Group theoretic properties of the group of computable automorphisms of a countable dense linear order

Steffen Lempp[1]
Charles McCoy[1]
Andrei Morozov[2]
Reed Solomon[1]

[1] Department of Mathematics, University of Wisconsin-Madison, USA

[2] Sobolev Institute of Mathematics, Novosibirsk, Russia

October 21, 2002

Abstract

We compare $\text{Aut}(\mathbb{Q})$, the classical automorphism group of a countable dense linear order, with $\text{Aut}_c(\mathbb{Q})$, the group of all computable automorphisms of such an order. They have a number of similarities, including the facts that every element of each group is a commutator and each group has exactly three nontrivial normal subgroups. However, the standard proofs of these facts in $\text{Aut}(\mathbb{Q})$ do not work for $\text{Aut}_c(\mathbb{Q})$. Also, $\text{Aut}(\mathbb{Q})$ has three fundamental properties which fail in $\text{Aut}_c(\mathbb{Q})$: it is divisible, every element is a commutator of itself with some other element, and two elements are conjugate if and only if they have isomorphic orbital structures. Keywords: lattice-ordered groups, automorphism groups, computability theory, effective algebra, reverse mathematics.

1 Introduction

Our goal is to examine the group of automorphisms of a countable dense linear order without endpoints, denoted $\text{Aut}(\mathbb{Q})$, from the perspective of computability theory. We begin with some general motivation for the study of automorphism groups of linear orders and we present the basic definitions for the study of $\text{Aut}(\mathbb{Q})$ in this section. In the next section, we turn to our

This research was conducted while Morozov was visiting the University of Wisconsin-Madison. Morozov's visit was partially supported by the University of Wisconsin and the binational NSF grant DMS-0075899. Lempp's research was partially supported by NSF grant DMS-9732526, McCoy's research was partially supported by an NSF VIGRE Fellowship, and Solomon's research was partially supported by NSF Fellowship DMS-0071586.

motivation for studying the group of computable automorphisms of $\mathbb{Q}$ and to a summary of our results.

For any linear order L, there is a corresponding group of automorphisms, $\mathrm{Aut}(L)$. Such groups have been extensively studied, partially due to their connection with lattice-ordered groups. To define a lattice-order on $\mathrm{Aut}(L)$, set $f \leq_{\mathrm{Aut}(L)} g$ if $\forall x \in L(f(x) \leq_L g(x))$. Holland showed that such automorphism groups play a central role in the theory of lattice-ordered groups.

Theorem 1.1 (Holland [4]). *Every lattice-ordered group can be embedded in $Aut(L)$ for some linear order L.*

Consider the following two theorems to illustrate the importance of the study of automorphism groups for the theory of lattice-ordered groups.

Theorem 1.2 (Holland [4], Weinberg [9]). *Every lattice-ordered group can be embedded (as a lattice-ordered group) in a divisible lattice-ordered group.*

Theorem 1.3 (Glass and Gurevich [2]). *There is a finitely presented lattice-ordered group which has unsolvable word problem.*

Theorem 1.2 is proved by showing that in Holland's Theorem, the linear orders L can be assumed to have the property that $\mathrm{Aut}(L)$ is divisible. Holland proved this fact assuming the generalized continuum hypothesis, and Weinberg later removed this assumption. Theorem 1.3, perhaps of more interest to logicians, was proved by considering properties of the automorphism group of the reals.

There are also interesting model theoretic and set theoretic properties of lattice-ordered groups. For example, the class of all lattice-ordered groups does not have the model theoretic amalgamation property, although it is still true that every lattice-ordered group can be embedded in a two generator group (see the discussion on pages 183-184 in [1]). In set theory, Glass, Gurevich, Holland, and Shelah [3] give an example of a statement about lattice-ordered groups which is independent of ZFC.

In [5], Morozov and Truss considered the automorphism group of $\mathbb{Q}$, a countable dense linear order without endpoints, from the viewpoint of computability theory. For an arbitrary ideal $\mathbf{I}$ in the Turing degrees, they defined $\mathrm{Aut}_{\mathbf{I}}(\mathbb{Q})$ to be the set of automorphisms of $\mathbb{Q}$ which (under a suitable coding, discussed below) are computable from some element of $\mathbf{I}$. (Turing ideals play no role in the rest of this article, so the reader who is unfamiliar with them can safely skip this motivational example.) They proved that for Turing ideals $\mathbf{I}$ and $\mathbf{J}$,

$$\mathrm{Aut}_{\mathbf{I}}(\mathbb{Q}) \cong \mathrm{Aut}_{\mathbf{J}}(\mathbb{Q}) \;\Leftrightarrow\; \mathbf{I} = \mathbf{J}.$$

Along the way to proving this result, Morozov and Truss gave one example of a natural group theoretic property that holds in $\mathrm{Aut}(\mathbb{Q})$ but not in the group of computable automorphisms of $\mathbb{Q}$. This example leads into our current work, which is to continue the study of $\mathrm{Aut}(\mathbb{Q})$ from the point of view of computability theory by studying the group theoretic properties of the group of all computable automorphisms of $\mathbb{Q}$.

Before giving more motivation for our work and stating our main results, we need some background in the theory of $\mathrm{Aut}(\mathbb{Q})$. The first definition introduces the main concept used to prove many of the fundamental properties of $\mathrm{Aut}(\mathbb{Q})$.

