n$-cycles in $\pi$ for $1 \leq n \leq \infty$ must be 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 43.** *For all $k = 1, 2, \ldots$ and $n = 1, 2, \ldots$ or $n = \infty$, the set*

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

*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 clearly clopen in $S_\infty$, because 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 $m = 2, 3, \ldots$

$$\begin{aligned} V(a, b; m) &= \{\pi \mid \exists b_2, \ldots, b_m \in \mathbb{N}, \pi(a) = b_2, \pi(b_2) = b_3, \ldots, \pi(b_m) = b\} \\ &= \bigcup_{b_2, \ldots, b_m \in \mathbb{N}} U(a, b_2, \ldots, b_m, b). \end{aligned}$$

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

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

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

$$\begin{aligned} W(a_1; n) &= \{\pi \mid \exists b_2, \ldots, b_n \in \mathbb{N} \text{ such that } \pi \text{ contains } (a_1\ b_2\ \cdots b_n)\} \\ &= \bigcup_{b_2, \ldots, b_n \in \mathbb{N}} U(a_1, b_2, \ldots, b_n, a_1), \end{aligned}$$

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

$$\begin{aligned} W(a_1; \infty) &= \{\pi \mid \pi \text{ contains a cycle } (\cdots a_1 \cdots) \text{ of infinite length}\} \\ &= \{\pi \mid \forall m = 1, 2, \ldots, \pi \text{ does not contain } (\underbrace{\cdots a_1 \cdots}_{m})\} \\ &= \bigcap_{m \geq 1} (S_\infty \setminus W(a_1; m)). \end{aligned}$$

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

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

is Borel in $S_\infty$. We have already shown this set is Borel in the case $k = 1$. For $k > 1$ and $1 \le n \le \infty$, $W(a_1, \dots, a_k; n)$ is Borel ($F_\sigma$ and $G_\delta$) because

$$\begin{aligned} W(a_1,\dots,a_k;n) &= \{\pi \mid \forall i = 1,\dots,k,\ \ \pi \text{ contains } (\underbrace{\cdots a_i \cdots}_{n}) \text{ and} \\ &\quad \forall i \neq j \text{ in } \{1,\dots,k\},\ \ \text{the cycles containing } a_i \text{ and } a_j \text{ are distinct}\} \\ &= \bigcap_{1\le i\le k} \{\pi \mid \pi \text{ contains } (\underbrace{\cdots a_i \cdots}_{n})\} \ \cap \\ &\quad \cap \bigcap_{1\le i\le j\le k} \{\pi \mid \forall m = 1,2,\dots \ \ \pi^m(a_i) \neq a_j \text{ and } \pi^m(a_j) \neq a_i\} \\ &= \bigcap_{1\le i\le k} W(a_i;n) \cap \bigcap_{\substack{1\le i\le j\le k \\ m\ge 1}} (S_\infty \setminus (V(a_i,a_j;m) \cup V(a_j,a_i;m))). \end{aligned}$$

Finally, for $k = 1, 2, \dots$ and $1 \le n \le \infty$,

$$\begin{aligned} B(k;n) &= \{\pi \mid \exists a_1,\dots,a_k \in \mathbb{N} \text{ such that } \pi \text{ contains } (\underbrace{\cdots a_1 \cdots}_{n}) \cdots (\underbrace{\cdots a_k \cdots}_{n})\} \\ &= \bigcup_{a_1,\dots,a_k \in \mathbb{N}} W(a_1,\dots,a_k;n). \end{aligned}$$

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

**Theorem 44.** *The set $S_\infty^{(2)}$ of squares in $S_\infty$ is Borel ($F_{\sigma\delta}$).*

*Proof.* Using the characterization of the square permutations given in Theorem 42, we express $S_\infty^{(2)}$ as a Boolean combination of sets previously shown to be Borel:

$$\begin{aligned} S_\infty^{(2)} &= \{\pi \in S_\infty \mid \text{for all } 1 \le n \le \infty \text{ and for all } k \ge 1, \text{ if } \pi \text{ has } 2k-1 \text{ cycles} \\ &\quad \text{of length } 2n, \text{ then it has } 2k \text{ cycles of length } 2n\} \\ &= \bigcap_{n,k} (\{\pi \mid \pi \text{ does not have } 2k-1\ 2n\text{-cycles}\} \cup \{\pi \mid \pi \text{ has } 2k\ 2n\text{-cycles}\}) \\ &= \bigcap_{n,k} ((S_\infty \setminus B(2k-1;2n)) \cup B(2k;2n)). \end{aligned}$$

So by Lemma 43, the set $S_\infty^{(2)}$ is Borel ($F_{\sigma\delta}$). □

### 5.2.2 Set of $m$-th Powers

Consider now the set $S_\infty^{(m)}$ of all $m$-th powers in $S_\infty$, where $m \geq 1$. We will characterize the elements of this set (Theorem 46), and then show that it is Borel (Theorem 47).

**Lemma 45.** *(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 $k = (1 + jm) \bmod N$, for some $j = 0, 1, 2, \ldots$ (Here, $s \bmod N$ 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 $(1 + jm) \bmod N$. In other words, the length of the cycle containing $a_1$ is precisely $x$. Now, $1 + xm \equiv 1 (\bmod\ N)$ 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. □

**Theorem 46** (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) $\pi \in S_\infty^{(m)}$,*

*(ii) For every $1 \leq n \leq \infty$ the number of $p_i n$-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 $\pi \in S_\infty^{(m)}$ and let $\rho \in S_\infty$ be such that $\pi = \rho^m$.

Let $n \in \{1, 2, \ldots\}$. By Lemma 45, cycles of a given length in $\pi$ appear in groupings of equal size, more precisely: if $\pi$ contains a cycle of length $p_i n$, then there exist $k \geq 1$, disjoint $p_i n$-cycles $\sigma_2, \ldots, \sigma_k$ in $\pi$, and a $p_i nk$-cycle $\sigma$ in $\rho$ such that

$$\sigma^m = \sigma_1 \sigma_2 \cdots \sigma_k$$

and

$$(m, p_i nk) = k.$$

Writing $m = p_i^{\alpha_i} m_1$, $n = p_i^{\beta_i} n_1$, and $k = p_i^{\gamma_i} k_1$, where $(m_1, p_i) = (n_1, p_i) = (k_1, p_i) = 1$, we get

$$(p_i^{\alpha_i} m_1, p_i^{1+\beta_i+\gamma_i} n_1 k_1) = p_i^{\gamma_i} k_1.$$

It follows that $\gamma_i = \min(\alpha_i, 1 + \beta_i + \gamma_i)$, so $\gamma_i = \alpha_i$. Thus, $k$ is divisible by $p^{\alpha_i}$. We conclude that the number of $p_i n$-cycles in $\pi$ is divisible by $p_i^{\alpha_i}$ (possibly infinite).

If $n = \infty$, and $\sigma_1$ is an infinite cycle in $\pi$, then by Lemma 45, there exist disjoint infinite cycles $\sigma_2, \ldots, \sigma_m$ in $\pi$ and an infinite cycle $\sigma$ in $\rho$ such that

$$\sigma^m = \sigma_1 \sigma_2 \cdots \sigma_m.$$

Thus, the number of infinite cycles in $\pi$ is divisible by $m$.

Conversely, let $\pi$ be a permutation in $S_\infty$ satisfying (ii). We will construct a permutation $\rho$ such that $\rho^m = \pi$.

Fix $1 \leq l \leq \infty$. By (ii), the number of cycles in $\pi$ of length $l$ is divisible by $p_i^{\alpha_i}$, for each $i$ with $p_i | l$. Thus, the number of $l$-cycles in $\pi$ is divisible by

$$d := \prod_{p_i | l} p_i^{\alpha_i}$$

(possibly infinite). Let

$$N := dl \quad (N = \infty \text{ if } l = \infty).$$

Note that for finite $l$, $d = (N, m)$. For $l = \infty$, $d = \prod_{i=1}^{s} p_i^{\alpha_i} = m$.

Divide the cycles of length $l$ in $\pi$ into pairwise disjoint groupings of $d$-many. Let $\sigma_1, \sigma_2, \ldots, \sigma_d$ be one such grouping of $l$-cycles in $\pi$. By Lemma 45, 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 $l$, $1 \le l \le \infty$, and each grouping of $l$-cycles in $\pi$, we complete the construction of $\rho$. It is clear by design that $\rho^m = \pi$. □

**Theorem 47.** *For all $m \geq 1$, the set $S_\infty^{(m)}$ of $m$-th powers in $S_\infty$ is Borel ($F_{\sigma\delta}$).*

*Proof.* Let $m = \prod_{i=1}^{s} p_i^{\alpha_i}$, $\alpha_i > 0$, be the unique prime factorization of $m$. By Theorem 46, a permutation $\pi$ is in $S_\infty^{(m)}$ 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,

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

where $B(k; n)$ denotes the set of permutations that have (at least) $k$ cycles of length $n$. By Lemma 43, it follows that $S_\infty^{(m)}$ is Borel ($F_{\sigma\delta}$). □

## 5.3 AUTOHOMEOMORPHISM GROUP OF THE UNIT INTERVAL

Let $Homeo(I)$ denote the group of autohomeomorphisms of the (closed) unit interval $I$. With the topology of uniform convergence, $Homeo(I)$ is a Polish group. We will show that the set of squares

$$Homeo(I)^{(2)} = \{f^2 = f \circ f \mid f \in Homeo(I)\}$$

is Borel (clopen).

Let $Homeo(I)$ be the set of order-preserving (increasing) homeomorphisms of $I$:

$$Homeo^+(I) = \{f \in Homeo(I) \mid \forall x, y \in I, \;\; x < y \Rightarrow f(x) < f(y)\},$$

and $Homeo^-(I)$ the set of order-reversing ones. Then $Homeo^+(I)$ is a clopen subgroup of $Homeo(I)$ of index 2 whose other coset is $Homeo^-(I)$.

We will show that $Homeo(I)^{(2)} = Homeo^{+}(I)$, 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 [9]. 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 $Homeo(J)$ and $Homeo^{+}(J)$ denote the homeomorphisms and the order-preserving homeomorphisms of $J$, respectively. Further, let

$$K(J) = \{f \in Homeo^{+}(J) \mid \forall x \in J^{\circ}, f(x) > x\},$$

$$L(J) = \{f \in Homeo^{+}(J) \mid \forall x \in J^{\circ}, f(x) < x\}.$$

**Lemma 48.** *(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 part (a); the proof of 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 3):

$$\begin{aligned} a_{0,0} &:= \tfrac{1}{2}, \\ a_{n,0} &:= f^n(a_{0,0}), \\ a_{0,r} &:= a_{0,0} + r(a_{1,0} - a_{0,0}), \\ a_{n,r} &:= f^n(a_{0,r}). \end{aligned}$$

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 $x = a_{n,r}$.

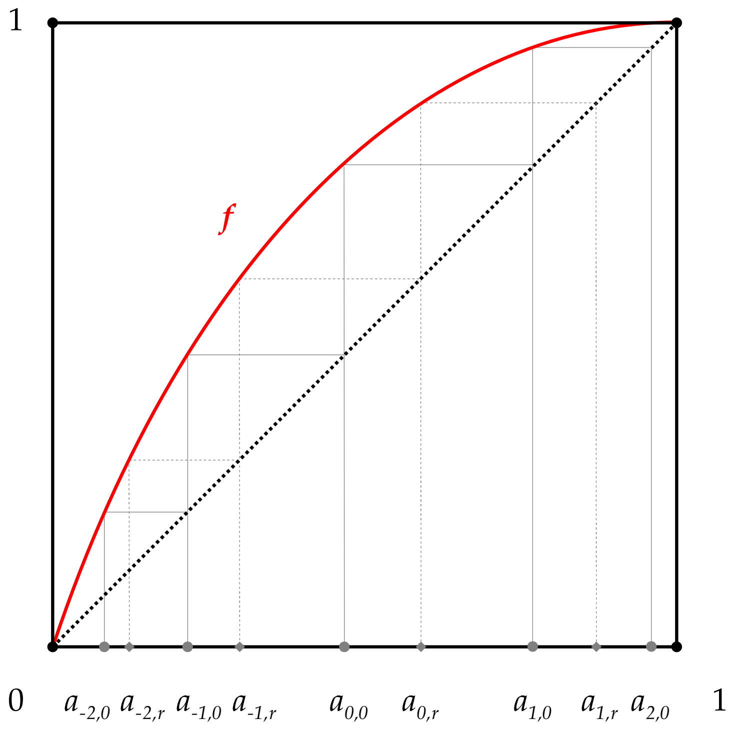

Figure 3: Constructing a square root: Sequence $(a_{n,r})$.

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

$$\prod_{r\in[0,1)} (\cdots \ a_{-1,r} \ \ a_{0,r} \ \ a_{1,r} \ \ a_{2,r} \ \cdots).$$

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 $g \in K(I)$. □

**Lemma 49.** *For every $f \in Homeo^+(I)$, there exists $g \in Homeo^+(I)$ such that $f = g^2$.*

*Proof.* Given $f \in Homeo^+(I)$, let $\{I_\lambda\}$ be the set of all maximal subintervals of $I$ on which the function $f(x) - x$ does not change sign. Let $J_\lambda$ be the closure of $I_\lambda$: $J_\lambda = \overline{I_\lambda}$. Then by Lemma 48, for each $\lambda$ there exists $g_\lambda \in Homeo(J_\lambda)$ such that $f \upharpoonright J_\lambda = g_\lambda^2$. 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 $g \in Homeo^+(I)$ and $f = g^2$. □

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

**Theorem 50.** *The set $Homeo(I)^{(2)}$ of the squares in $Homeo(I)$ is Borel.*

## 5.4 AUTOHOMEOMORPHISM GROUP OF THE UNIT CIRCLE

Note that the material of this section can be found in [8].

Let $Homeo(S^1)$ be the group of autohomeomorphisms of the unit circle $S^1$. Equipped with the topology of uniform convergence, it is a Polish group. In this section we investigate the complexity of the set

$$Homeo(S^1)^{(2)} = \{f^2 = f \circ f \mid f \in Homeo(S^1)\}$$

of squares in $Homeo(S^1)$.

We have seen in Section 5.3 that the set of squares in the autohomeomorphism group $Homeo(I)$ 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 $Homeo(S^1)$ is (analytic but) not Borel. In fact, it is complete analytic.