Definition 1.4. Fix $f \in \mathrm{Aut}(\mathbb{Q})$. For $q \in \mathbb{Q}$, we define the **orbital** of q (relative to f) to be the convexification of the set containing $f^n(q)$ for all $n \in \mathbb{Z}$. More formally, if $f(q) \geq q$, then we define

$$\mathrm{orbital}(q) = \bigcup_{n \in \mathbb{N}} [f^{-n}(q), f^n(q)].$$

If $f(q) < q$, then we take the union of the intervals $[f^n(q), f^{-n}(q)]$. We label orbital(q) **positive** if $f(q) > q$, **negative** if $f(q) < q$, and **neutral** if $f(q) = q$.

For any $f \in \mathrm{Aut}(\mathbb{Q})$ and any $q \in \mathbb{Q}$, orbital(q) is either a single point (if $f(q) = q$) or a convex open (possibly unbounded and possibly without rational endpoints) interval (if $f(q) \neq q$). If $\hat{q} \in \mathrm{orbital}(q)$, then $\mathrm{orbital}(q) = \mathrm{orbital}(\hat{q})$ and the labels on the orbitals are the same. Therefore, the relation $q \sim \hat{q}$ if and only if $\mathrm{orbital}(q) = \mathrm{orbital}(\hat{q})$ is an equivalence relation which respects the ordering on $\mathbb{Q}$ and the labeling of orbitals. Hence, there is both a natural order on the equivalence classes (given by $[q] \leq [\hat{q}]$ if and only if $[q] = [\hat{q}]$ or $[q] \neq [\hat{q}]$ and $q < \hat{q}$) and a natural labeling of the equivalence classes.

Definition 1.5. Fix $f \in \mathrm{Aut}(\mathbb{Q})$. The structure $\mathbb{Q}$ mod the relation $\sim$ with the induced ordering and labeling is called the **orbital structure** of f. We say that the orbital structures of f and g are **isomorphic** if there is a bijection between the orbital structures which preserves both the order of the orbitals and the labels of the orbitals.

The support of f, denoted supp(f), is the set of q such that $f(q) \neq q$. There are three nontrivial normal subgroups of $\mathrm{Aut}(\mathbb{Q})$:

$$L(\mathbb{Q}) = \{f \mid \mathrm{supp}(f) \text{ is bounded above}\},$$
$$R(\mathbb{Q}) = \{f \mid \mathrm{supp}(f) \text{ is bounded below}\}, \text{ and}$$
$$B(\mathbb{Q}) = \{f \mid \mathrm{supp}(f) \text{ is bounded above and below}\}.$$

For these subgroups, we follow the notation given in [1]. The intuition is that $L(\mathbb{Q})$ consists of the automorphisms that "live on the left", meaning that they are equal to the identity for values far enough right on the line $\mathbb{Q}$. Similarly, $R(\mathbb{Q})$ consists of those automorphisms that "live on the right" and $B(\mathbb{Q})$ refers to those automorphisms that are bounded on both sides.

The following theorem states several properties of $\mathrm{Aut}(\mathbb{Q})$. During the course of this article, we will sketch proofs of some of these properties, all of which are based on those given in Glass [1]. The only difference in the proofs is that Glass considers the general case of a doubly homogeneous linear order (of which $\mathbb{Q}$ is an example), while we specialize our proofs to $\mathrm{Aut}(\mathbb{Q})$. Recall that a group G is divisible if for every element $g \in G$ and every $n \in \mathbb{N}$ with $n > 0$, the equation $x^n = g$ has a solution. We use $[f, g] = f^{-1}g^{-1}fg$ to denote the commutator of f and g in $\mathrm{Aut}(\mathbb{Q})$. We use similar notation, $[a, b]$, for points $a, b \in \mathbb{Q}$ to denote the closed interval between a and b in $\mathbb{Q}$. The context will make clear which meaning is intended by the bracket notation.

Theorem 1.6. *The following properties hold of Aut*$(\mathbb{Q})$.

1. *Aut*$(\mathbb{Q})$ *is divisible.*

2. *For every $f \in Aut(\mathbb{Q})$, there is a $g \in Aut(\mathbb{Q})$ such that $f = [f, g]$. Therefore, every element of $Aut(\mathbb{Q})$ is a commutator.*

3. *Two elements of $Aut(\mathbb{Q})$ are conjugate if and only if they have isomorphic orbital structures.*

4. *$Aut(\mathbb{Q})$ has exactly three nontrivial normal subgroups: $L(\mathbb{Q})$, $R(\mathbb{Q})$, and $B(\mathbb{Q})$.*

Before proceeding, we give references for these results in Glass [1]. Property 1 is stated as Theorem 2E on page 40 and is proved on page 57. Property 2 is a combination of Theorem 2F on page 40 and Corollary 2.2.6 on page 63. The proof of Property 2 is a trivial consequence of Property 3 since f and f^2 have identical orbital structures for any f. Property 3 is stated as Theorem 2.2.5 on page 62. Notice that the conditions in Theorem 2.2.5 that the map be 1-1, onto, left-right preserving, and parity preserving mean exactly that the map is an isomorphism between the orbital structures. Finally, Property 4 is stated as Theorem 2.3.2 on page 65. Notice that $\mathbb{Q}$ trivially has countable coterminality since $\mathbb{Q}$ is countable.