The result that the squares in $Homeo(I)$ 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 and Laczkovich showed in [13] 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 $Homeo(S^1)$ are complete analytic, we focus on the structure of the set of fixed points.

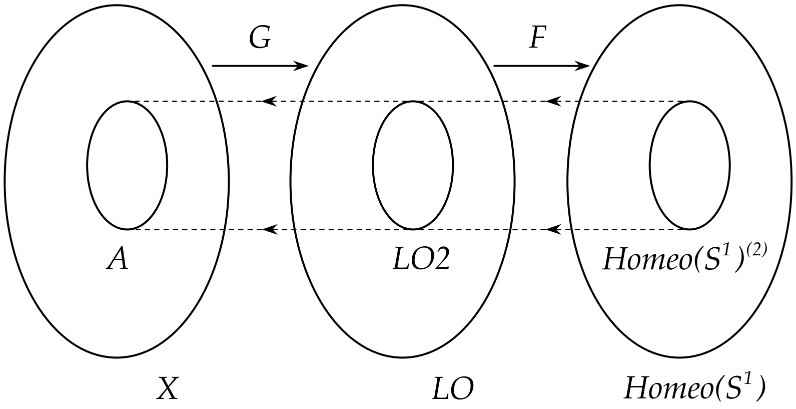

Figure 4: Showing the completeness of an analytic set.

A standard technique for showing completeness of an analytic set is to reduce an already known complete analytic set to the given set (see Figure 4). Beleznay in [2] showed that the set $LO2$ of linear orders of type $I + I$ (precise definition follows) is complete analytic. To show that $Homeo(S^1)^{(2)}$ is complete, we construct in Lemma 53 a continuous reduction $F$ of $LO2$ to $Homeo(S^1)^{(2)}$. Since $LO2$ 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 $Homeo(S^1)^{(2)}$. This proves that $Homeo(S^1)^{(2)}$ is complete.

We first give in Lemma 52 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 $LO2$ to $Homeo(S^1)^{(2)}$ in Lemma 53.

### 5.4.1 Definitions and Notation

First, we give a definition of the set $LO2$, 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 $LO$ is defined to be the set of those codes $\alpha \in 2^{\mathbb{N}\times\mathbb{N}}$ that code a linear order. $LO$ 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 $LO$, we write $n <_\alpha m$ instead of $\alpha(n,m) = 1$. The set $LO2$ is the collection of codes from $LO$ which code a linear order of the form $I + I$:

$$\begin{aligned} LO2 = \{\alpha \in LO \mid \exists f \in 2^{\mathbb{N}}, g \in \mathbb{N}^{\mathbb{N}} &\text{ such that } g : \mathbb{N} \to \mathbb{N} \text{ is a bijection, and} \\ &\forall n,m \in \mathbb{N},\ \ f(n) = 0 \text{ and } f(m) = 1 \text{ imply } n <_\alpha m, \\ &\forall n \in \mathbb{N},\ \ f(n) = 0 \text{ if and only if } f(g(n)) = 1, \\ &\forall n \in \mathbb{N},\ \ g(g(n)) = n, \\ &\forall n,m \in \mathbb{N},\ \ \text{if } f(n) = f(m) = 0 \ \text{ then } \ n <_\alpha m \text{ iff } g(n) <_\alpha g(m)\}. \end{aligned}$$

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, $LO2$ 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 $x_1, x_2, \dots, x_n$ ($n \geq 3$) in $S^1$, we write $x_1 < x_2 < \cdots < x_n (< x_1)$ if, when traveling counterclockwise along the circle $S^1$ starting from $x_1$, we reach points $x_2, \dots, x_n$ 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 $S^1$.

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

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

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

For $f \in Homeo^{+}(S^1)$ and $a, b \in S^1$, define

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

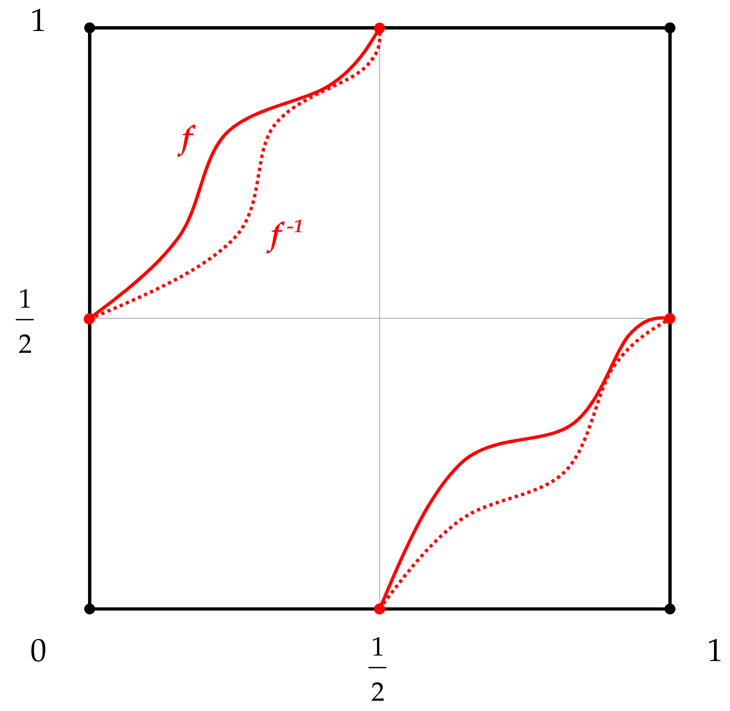

Figure 5: A function in $\mathcal{M}$ and its inverse.

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

$$\begin{aligned}\mathcal{M} = \{f \in Homeo^{+}(S^1) \mid f(0) = \tfrac{1}{2}, f(\tfrac{1}{2}) = 1 = 0,&\\ \forall x \in (0, \tfrac{1}{2}),\ \ 0 < x \leq f^2(x) < \tfrac{1}{2},\ \text{and}&\\ \forall x \in (\tfrac{1}{2}, 1),\ \ \tfrac{1}{2} < x \leq f^2(x) < 1\}.&\end{aligned}$$

The last two conditions in the definition of $\mathcal{M}$ can be rewritten as

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

A typical function in $\mathcal{M}$, together with its inverse, is shown in Figure 5.

### 5.4.2 The Proof

**Lemma 51.** *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 $f \restriction A = g^2$.*

*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 $n + r < m + s$,

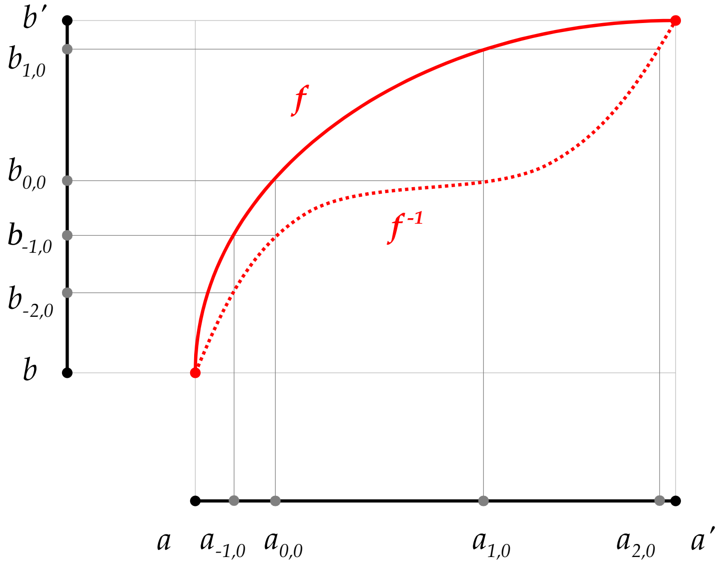

Figure 6: Constructing a square root: Sequences $(a_{n,0})$ and $(b_{n,0})$.

(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 48. Note that in (i) we use the assumption that $f \in \mathcal{M}$ (see Figure 6).

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.

Define $g$ to be the permutation of $A$ given by the following disjoint cycle representation (see Figure 7):

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

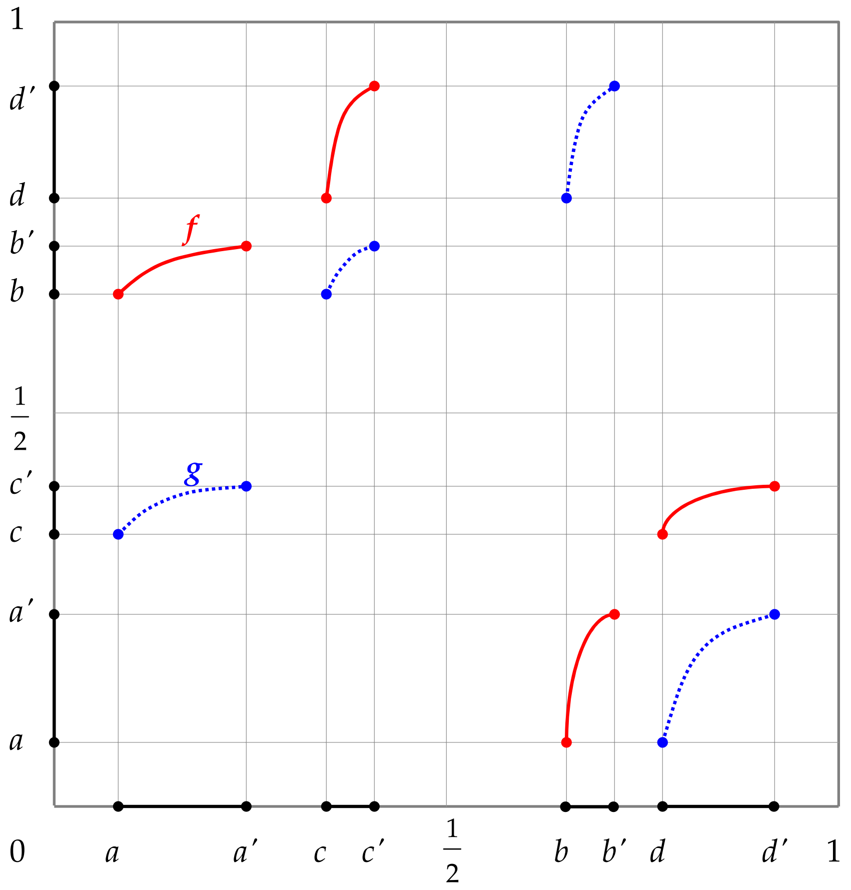

Figure 7: A square root $g$ of $f\restriction A$.

Then clearly $g^2 = f\restriction A$. 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 52** (Characterization of Squares in $\mathcal{M}$)**.** *For a homeomorphism $f \in \mathcal{M}$, the following are equivalent:*

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

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

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

*Proof.* Suppose that $f \in Homeo(S^1)^{(2)}$ and let $g \in Homeo(S^1)$ 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 $g \in Homeo^+(S^1)$. Suppose, for a contradiction, $g \in Homeo^-(S^1)$. 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! The case $0 < \frac{1}{2} < g(0) < 0$ yields a contradiction in a similar way. So $g$ must indeed 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 $\phi = g\restriction[0, c]$. 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

$$\begin{aligned} x \in \phi(D(f\restriction[0,c])) &\iff g^{-1}(x) \in D(f\restriction[0,c]) \\ &\iff f^2(g^{-1}(x)) \neq g^{-1}(x) \\ &\iff g^3(x) \neq g^{-1}(x) \\ &\iff g^4(x) \neq x \\ &\iff f^2(x) \neq x \\ &\iff x \in D(f\restriction[c, \tfrac{1}{2}]) \end{aligned}$$

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

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 $g_K^2 = f\restriction K'$. Set $D(f\restriction[0,c])$ consists of disjoint open intervals. Let $L$ be a component of $D(f\restriction[0,c])$. Let $g_L$ be the order-preserving homeomorphism of $L' = \overline{L} \cup \overline{\phi(L)} \cup \overline{f(L)} \cup \overline{f(\phi(L))}$ such that $f\restriction L' = g_L^2$, constructed in Lemma 51. Define

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

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

**Lemma 53.** *There is a continuous function $F : LO \to \mathcal{M}$ such that*

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

*Proof.* **Construction.** Fix $\alpha \in LO$. We want to define $F(\alpha) \in \mathcal{M}$. 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 $\alpha$ has no smallest element,

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

(d) For any $x \notin \cup_{n\in\mathbb{N}}(p_n, q_n)$, $\sup\{q_n \mid q_n \leq x\} = \inf\{p_n \mid p_n \geq x\}$ 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 $k <_\alpha l$ 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 $(a_m, b_m)$ 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 8.

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

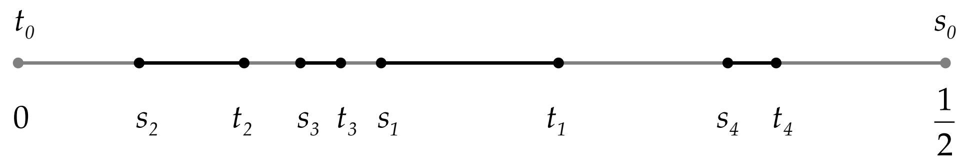

Figure 8: Constructing intervals from a linear order: Intervals $(s_n, t_n)$ for $n = 0, 1, \dots, 4$, when $2 <_\alpha 3 <_\alpha 1 <_\alpha 4$.

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 $F(\alpha)$, see Figure 9. For $x \in S^1 = [0,1]/{\sim}$, let

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

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. 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

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

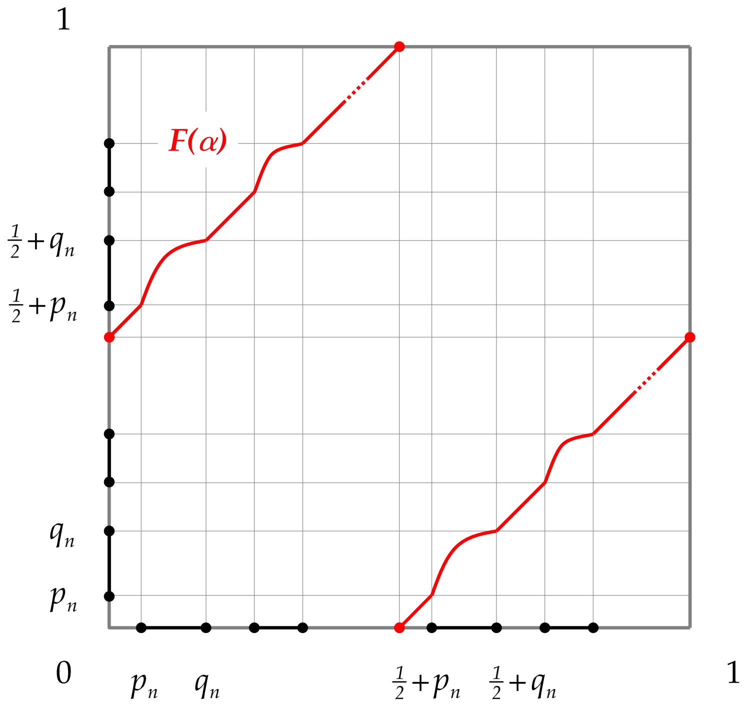

Figure 9: Constructing a continuous reduction: Function $F(\alpha)$.