The standard proofs of these properties rely on the technique of defining automorphisms uniformly on orbitals. Formally, this means applying the Patching Lemma 1.10.9 from [1]. To illustrate this technique, consider $f \in \mathrm{Aut}(\mathbb{Q})$ and suppose we want to show that there is a $g \in \mathrm{Aut}(\mathbb{Q})$ such that $g^2 = f$. For each orbital of f, pick a representative q for that orbital. Without loss of generality, assume that orbital(q) is positive. Pick any point $p \in (q, f(q))$ and an isomorphism $h_1 : [q, p] \to [p, f(q)]$. Define $h_2 : [p, f(q)] \to [f(q), f(p)]$ by $h_2(x) = f(h_1^{-1}(x))$. To define $g(x)$ for a point $x \in \text{orbital}(q)$, notice that there is a unique $n \in \mathbb{Z}$ such that $x \in [f^n(q), f^{n+1}(q))$. Define $g(x)$ by first applying f^{-n}, then applying either h_1 or h_2 depending on whether $f^{-n}(x)$ is in $[q, p]$ or $[p, f(q)]$, and finally applying f^n. Pasting together the definitions for g on each orbital yields an automorphism such that $g^2 = f$.

2 Motivation and summary of results

Our goal is to study the group of computable automorphisms of $\mathbb{Q}$, denoted $\mathrm{Aut}_c(\mathbb{Q})$. Similarly, we use $L_c(\mathbb{Q})$, $R_c(\mathbb{Q})$ and $B_c(\mathbb{Q})$ to denote the restrictions of $L(\mathbb{Q})$, $R(\mathbb{Q})$ and $B(\mathbb{Q})$ respectively to the group of computable automorphisms.

Our motivation is threefold. First, from the point of view of computability theory, $\mathrm{Aut}_c(\mathbb{Q})$ is a naturally defined group deserving study. In particular, we wish to understand which properties of $\mathrm{Aut}(\mathbb{Q})$ are captured in $\mathrm{Aut}_c(\mathbb{Q})$ and which are not. There are obvious similarities, such as the fact that both groups are nonabelian and torsion-free, as well as obvious differences, such as the fact that $\mathrm{Aut}(\mathbb{Q})$ is uncountable while $\mathrm{Aut}_c(\mathbb{Q})$ is countable. We hope that a wider audience, once introduced to $\mathrm{Aut}_c(\mathbb{Q})$, will find this group interesting in its own right.

Second, we are motivated by the general program of effective algebra. In effective algebra, one attempts to determine which theorems and techniques in algebra remain true when we restrict our attention to the computable sets. (Below, we will discuss the concept of a computable set for the reader who is unfamiliar with this terminology.) Thus, this program is one attempt at capturing which parts of mathematics are constructively true. (However, unlike an intuitionistic approach to constructive mathematics, we continue to work in classical logic.)

The most widely known results in this area are the fact that the word problem for groups is unsolvable and the negative solution to Hilbert's 10th problem that there is no algorithm to determine if a Diophantine equation has a root.

In the context of this article, we are interested in questions such as whether, given an automorphism f of $\mathbb{Q}$, we can effectively construct an automorphism g such that $g^2 = f$. In Theorem 3.1, we show that the method of constructing g described above is not effective because there is no computable procedure to determine if two elements of $\mathbb{Q}$ are in the same f orbital for an arbitrary computable automorphism f. This result does not say that there is not a computable g such that $g^2 = f$, but it does say that the classical proof does not yield a method to construct such a g. We proceed to show in Theorem 4.1 that in general such a g does not exist by building a computable automorphism f such that for all computable automorphisms g, $g^2 \neq f$.

Our results on effectiveness for the properties listed in Theorem 1.6 are not all negative. In fact, they are an interesting mix of positive and negative results, all of which are surveyed at the end of this section. To give one example of a positive result, we show in Section 6 that $L_c(\mathbb{Q})$, $R_c(\mathbb{Q})$, and $B_c(\mathbb{Q})$ are the only nontrivial normal subgroups of $\mathrm{Aut}_c(\mathbb{Q})$. Therefore the effective analogue of Property 4 of Theorem 1.6 is true.

Third, we are motivated by the program of reverse mathematics, which seeks to determine which set existence axioms are required to prove particular theorems of mathematics. Second order arithmetic (which is much weaker than ZFC and therefore more sensitive to axiomatic differences between theorems) is the model of set theory used in reverse mathematics. While the details of second order arithmetic are outside the scope of this article, the general method of reverse mathematics proceeds as follows. There are five basic axioms systems called (in increasing order of strength) RCA_0, WKL_0, ACA_0, ATR_0 and Π^1_1-CA_0. Most theorems in countable algebra are equivalent to one of these systems. To find an upper bound on the axioms required to prove a theorem T, one looks for a proof of T in one of these systems. To find a lower bound on the axioms required for T, one tries to prove the axioms of one of these systems from the statement of T. (Technically, one usually works in the axiom system RCA_0 plus the statement of T.) So, if ACA_0 suffices to prove T and $\mathrm{RCA}_0 + T$ suffices to prove the axioms in ACA_0, then we can say that ACA_0 gives the minimum collection of set theoretic axioms required to prove T. The process of proving axioms from theorems (that is, proving ACA_0 from $\mathrm{RCA}_0 + T$) is called a reversal and gives rise to the name reverse mathematics.

Two of these axiom systems are relevant to providing motivational background. In our context, RCA_0 consists (roughly) of axioms which prove that the computable sets exist. The axiom system ACA_0 is stronger and it proves the existence of subsets of $\mathbb{Q}$ which are defined using quantification over elements of $\mathbb{Q}$ and $\mathbb{N}$.