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,

$$\begin{aligned} d(F(\alpha), F(\beta)) &= \sup\{|F(\alpha)(x) - F(\beta)(x)| \mid x \in S^1\} \\ &= \sup\{|F(\alpha)(x) - F(\beta)(x)| \mid x \in A\}. \end{aligned}$$

If $x \in A$, then $x \in (p_n^\alpha, q_n^\alpha)$ for some $n \geq n_\varepsilon$ 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 $(p^{\beta}_m, q^{\beta}_m)$ only, then

$$|F(\alpha)(x) - F(\beta)(x)| \leq |q^{\beta}_m - p^{\beta}_m| < \varepsilon.$$

Finally, if $x \in (p^{\alpha}_n, q^{\alpha}_n) \cap (p^{\beta}_m, q^{\beta}_m)$, then

$$|F(\alpha)(x) - F(\beta)(x)| \leq \max(|q^{\alpha}_n - p^{\alpha}_n|, |q^{\beta}_m - p^{\beta}_m|) < \varepsilon.$$

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 $F(\alpha) \in Homeo(S^1)^{(2)} \iff \alpha \in LO2$.

Suppose $F(\alpha) \in Homeo(S^1)^{(2)}$. Then by Lemma 52, there exist $c \in (0, \frac{1}{2})$ and an order-preserving homeomorphism $\phi : [0, c] \to [c, \frac{1}{2}]$ such that

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

Then $c \notin U$. For, otherwise, $c \in D(F(\alpha){\restriction}[0, c])$, and so $\phi(c) \in D(F(\alpha){\restriction}[c, \frac{1}{2}])$, 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 $D(F(\alpha){\restriction}[0, \frac{1}{2}]) = U$, 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 52, we need to find a point $c \in (0, \frac{1}{2})$ and an order-preserving homeomorphism $\phi : [0, c] \to [c, \frac{1}{2}]$ with the property $\phi(D(F(\alpha){\restriction}[0, c])) = D(F(\alpha){\restriction}[c, \frac{1}{2}])$.

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 $c < c_2$.

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 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 that $\sup\{q_m \mid q_m \leq z\} = \inf\{p_m \mid p_m \geq z\}$, i.e., $y = z$. Clearly $\phi$ is continuous and order-preserving on $\overline{S}$.

Note that

$$\begin{aligned}
\inf S = 0 \quad &\iff \quad J \text{ has no smallest element (by (b))} \\
&\iff \quad K \text{ has no smallest element} \\
&\iff \quad \inf \tau(S) = c \text{ (by the definition of } c\text{).}
\end{aligned}$$

and

$$\begin{aligned}
\sup S = c \quad &\iff \quad J \text{ has no biggest element (definition of } c\text{)} \\
&\iff \quad K \text{ has no biggest element} \\
&\iff \quad \inf \tau(S) = \tfrac{1}{2} \text{ (by (c)).}
\end{aligned}$$

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

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

**Theorem 54.** *The set of squares $Homeo(S^1)^{(2)}$ in $Homeo(S^1)$ is complete analytic.*

*Proof.* The set $Homeo(S^1)^{(2)}$ is obviously analytic, since $f \mapsto f \circ f$ is continuous. Lemma 53 gives a continuous reduction of $LO2$, a complete analytic set, to $Homeo(S^1)^{(2)}$. By the discussion from the beginning of this section, $Homeo(S^1)^{(2)}$ is complete. □

## 5.5 AUTOMORPHISM GROUP OF THE RATIONAL CIRCLE

An important class of Polish groups is the class of the automorphism groups of countable first-order structures, which are precisely the closed subgroups of $S_\infty$. They are of particular interest to logicians and permutation group theorists (see Section 6.3). It is a natural question to ask if in these Polish groups, as in $S_\infty$, the full verbal sets are necessarily Borel. The answer turns out to be negative: we show here that the set of squares in the automorphism group $Aut(Q, <)$ of the rational circle (definition follows) is complete analytic.

### 5.5.1 Definitions and Notation

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 $t \mapsto e^{2\pi i t}$. 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 counterclockwise 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 $(Q,<)$:

$$Aut(Q,<) = \{\pi \in Sym(Q) \mid \forall x,y,z \in Q,\ x<y<z \Rightarrow \pi(x) < \pi(y) < \pi(z)\}.$$

We give $Aut(Q,<)$ the relative topology as a subspace of the group $Sym(Q)$ of permutations of $Q$ (which is homeomorphic to $S_\infty$). $Aut(Q,<)$ is then a closed subgroup of the Polish group $S_\infty$, and thus a Polish group itself.

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

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

Let $\pi \in Aut(Q,<)$. 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 $\pi$: $\hat{\pi} \in Homeo^+(S^1)$ and $\hat{\pi}\restriction Q = \pi$. Also, if $f \in Homeo^+(S^1)$ and $f(Q) = Q$, then $f\restriction Q \in Aut(Q,<)$ and $\widehat{f\restriction Q} = f$.

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

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

Let $\tau$ be the usual Polish group topology on $Aut(Q,<)$, that is, the relative topology as a subset of $Sym(Q)$. Let $\tau'$ denote the topology on $Aut(Q,<)$ inherited from $Homeo(S^1)$: $\tau' = \{\psi^{-1}(U) \mid U \text{ is open in } Homeo(S^1)\}$. We show that the topologies $\tau$ and $\tau'$ are comparable, but not equal. Thus, by Theorem 6, $\tau'$ 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 $U(\pi,\varepsilon) := \{\sigma \in Aut(Q,<) \mid \sup_{x\in S^1} d(\hat{\sigma}(x),\hat{\pi}(x)) < \varepsilon\}$ 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 $i = 1,\dots,n$. Then $V(\pi,\{x_1,\dots,x_n\}) := \{\sigma \in Aut(Q,<) \mid \sigma(x_i) = \pi(x_i), i = 1,\dots,n\}$ is a basic open set of $\tau$ contained in $U(\pi,\varepsilon)$. To see that $\tau$ is *strictly* finer than $\tau'$, observe that $V(\mathrm{id},\{0\}) = \{\sigma \in Aut(Q,<) \mid \sigma(0) = 0\}$ is an open set in $\tau$, but not open in $\tau'$.

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

Define

$$\begin{aligned}\mathcal{M}(A,B) = \{f \in Homeo^+(S^1) \mid\ & f(A) = B, f(B) = A, \\ & \forall x \in (A,B),\ \ A < x \leq f^2(x) < B, \text{ and} \\ & \forall x \in (B,A),\ \ B < x \leq f^2(x) < A\}.\end{aligned}$$

and

$$\begin{aligned}\mathcal{M}_Q(A,B) = \{\pi \in Aut(Q,<) \mid\ & \hat{\pi}(A) = B, \hat{\pi}(B) = A, \\ & \forall x \in (A,B) \cap Q,\ \ A < x \leq \pi^2(x) < B, \text{ and} \\ & \forall x \in (B,A) \cap Q,\ \ B < x \leq \pi^2(x) < A\}.\end{aligned}$$

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 $f{\restriction}Q \in \mathcal{M}_Q(A,B)$.

### 5.5.2 The Proof

We now show that the set of squares $Aut(Q,<)^{(2)}$ is complete analytic. 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 [21], it is sufficient to find a *Borel* reduction. To show that $Aut(Q,<)^{(2)}$ is complete, we construct in Lemma 58 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 56.

**Lemma 55.** *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*

$$(a\,b)(c\,d)(a'\,b')(c'\,d')$$

*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 $S = [a,a'] \cup [c,c'] \cup [b,b'] \cup [d,d']$. Then there exists an order-preserving homeomorphism $g$ of $S$ such that $g(S \cap Q) = S \cap Q$, $g$ contains*

$$(a\,c\,b\,d)(a'\,c'\,b'\,d')$$

*and $f{\restriction}S = g^2$. Then, $\sigma := g{\restriction}S \cap Q$ is an automorphism of $(S \cap Q,<)$ and $\pi{\restriction}S \cap Q = \sigma^2$.*

*Proof.* The proof is the same as that of Lemma 51, only with $A$ and $B$ in place of 0 and $\frac{1}{2}$, and with $a_{0,0} \in (a,a') \cap Q$, $c_{0,0} \in (c,c') \cap Q$ and $r \in [0,1) \cap \mathbb{Q}$. □

**Lemma 56** (Characterization of Squares in $\mathcal{M}_Q(A,B)$)**.** *For an automorphism $\pi \in \mathcal{M}_Q(A,B)$, the following are equivalent:*

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

*(ii) There exist 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*

$$\phi(D(\hat{\pi}{\restriction}[A,c])) = D(\hat{\pi}{\restriction}[c,B]).$$

*Proof.* Suppose that $\pi \in Aut(Q,<)^{(2)}$ and let $\sigma \in Aut(Q,<)$ 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 52, let $c = g(A)$ and $\phi = g\restriction[A,c]$ if $g(A) \in (A,B)$, or, let $c = g^{-1}(A)$ and $\phi = g^{-1}\restriction[A,c]$ 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 that (ii) holds. We construct $g_K$, $g_L$ and $g$ as in the proof of Lemma 52, except, we replace 0 and $\frac{1}{2}$ by $A$ and $B$ respectively, and we use Lemma 55 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 $\sigma = g\restriction Q$. Then $\sigma \in Aut(Q,<)$ and $\pi = \sigma^2$. So $\pi \in Aut(Q,<)^{(2)}$. □

**Lemma 57.** *For each linear order $\alpha \in LO$, 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 $x \notin \cup_{n\in\mathbb{N}}(p_n, q_n)$, $\sup\{q_n \mid q_n \leq x\} = \inf\{p_n \mid p_n \geq x\}$ 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 $\alpha \in LO$ 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 $(s_n, t_n)$.

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 the 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 $n = 1, \ldots, N$. □

**Lemma 58.** *There is a Borel function $G : LO \to \mathcal{M}_Q(A, B) \subseteq Aut(Q, <)$ such that*

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

*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 57. 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 10. (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 $\widehat{G(\alpha)} = F(\alpha)$.

**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

$$S = G^{-1}(B(\pi, x_1)) = \{\alpha \in LO \mid G(\alpha)(x_1) = \pi(x_1)\}.$$

Fix $\beta \in S$ (case $S = \emptyset$ is trivial). Then $G(\beta)(x_1) = \pi(x_1)$, so

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

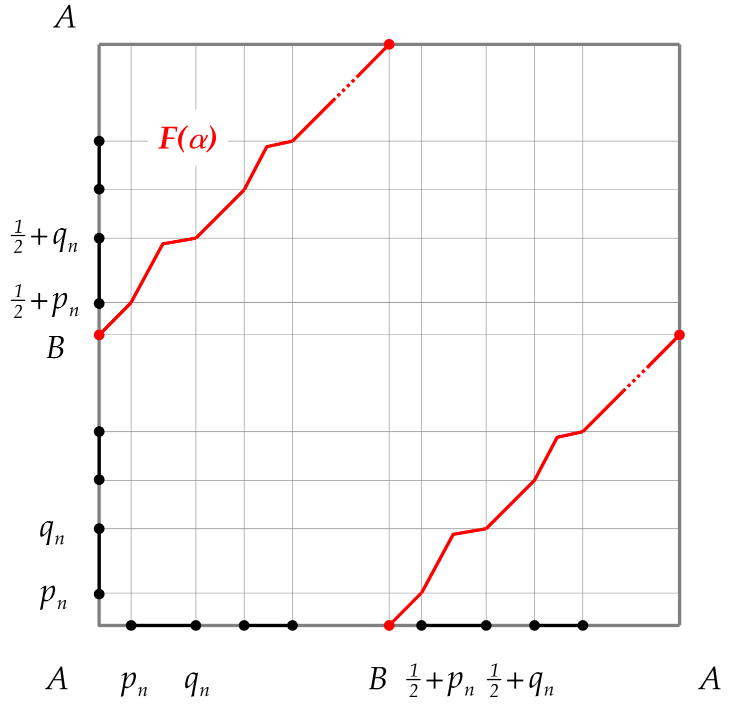

Figure 10: Constructing a Borel reduction: Function $F(\alpha)$.

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

$$\begin{aligned} x_1 \in U_\beta \cup (\tfrac{1}{2} + U_\beta) &\iff G(\beta)(x_1) \neq \tfrac{1}{2} + x_1 \\ &\iff G(\alpha)(x_1) \neq \tfrac{1}{2} + x_1 \\ &\iff x_1 \in U_\alpha \cup (\tfrac{1}{2} + U_\alpha). \end{aligned}$$

Thus, $x_1 \in (p_N^\alpha, q_N^\alpha) \cup (\frac{1}{2} + (p_N^\alpha, q_N^\alpha))$ 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

$$\begin{aligned} S &= \{\alpha \in LO \mid G(\alpha)(x_1) = \tfrac{1}{2} + x_1\} \\ &= \{\alpha \in LO \mid x_1 \notin U_\alpha \cup (\tfrac{1}{2} + U_\alpha)\}. \end{aligned}$$

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 $x_1 \in (p_N^\alpha, q_N^\alpha) \cup (\frac{1}{2} + (p_N^\alpha, q_N^\alpha))$. Then $N(\alpha, \{1, \dots, N\} \times \{1, \dots, N\})$ 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 56. Continuing as in the proof of Lemma 53, we see that $\alpha \in LO2$.