The difference between these systems is best illustrated with examples. For any given $q \in \mathbb{Q}$, RCA_0 can prove the existence of sets such as the set of all $a \in \mathbb{Q}$ for which $q < a$ or the set of all $a \in \mathbb{Q}$ such that a has a nonzero power of 2 in its denominator when it is written in reduced form. There are obvious computational procedures to determine the elements of each of those sets. On the other hand, if ACA_0 is given an automorphism f, then it is strong enough to prove the existence of the set of all pairs of rationals a and q such that a and q are in the same orbital with respect to the automorphism f. The definition for a and q being in the same orbital can be given using only a quantifier over $\mathbb{N}$. The formal definition splits into cases depending on whether $f(q) > q$, $f(q) = q$ or $f(q) < q$. In the case when $f(q) > q$, we have

$$a \sim q \Leftrightarrow \exists n \in \mathbb{N}(f^{-n}(q) \leq a \leq f^n(q)).$$

Therefore, in ACA_0, we can define automorphisms uniformly on orbitals and hence prove the first three properties in Theorem 1.6 using the classical proofs as given in [1].

By Theorem 3.1, we cannot use this method in RCA_0 since there is no computable procedure to determine if two points are in the same orbital. This fact does not say that the first three properties in Theorem 1.6 are not provable in RCA_0. It only says that if they are provable in RCA_0, then they require a different proof. However, Theorem 4.1 does say that RCA_0 cannot prove Property 1 in Theorem 1.6 because there is a computable automorphism (which RCA_0 can prove exists) which has no computable divisors. Therefore, axioms (like RCA_0) which can only prove the existence of computable sets cannot prove that this automorphism has divisors.

Hopefully these examples give the reader a glimpse into the interaction between questions in effective algebra and reverse mathematics. Since our original goal was to study the group $\mathrm{Aut}_c(\mathbb{Q})$, we did not attempt to get exact classifications of the properties of Theorem 1.6 in terms of reverse mathematics. We leave the exact classification of these results as open questions which we hope someone will seek to answer. For example, by the comments above, ACA_0 suffices to prove Property 1 in Theorem 1.6, but RCA_0 does not prove this property. It remains open whether WKL_0 suffices to prove this property (although the proof given above does not work in WKL_0), and it remains open whether there is a reversal from this property to either WKL_0 or ACA_0. The curious reader is referred to Chapter 1 of Simpson [6] for a more detailed introduction to reverse mathematics and to Solomon [8] for a survey of results in reverse mathematics concerning ordered groups.

Our notation is standard and follows Glass [1] for automorphism groups and Soare [7] for computability theory. In particular, we use φ_e, $e \in \omega$ to denote the partial computable functions. The reader unfamiliar with the set of partial computable functions can think of φ_e as the e-th program in an effective list of all computer programs in a given language. (Almost any language currently in use will have the same computational power, so the exact choice of language does not matter.) These programs are assumed to run on a computer with unlimited memory and they are allowed to run for arbitrarily long finite amounts of time. Each program take inputs from $\mathbb{N}$. On input n, φ_e either runs forever without halting (in which case $\varphi_e(n)$ is undefined and we say the computation does not halt or is divergent) or φ_e halts after some finite amount of time giving an output in $\mathbb{N}$ (in which case we define $\varphi_e(n)$ to be this output and we say that the computation converges). Because of the potential for divergence, the functions φ_e need not be total.

Furthermore, we use $\varphi_{e,s}(n)$ to (roughly) stand for the action of φ_e after executing s many instructions in its program. Thus, $\varphi_e(n)$ is defined if and only if there is a $t \in \mathbb{N}$ such that $\varphi_{e,s}(n)$ is defined for all $s \geq t$. That is, the program for φ_e on input n halts if and only if it halts at some finite stage. (By definition, once a computation halts, it remains halted forever.)

To view a partial computable function on $\mathbb{N}$ as a function on $\mathbb{Q}$, we fix an effective 1-1 enumeration q_n, $n \in \mathbb{N}$, of $\mathbb{Q}$. We treat φ_e as the effective partial function on $\mathbb{Q}$ which sends q_n to $q_{\varphi_e(n)}$ if $\varphi_e(n)$ is defined, and is undefined if $\varphi_e(n)$ is undefined. We routinely use the notation $\varphi_e(q)$ for $q \in \mathbb{Q}$ with the understanding that φ_e is defined in this way.

Any two countable dense linear orders without endpoints can be shown to be isomorphic using a back-and-forth argument that can be made effective in the case when the orders are computable. (Formally, any computable copy of the ordering $\mathbb{Q}$ is computably categorical.) Therefore, the theorems in this article do not depend on the choice of our effective enumeration of $\mathbb{Q}$. That is, if q_n and r_n are different computable 1-1 enumerations of $\mathbb{Q}$, then there is a total computable function f such that the map $q_n \mapsto r_{f(n)}$ is an isomorphism between the countable dense linear orders given by $\{q_n | n \in \mathbb{N}\}$ and $\{r_n | n \in \mathbb{N}\}$. Hence questions of effectiveness with respect to the enumeration q_n will have exactly the same answers as questions of effectiveness with respect to the enumeration r_n.

In Section 3, we show that the method of defining an automorphism uniformly on the orbitals of another automorphism cannot be used in the context of $\mathrm{Aut}_c(\mathbb{Q})$ because there is no effective procedure to determine when two elements are in the same orbital. Formally, we construct an $f \in \mathrm{Aut}_c(\mathbb{Q})$ such that the relation $p \sim q$, which holds if and only if $\mathrm{orbital}(p) = \mathrm{orbital}(q)$, is as complicated as the halting problem. Similar constructions are implicit in [5], but we present the details to emphasize a method which is repeated in all of our negative results.

Once we know that the method of defining automorphisms uniformly on orbitals does not work in the context of $\mathrm{Aut}_c(\mathbb{Q})$, we consider each of the properties in Theorem 1.6 separately to see if we can construct a computable counter-example or if we can find an effective proof of the property which applies to $\mathrm{Aut}_c(\mathbb{Q})$.