Conversely, suppose $\alpha \in LO2$. According to Lemma 56, 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

$$\phi(D(\hat{\pi} \restriction [A, c])) = D(\hat{\pi} \restriction [c, B]).$$

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 $S = \overline{\{p_n, q_n \mid n \in \mathbb{N}\}} \cup \{A, c\}$. 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, in order to ensure that $\phi$ preserves rationality, we 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 56, so $G(\alpha) \in Aut(Q, <)^{(2)}$. □

**Theorem 59.** *The set of squares $Aut(Q, <)^{(2)}$ in $Aut(Q, <)$ is complete analytic.*

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

## 6.0 OPEN QUESTIONS

We conclude the dissertation with a discussion of open problems.

### 6.1 EXTENDING MACKEY'S THEOREM

One of the first questions that we set out to answer was whether Mackey's theorem can be extended to hold with analytic sets. In other words, if a group has a countable point-separating family of sets that are analytic in any Polish group topology, can we conclude that the group admits a unique Polish group topology? The example in Lemma 20 suggests otherwise, but it does not completely rule out such an extension. And while we have had success with certain variants of Mackey's theorem for analytic sets (see Theorems 21, 22 and 23), the question of whether the 'full' Mackey theorem holds for analytic sets remains open.

### 6.2 AUTOMATIC CONTINUITY

The theory of automatic continuity for Polish groups is still largely an open field.

Recall from Section 3.1 that a Polish group has the automatic continuity property, (AC), if every abstract group homomorphism from the given group into an arbitrary Polish group is continuous. One can replace Polish target groups by second-countable, or separable, or $\aleph_0$-bounded groups, as the resulting properties are all equivalent according to Lemma 16.

In recent years a number of results concerning automatic continuity in specific cases have appeared. Kechris and Rosendal [22] show that Polish groups that admit 'ample generics' (i.e., admit comeager conjugacy classes in any dimension) have the property of automatic continuity into any separable group. Examples of Polish groups that have ample generics include: the infinite symmetric group $S_\infty$, automorphism groups of various countable first-order structures (e.g., automorphism group of the free group on countably many generators), the isometry group $Iso(U_0)$ of the rational Urysohn space. Rosendal and Solecki [29] add the following to the list of spaces that have the automatic continuity property: $Homeo(\mathbb{R}), Homeo(S^1), Homeo(2^{\mathbb{N}}), Homeo(2^{\mathbb{N}})^{\mathbb{N}}, Aut(\mathbb{Q}, <)$. In [28], Rosendal proves the automatic continuity for the homeomorphism group of a compact manifold of dimension 2.

While we know from the work of Kallman that homeomorphism groups of all compact manifolds have a unique Polish group topology, the problem of automatic continuity for homeomorphism groups of compact manifolds of dimension higher than 2 remains open. Also, we have seen that certain compact Lie groups and all finitely generated profinite groups have a unique Polish group topology. It is unknown if the stronger property of automatic continuity holds for these groups.

## 6.3 AUTOMORPHISM GROUPS

If $M$ is a countable model of some first-order theory, then $Aut(M)$, the group of all automorphisms of $M$, is a Polish group when considered with the topology of pointwise convergence. Every profinite group is topologically isomorphic to the automorphism group of a Galois field extension (i.e., every profinite group can be considered to be Galois group). The infinite symmetric group, $S_\infty$ is the automorphism group of $\mathbb{N}$ with no structure. It is well-known that the automorphism groups of countable first-order structures are precisely the closed subgroups of $S_\infty$. Automorphism groups attract a lot of interest from logicians and group theorists (permutation group theory).

A key problem is that of recovering the model $M$ from the topological group $G =$

$Aut(M)$. The question is particularly pressing when the structure is $\aleph_0$-categorical, i.e., if all countable models of its first-order theory are isomorphic. Let $\mathcal{S}$ be the collection of all separable, metrizable topological groups such that the identity has a neighborhood base consisting of (open) subgroups. It turns out that members of $\mathcal{S}$ are precisely the subgroups of $S_\infty$. The problem of recovering the model from the automorphism group turns out to become: does the algebraic structure of $Aut(M)$ completely determine the topology? In other words, which automorphism groups have a unique Polish group topology in the class $\mathcal{S}$.

Logicians and group theorists have approached the problem by considering the so called *small index property*, which says that every subgroup of countable index is open (see [3], p. 106). Homomorphisms from a group with the small index property into any group in $\mathcal{S}$ are automatically continuous. (Hence, for an automorphism group of a countable first-order structure, the small index property does indeed imply uniqueness of Polish group topology in the class $\mathcal{S}$.) In fact, for groups $G \in \mathcal{S}$ the converse is true. We can retopologize $G$ by declaring that every subgroup of countable index be an open neighborhood of the identity. The group $G$ with this new group topology is also in $\mathcal{S}$. The identity map must be continuous from $G$ with the original topology to $G$ with the new one. This forces $G$ to have the small index property.

It is now known that many closed subgroups of $S_\infty$ posses the small index property (see [34]). Some examples are $S_\infty$, $Aut(\mathbb{Q}, <)$, the automorphism group of the countable homogeneous Boolean algebra.

A number of interesting questions arise. How are the small index property (SIP), uniqueness of the Polish group topology (U), and automatic continuity property into Polish groups (AC) related? Of course, for all Polish groups, (AC) implies (U), and for Polish groups in $\mathcal{S}$, (AC) implies (SIP) — but no other relations are known.

Note that Kechris and Rosendal [22] show that if a Polish group has ample generic elements, then it has the small index property and the automatic continuity property.

## 6.4 CONNECTING WITH BANACH ALGEBRAS

Results on uniqueness of topology and automatic continuity in the domain of Banach algebras may *suggest* results and techniques in the domain of topological groups, and vice versa. In Section 3.8, we started work on translating ideas from the theory of Banach algebras into the framework of Polish groups by introducing the separating group. Other notions from the theory of Banach algebras may translate: the 'continuity ideal', which is the annihilator of the separating space; 'intertwining operators', which assist in proving that certain types of homomorphisms are continuous; concentration of discontinuity on a small 'singular set'; 'factorization' of homomorphisms into a continuous and discontinuous part, and so on.

It is convenient that the emphasis in Banach algebras has been on automatic continuity, because the automatic continuity in Polish groups is not well understood. Conversely, the techniques typically used for the uniqueness of topology on Polish groups may well have significant application in the field of Banach algebras.

## 6.5 GENERAL QUESTIONS

Turning to more general questions, consider the following statements about a topological group $G$, and a property $\mathcal{P}$ of topological groups:

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

(U$\mathcal{P}$) The group $G$ has a *unique* group topology satisfying $\mathcal{P}$.

(N$\mathcal{P}$) The group $G$ has *no* group topology satisfying $\mathcal{P}$.

(AC$\mathcal{P}$) Every homomorphism $\phi : G \to H$, where $H$ is a topological group satisfying $\mathcal{P}$, is continuous.

Specific instances of properties $\mathcal{P}$ that we are interested in include: 'the topology is compact','the topology is completely metrizable','the topology is Polish', 'the topology is locally compact, separable metrizable', 'the topology is profinite'.

The following claims are easy to check for a topological group $G$ with property $\mathcal{P}$:

(a) (U$\mathcal{P}$) if and only if every isomorphism $\phi : G \to H$, where $H$ is a topological group satisfying $\mathcal{P}$, is continuous.