In most cases, we define our computable automorphisms by an effective back-and-forth argument, utilizing the fact that $(\mathbb{Q}, \leq)$ is homogeneous. If we have an order preserving bijection $f : F_0 \to F_1$ between finite subsets of $\mathbb{Q}$, then for any $x \notin \mathrm{domain}(f)$ and for any $y \notin \mathrm{range}(f)$, there is a finite extension $\hat{f}$ of f such that $x \in \mathrm{domain}(\hat{f})$ and $y \in \mathrm{range}(\hat{f})$.

Starting in Section 4, we consider the various properties in Theorem 1.6. Concerning divisibility, we show in Theorem 4.1 that there are elements of $\mathrm{Aut}_c(\mathbb{Q})$ which are not divisible by k in $\mathrm{Aut}_c(\mathbb{Q})$ for any $k \geq 2$. We have already mentioned the implications of this result for effective algebra and reverse mathematics.

We examine the more subtle question of commutators in Section 5. The stronger statement in Property 2 of Theorem 1.6 fails in the computable context. That is, there is an $f \in \mathrm{Aut}_c(\mathbb{Q})$ such that for every $g \in \mathrm{Aut}_c(\mathbb{Q})$, $f \neq [f, g]$. However, it turns out that every element of $\mathrm{Aut}_c(\mathbb{Q})$ is a commutator. In terms of reverse mathematics, we are in the interesting situation that RCA_0 suffices to prove that every element automorphism is a commutator, but does not suffice to prove the stronger property. As with divisibility, ACA_0 is strong enough to prove the stronger property, but it is unknown whether WKL_0 suffices and there are no known reversals.

In Section 5, we also show why the failure of the stronger form of Property 2 of Theorem 1.6 implies that the effective version of Property 3 also fails. Morozov and Truss [5] give a counter-example to the effective version of this property by noting that if f and g are conjugate in $\mathrm{Aut}_c(\mathbb{Q})$, then the orbital structures of f and g have the same Turing degree.

They build computable automorphisms f and g which have isomorphic orbital structures, but for which the orbital structure for f is computable and the orbital structure for g is not. In our counter-example to Property 3, the automorphisms f and g not only have isomorphic orbital structures, but they have identical orbitals. Hence their orbital structures have the same Turing degree.

The fact that there are $f, g \in \mathrm{Aut}_c(\mathbb{Q})$ which have isomorphic orbital structures, but are not conjugate in $\mathrm{Aut}_c(\mathbb{Q})$ indicates that conjugation behaves quite differently in $\mathrm{Aut}(\mathbb{Q})$ and $\mathrm{Aut}_c(\mathbb{Q})$. Therefore, one might expect that there would be more than three nontrivial normal subgroups in $\mathrm{Aut}_c(\mathbb{Q})$. However, it turns out that $L_c(\mathbb{Q})$, $R_c(\mathbb{Q})$, and $B_c(\mathbb{Q})$ are the only nontrivial normal subgroups in $\mathrm{Aut}_c(\mathbb{Q})$. This result is proved in Section 6.

3 Orbital structures

For any $f \in \mathrm{Aut}_c(\mathbb{Q})$, the relation $q \in \mathrm{orbital}(x)$ for $q, x \in \mathbb{Q}$ is clearly computably enumerable. That is, for each pair $q, x \in \mathbb{Q}$ and each $n \in \mathbb{N}$ with $n > 0$, we can computably check the conditions such as $f^{-n}(x) \leq q \leq f^n(x)$ which would indicate that $q \in \mathrm{orbital}(x)$. By systematically searching over all such q, x and n, we can effectively list the pairs q and x such that $q \in \mathrm{orbital}(x)$. If q and x are in the same orbital, then they will eventually be listed as being in the same orbital. However, our search procedure does not tell us if two elements of $\mathbb{Q}$ are in different orbitals. The challenge here is to determine if $q \notin \mathrm{orbital}(x)$ since our procedure only lists positive information.

We show that the relation $q \in \mathrm{orbital}(x)$ can be as complicated as possible, that is, as complicated as the halting problem. Let $K = \{e | \varphi_e(e) \,\mathrm{converges}\}$ denote the halting set and let K_n denote the set of $e < n$ for which $\varphi_{e,n}(e)$ converges. K is a noncomputable set and it is the most complicated (in the sense of Turing reducibility) set which can be effectively listed. In the next theorem, we construct a computable automorphism f such that $3e+1 \in \mathrm{orbital}(3e+2)$ if and only if $e \in K$. Therefore, if we could determine in general if $q \in \mathrm{orbital}(x)$ for the computable automorphism f, then we could determine if $e \in K$. Since K is not computable, this fact tells us that determining if $q \in \mathrm{orbital}(x)$ is not in general computable.

Theorem 3.1. *There is an $f \in Aut_c(\mathbb{Q})$ for which the set of pairs $\langle q, x \rangle$ such that q and x are in the same orbital is Turing equivalent (in fact 1-equivalent) to K.*

Proof. The proof of this fact is quite straightforward, but we present it in some detail, because all of our other negative results use variations on the same idea. The function $f \in \mathrm{Aut}_c(\mathbb{Q})$ we build has some additional properties that are not necessary for this argument, but which will be needed in more complicated constructions later. First of all, we guarantee that f satisfies $f(q) \geq q$ for all q and $f(q) = q$ if and only if $q \leq 0$ or $q = 3n$ for some $n \in \mathbb{N}$. We refer to these as *global* properties of f, since we define these parts of f before the construction begins. This leaves an infinite number of intervals of the form $(3n, 3(n+1))$ in which to code K, or in later constructions to diagonalize. We also make sure that each of these intervals consists of either exactly one positive orbital or exactly two positive orbitals. This requirement is unnecessary for this construction, but it will be useful later.

We have to meet the following requirements.

$$D_n : q_n \in \text{domain}(f).$$
$$R_n : q_n \in \text{range}(f).$$
$$P_e : e \in K \leftrightarrow \text{orbital}(3e+1) = \text{orbital}(3e+2).$$

We use the interval $(3e, 3(e+1))$ to meet P_e and our construction allows us to meet each P_e independently with no injury. We describe the construction on $(0,3)$, guaranteeing that 1 and 2 are in the same orbital if and only if $0 \in K$. We assume that similar constructions are simultaneously occurring in each interval $(3e, 3(e+1))$.

Construction:

Stage 0: Set $f^{-1}(1) = 1/2$, $f(1) = 5/4$, $f^{-1}(2) = 7/4$, and $f(2) = 5/2$. Set $m_1 = m_2 = p_1 = p_2 = 1$.

Stage $s+1$: Assume that we have not met P_0 yet and that we have defined a partial isomorphism f on some finite subset of $(0,3)$. Assume, for $i \in \{1,2\}$, that m_i is the highest power such that $f^{m_i}(i)$ is defined and p_i is the highest power such that $f^{-p_i}(i)$ is defined. Assume by induction that f satisfies the following properties.

1. $f^{m_1}(1) < f^{-p_2}(2)$.

2. $(0,3) \cap \text{domain}(f) \subset [f^{-p_1}(1), f^{m_1-1}(1)] \cup [f^{-p_2}(2), f^{m_2-1}(2)]$.

3. $(0,3) \cap \text{range}(f) \subset [f^{-p_1+1}(1), f^{m_1}(1)] \cup [f^{-p_2+1}(2), f^{m_2}(2)]$.

4. $f(x) > x$ for all $x \in (0,3)$ at which $f(x)$ is defined.

Case $s = 3n$**:** Let $q = q_n$. If $q \in (0,3)$, then extend f (if necessary) so that $q \in \text{domain}(f)$. To perform this extension, find the first case below that applies.

1. If $0 < q < f^{-p_1}(1)$, then set $f^{-p_1-1}(1) = q$. Reset p_1 to $p_1 + 1$.

2. If $f^{m_1-1}(1) < q < f^{m_1}(1)$, then pick x, y such that $f^{m_1}(1) < x < y < f^{-p_2}(2)$ and set $f(q) = x$ and $f^{m_1+1}(1) = y$. Reset m_1 to $m_1 + 1$.

3. If $q = f^{m_1}(1)$, then pick x such that $q < x < f^{-p_2}(2)$ and set $f(q) = x$. Reset m_1 to $m_1 + 1$.

4. If $f^{m_1}(1) < q < f^{-p_2}(2)$, then set $f^{-p_2-1}(2) = q$. Reset p_2 to $p_2 + 1$.

5. If $f^{m_2-1}(2) < q < f^{m_2}(2)$, then pick x, y such that $f^{m_2}(2) < x < y < 3$ and set $f(q) = x$ and $f^{m_2+1}(2) = y$. Reset m_2 to $m_2 + 1$.

6. If $q = f^{m_2}(2)$, then pick x such that $q < x < 3$ and set $f^{m_2+1}(2) = x$. Reset m_2 to $m_2 + 1$.

7. If $f^{m_2}(2) < q$, then pick x such that $q < x < 3$ and set $f^{m_2+1}(2) = q$ and $f(q) = x$. Reset m_2 to $m_2 + 2$.

8. If no case so far applies, extend f in any consistent manner to put q into its domain.

Proceed to the next stage, noting that in each case, the extension of f we defined was consistent with our previous definitions and that the induction hypotheses still hold.
Case $s = 3n + 1$: Let $q = q_n$. If $q \in (0, 3)$, then extend f (if necessary) so that $q \in \text{range}(f)$. To accomplish this extension, find the first case that applies below.

1. If $0 < q < f^{-p_1}(1)$, then pick x such that $0 < x < q$ and set $f^{-p_1-1}(1) = q$ and $f^{-1}(q) = x$. Reset p_1 to $p_1 + 2$.

2. If $q = f^{-p_1}(1)$, then pick x such that $0 < x < q$ and set $f^{-1}(q) = x$. Reset p_1 to $p_1 + 1$.

3. If $f^{-p_1}(1) < q < f^{-p_1+1}(1)$, then pick x, y such that $0 < x < y < f^{-p_1}(x)$ and set $f(y) = q$ and $f(x) = f^{-p_1}(1)$. Reset p_1 to $p_1 + 1$.

4. If $f^{m_1}(1) < q < f^{-p_2}(2)$, then set $f^{m_1+1}(1) = q$. Reset m_1 to $m_1 + 1$.

5. If $q = f^{-p_2}(2)$, then pick x such that $f^{m_1}(1) < x < q$ and set $f(x) = q$. Reset p_2 to $p_2 + 1$.

6. If $f^{-p_2}(2) < q < f^{-p_2+1}(2)$, then pick x, y such that $f^{m_1}(1) < x < y < f^{-p_2}(2)$ and set $f^{-1}(q) = y$ and $f^{-p_2-1}(2) = x$. Reset p_2 to $p_2 + 1$.