(b) Provided $\mathcal{P}$ is finitely productive, (AC$\mathcal{P}$) if and only if every monomorphism $\phi : G \to H$, where $H$ is a topological group satisfying $\mathcal{P}$, is continuous.

(c) (AC$\mathcal{P}$) $\Longrightarrow$ (U$\mathcal{P}$) $\Longrightarrow$ (Aut).

**General Question 1** *For each of the properties $\mathcal{P}$ of interest: which, if any, of the implications in (c) are reversible?*

**General Question 2** *For any pair $\mathcal{P}$, $\mathcal{Q}$ of properties of interest: does (U$\mathcal{P}$) imply (U$\mathcal{Q}$)? Does (AC$\mathcal{P}$) imply (AC$\mathcal{Q}$)?*

### 6.6 SQUARES AND OTHER VERBAL SETS

The results of Sections 5.4 and 5.5 on the complexity of the set of squares are interesting in part because of their connections with broader mathematical context. Papers [2] and [13] are a part of it, but we should also mention connections between these results and a famous problem in ergodic theory. It was an old question whether each, say, weakly mixing transformation is a square of a transformation (see [11], p. 97). This was answered in the negative by Chacon [4]. On the other hand, the generic transformation was proved to be a square by King in [23]. In the same paper, King asks whether the set of squares is Borel in the Polish group of all invertible measure preserving transformations of the unit interval $I$ with Lebesgue measure. It may be possible to use the general techniques of Sections 5.4 and 5.5 to investigate King's question. In order to relate the sets of squares both in $Homeo(S^1)$ and $Aut(Q,<)$ to the complete analytic set $LO2$ of linear orders of type $I + I$, we used the fact that the maps in $Homeo^+(S^1)$ and $Aut(Q,<)$ preserve the order. Invertible measure preserving transformations of $I$, however, typically do not preserve the order. Thus, *if* our techniques can be used to answer King's question, the exact approach is not immediately obvious.

Other interesting questions include: are squares in the homeomorphism group of the unit disk Borel? What can be said about the complexity of the commutators in various groups? Are non-full verbal sets in $S_\infty$ Borel?

# BIBLIOGRAPHY

[1] H. Becker and A.S. Kechris, *The descriptive set theory of Polish group actions*, London Mathematical Society Lecture Note Series, 232, Cambridge University Press, 1996.

[2] F. Beleznay, *The complexity of the collection of countable linear orders of the form I+I*, J. Symbolic Logic **64** (1999), no. 4, 1519–1526.

[3] P.J. Cameron, *Oligomorphic permutation groups*, London Mathematical Society Lecture Note Series, 152, Cambridge University Press, 1990.

[4] R.V. Chacon, *A geometric construction of measure preserving transformations*, Proc. Fifth Berkeley Symp. on Math. Statist. Probab. **2** (1967), no. 2, 335–360.

[5] W.W. Comfort, *Topological groups*, Handbook of Set-Theoretic Topology (K. Kunen and J.E. Vaughan, eds.), North-Holland, Amsterdam, 1984.

[6] H.G. Dales, *Banach algebras and automatic continuity*, Oxford University Press, New York, 2001.

[7] R. Dougherty and J. Mycielski, *Representations of infinite permutations by words (II)*, Proc. Amer. Math. Soc. **127** (1999), no. 8, 2233–2243.

[8] P. Gartside and B. Pejić, *The complexity of the set of squares in the homeomorphism group of the circle*, Fund. Math. **195** (2007), no. 2, 125–134.

[9] M. Gerstenhaber, *On canonical constructions, II*, Proc. Natl. Acad. Sci. USA **42** (1956), no. 11, 881–883.

[10] I. Guran, *On topological groups close to being Lindelöf*, Soviet Math. Dokl. **23** (1981), 173–179.

[11] P.R. Halmos, *Lectures in ergodic theory*, Chelsea, Bronx, New York, 1956.

[12] S. Helgason, *Differential geometry and symmetric spaces*, Academic Press, New York and London, 1962.

[13] P. Humke and M. Laczkovich, *The Borel structure of iterates of continuous functions*, Proc. Edinb. Math. Soc. **32** (1989), 483–494.

[14] A. Mann J. Dixon, M. du Sautoy and D. Segal, *Analytic pro-p groups*, London Mathematical Society Lecture Note Series, 157, Cambridge University Press, 1991.

[15] B.E. Johnson, *The uniqueness of the (complete) norm topology*, Bull. Amer. Math. Soc. **73** (1967), 537–539.

[16] R.R. Kallman, *The topology of compact simple Lie groups is essentially unique*, Adv. Math. **12** (1974), 416–417.

[17] ______, *A uniqueness result for the infinite symmetric group*, Studies in Analysis, Adv. in Math. Suppl. Studies, edited by **4** (1979), 321–322.

[18] ______, *A uniqueness result for a class of compact connected groups*, Conference in Modern Analysis and Probability (New Haven, Conn., 1982) (R. Beals, A. Beck, A. Bellow, and A. Hajian, eds.) Contemporary Mathematics **26** (1984), 207–212.

[19] ______, *Uniqueness results for homeomorphism groups*, Trans. Amer. Math. Soc. **295** (1986), no. 1, 389–396.

[20] A.S. Kechris, *Classical descriptive set theory*, Springer-Verlag, New York, 1995.

[21] ______, *On the concept of $\Pi^1_1$-completeness*, Proc. Amer. Math. Soc. **125** (1997), no. 6, 1811–1814.

[22] A.S. Kechris and C. Rosendal, *Turbulence, amalgamation and generic automorphisms of homogeneous structures*, Proc. London Math. Soc. **94** (2007), no. 2, 302–350.

[23] J.L. King, *The generic transformation has roots of all orders*, Colloq. Math. **84/85** (2000), 531–547.

[24] G.W. Mackey, *Borel structures in groups and their duals*, Trans. Amer. Math. Soc. **85** (1957), 134–165.

[25] D.E. Miller, *On the measurability of orbits in Borel actions*, Proc. Amer. Math. Soc. **63** (1977), no. 1, 165–170.

[26] D. Montgomery and L. Zippin, *Topological transformation groups*, Interscience Publishers, Inc., New York, 1955.

[27] N. Nikolov and D. Segal, *On finitely generated profinite groups I: strong completeness and uniform bounds*, Ann. of Math. **165** (2007), 171–238.

[28] C. Rosendal, *Automatic continuity in homeomorphism groups of compact 2-manifolds*, to appear in Israel J. Math. (2006).

[29] C. Rosendal and S. Solecki, *Automatic continuity of homomorphisms and fixed points on metric compacta*, to appear in Israel J. Math. (2006).

[30] J.-P. Serre, *Lie algebras and Lie groups*, W.A. Benjamin, Inc., New York, 1965.

[31] ______, *Galois cohomology*, Springer-Verlag, Berlin–Heidelberg–New York, 1997.

[32] V.V. Uspenskii, *A universal topological group with a countable base*, Funct. Anal. Appl. **20** (1986), 160–161.

[33] B.L. van der Waerden, *Stetigkeitssätze für halbeinfache liesche gruppen*, Math. Zeitschrift **36** (1933), 780–786.

[34] D. Lascar W. Hodges, I. Hodkinson and S. Shelah, *The small index property for $\omega$-stable $\omega$-categorical structures and for the random graph*, J. London Math. Soc. **48** (1993), no. 2, 204–218.