7. If $f^{m_2}(2) < q$, then set $f^{m_2+1}(2) = q$. Reset m_2 to $m_2 + 1$.

8. If no case so far applies, extend f in any consistent manner to put q into its range.

Proceed to the next stage, noting that the extension of f we defined is consistent with our previous definition and that the induction hypotheses still apply.
Case s=3n+2: Check if $0 \in K_{n+1} - K_n$. If so, set $f^{m_1+1}(1) = f^{-p_2}(2)$ and starting with the next stage continue the construction with the *alternate continuation* given below.
Alternate Continuation: Once we have coded $0 \in K$ (or diagonalized in the case of later constructions), we want to continue defining f, making sure that $(0, 3)$ is a single positive orbital. At stage $s + 1$ when $s = 3n$, we put $q = q_n$ into the domain of f (if necessary and if $q \in (0, 3)$). Assume by induction that p_1 is the highest power such that $f^{-p_1}(1)$ is defined, m_2 is the highest power such that $f^{m_2}(2)$ is defined, and that both the domain and range of f are contained in $[f^{-p_1}(1), f^{m_2}(2)]$. To extend f so that $q \in \text{domain}(f)$, pick the first case that applies.

1. If $q < f^{-p_1}(1)$, then set $f^{-p_1-1}(1) = q$ and reset p_1 to be $p_1 + 1$.

2. If $q = f^{m_2}(2)$, then pick x such that $f^{m_2}(2) < x < 3$. Set $f^{m_2+1}(2) = x$ and reset m_2 to be $m_2 + 1$.

3. If $f^{m_2}(2) < q$, then pick x such that $q < x < 3$. Set $f^{m_2+1}(2) = q$ and $f(q) = x$. Reset m_2 to be $m_2 + 2$.

4. If none of these cases apply, extend f in any consistent manner such that $q \in \text{domain}(f)$.

Proceed to the next stage of the alternate continuation. A similar construction works at stages $s+1$ where $s = 3n+1$ to put $q = q_n$ into the range of f. If $s = 3n+2$, skip immediately to the next stage of the alternate continuation.

End of Construction

The construction clearly works, assuming that the induction hypotheses are met at the end of each stage as claimed. Verifying this fact involves checking each of the possibilities in each case. We give one example below.

Lemma 3.2. *Suppose we are at stage $s+1$ where $s = 3n$ and P_0 is not met yet. If none of conditions 1-7 apply to q, then the extension of f still satisfies the induction hypotheses.*

Proof. Under these assumptions, there must be an $i \in \mathbb{Z}$ such that either $-p_1 \leq i < m_1 - 1$ and $f^i(1) < q < f^{i+1}(q)$ or $-p_2 \leq i < m_2 - 1$ and $f^i(2) < q < f^{i+1}(q)$. Assume the former case. Then, $f^{i+2}(1)$ is defined, so any consistent extension of f must satisfy $f^{i+1}(1) < f(q) < f^{i+2}$. Notice that the values for p_1 and m_1 stay the same and $f(q) > q$. Therefore, the induction hypotheses are satisfied. □

We verify that at the end of the construction, the interval $(0, 3)$ is either a single positive orbital or two positive orbitals.

Lemma 3.3. *If $0 \notin K$, then the interval $(0, 3)$ consists of exactly two positive orbitals, with orbital(1) below orbital(2).*

Proof. If $0 \notin K$, then at each stage we have $f^{m_1}(1) < f^{-p_2}(2)$. The back-and-forth nature of the argument guarantees that both m_1 and p_2 approach infinity as the construction proceeds. Therefore, 1 and 2 lie in different orbitals. Furthermore, each q_n is either put in orbital(1) or orbital(2) when $f(q_n)$ is defined. Therefore, the orbitals for 1 and 2 cover the interval $(0, 3)$. □

Lemma 3.4. *If $0 \in K$, then the interval $(0, 3)$ consists of a single positive orbital.*

Proof. If $0 \in K_{n+1} - K_n$, then at stage $s+1$, where $s = 3n+2$, we make orbital(1) = orbital(2). In the alternate continuation, each q_n is put into orbital(1) = orbital(2) when $f(q_n)$ is defined. Therefore, orbital(1) covers $(0, 3)$. □

This completes the proof of Theorem 3.1.

□

4 Divisibility

In this section, we show that $\mathrm{Aut}_c(\mathbb{Q})$ is not divisible by proving the following theorem.

Theorem 4.1. *There is an $f \in Aut_c(\mathbb{Q})$ such that for all $g \in Aut_c(\mathbb{Q})$ and all $k \in \mathbb{N}$ with $k \geq 2$, $g^k \neq f$.*

Proof. We build $f \in \mathrm{Aut}_c(\mathbb{Q})$ which meets the requirements D_n and R_n from Theorem 3.1 as well as

$$P_e : \text{If } \varphi_e \in \mathrm{Aut}_c(\mathbb{Q}), \text{ then } \varphi_e^k \neq f \text{ for any } k \geq 2.$$

To meet P_e, if φ_e looks like it might be a k^{th} root of f for some $k \geq 2$, then we make sure that for some $q \in \mathbb{Q}$ and some $n \in \mathbb{N}$, $f^n(\varphi_e(q)) \neq \varphi_e(f^n(q))$. This action satisfies P_e, since if $\varphi_e^k = f$, then φ_e and f commute.

We begin with a function f which has the same global properties as in Theorem 3.1 and we use the witnesses $3e+1$ and $3e+2$ in the interval $(3e, 3(e+1))$ to meet P_e. As before, the parts of the construction working in different intervals act independently and there is no injury. Therefore, we describe only the action in $(0,3)$.

Construction:

Stage 0**:** Define $f^{-1}(1) = 1/2$, $f(1) = 5/4$, $f^{-1}(2) = 7/4$, and $f(2) = 5/2$. Set $p_1 = m_1 = p_2 = m_2 = 1$.

Stage $s+1$**:** Assume we have not met P_0 yet and the induction hypotheses from Theorem 3.1 hold.

Case $s = 3n$**:** Proceed as in stage $s+1$ where $s = 3n$ in Theorem 3.1.

Case $s = 3n+1$**:** Proceed as in stage $s+1$ where $s = 3n+1$ in Theorem 3.1.

Case $s = 3n+2$**:** If either $\varphi_{0,s}(1)$ or $\varphi_{0,s}(2)$ fails to converge, then go to the next stage. If both these computations converge, then check whether $1 < \varphi_0(1) < f(1)$ and $2 < \varphi_0(2) < f(2)$. If either inequality fails, then φ_0 cannot be a k^{th} root of f, so we go on to the next stage.

If both of these inequalities hold, then we need to actively diagonalize to meet P_0. Let $\hat{m}$ and $\hat{p}$ be the highest powers such that $f^{\hat{m}}(\varphi_0(1))$ and $f^{-\hat{p}}(\varphi_0(2))$ are defined. By the induction assumptions, it must be that $\hat{m} \leq m_1 - 1$ and $\hat{p} \leq p_2$. Extend f consistently so that $f^i(\varphi_0(1))$ and $f^{-j}(\varphi_0(2))$ are defined for all $i \leq m_1 - 1$ and all $j \leq p_2$. We have

$$f^{m_1-1}(1) < f^{m_1-1}(\varphi_0(1)) < f^{m_1}(1) \text{ and } f^{-p_2}(2) < f^{-p_2}(\varphi_0(2)) < f^{-p_2+1}(2).$$

Fix $b, c \in \mathbb{Q}$ such that

$$f^{m_1}(1) < b < f^{-p_2}(2) \text{ and } f^{-p_2}(\varphi_0(2)) < c < f^{-p_2+1}(2).$$

Set $f^{m_1+1}(1) = f^{-p_2}(2)$, $f^{m_1}(\varphi_0(1)) = b$, and $f(b) = c$. The inequalities above imply that this gives a consistent extension of f.

We now have $f^{m_1+p_2+1}(1) = 2$, so $\varphi_0(f^{m_1+p_2+1}(1)) = \varphi_0(2)$. Furthermore, $f^{m_1+1}(\varphi_0(1)) = c$ implies that $f^{-p_2}(\varphi_0(2)) < f^{m_1+1}(\varphi_0(1))$. Therefore, as long as f is eventually extended to an automorphism, we will have $\varphi_0(2) < f^{m_1+p_2+1}(\varphi_0(1))$, and so $\varphi_0(f^{m_1+p_2+1}(1)) < f^{m_1+p_2+1}(\varphi_0(1))$, satisfying P_0. From this stage on (since the induction hypotheses are now violated) continue exactly as in the *alternate continuation* of Theorem 3.1.

End of construction

The verification that the diagonalization succeeds is contained in the $s = 3n+2$ case. □

5 Commutators

Recall the standard notation for conjugation, $f^g = g^{-1}fg$, and for commutators, $[f,g] = f^{-1}g^{-1}fg$. We begin this section by sketching the classical proofs for two facts about $\mathrm{Aut}(\mathbb{Q})$.

Theorem 5.1. *If $f, g \in Aut(\mathbb{Q})$ have isomorphic orbital structures, then they are conjugate in $Aut(\mathbb{Q})$.*

Proof. Define the conjugating map h on each f-orbital separately. Suppose q represents an f-orbital and r represents the corresponding g-orbital. If orbital(q) is neutral, then $h(q) = r$. If orbital(q) is positive, then let h be an arbitrary order preserving bijection from $[q, f(q)]$ onto $[r, g(r)]$. For any $x \in$ orbital(q), there is a unique $n \in \mathbb{Z}$ such that $x \in [f^n(q), f^{n+1}(q))$. Define $h(x) = g^n(h(f^{-n}(x)))$. If orbital(q) is negative, define h similarly. □

This proof does not work for $\mathrm{Aut}_c(\mathbb{Q})$ because of Theorem 3.1. However, if the orbital structures of f and g are computable and are computably isomorphic, then this proof shows that f and g are conjugate in $\mathrm{Aut}_c(\mathbb{Q})$. We refer to this fact as the effectivization of Theorem 5.1 and we use this fact repeatedly.

Classically, the fact that every $f \in \mathrm{Aut}(\mathbb{Q})$ is a commutator of the form $[f, g]$ is a trivial consequence of Theorem 5.1. That is, fix f and notice that the identity map on $\mathbb{Q}$ matches up the orbitals of f and the orbitals of f^2. Therefore, f and f^2 have isomorphic orbitals structures and must be conjugate. But, if $f^2 = g^{-1}fg$, then $f = [f, g]$. This gives a quick proof that every element of $\mathrm{Aut}(\mathbb{Q})$ is a commutator.

This proof does not work in the computable case, since Theorem 5.1 fails for $\mathrm{Aut}_c(\mathbb{Q})$ (as we shall see below). For $\mathrm{Aut}_c(\mathbb{Q})$, we replace the connection from that theorem with the following definition and lemma to show that every element in $\mathrm{Aut}_c(\mathbb{Q})$ is a commutator.

Definition 5.2. We say that f has a **single unbounded positive orbital** if $f(0) > 0$ and orbital$(0) = \mathbb{Q}$.

Lemma 5.3. *For any $h \in Aut_c(\mathbb{Q})$, there is a $p \in Aut_c(\mathbb{Q})$ such that both p and ph consist of a single unbounded positive orbital.*

Proof. Define $p(x) = \max\{h(x), h^{-1}(x)\} + 1$. Since either $h(x) \geq x$ or $h^{-1}(x) \geq x$, we have $p(x) \geq x + 1$, so p consists of one unbounded positive orbital. Furthermore, $p(h(x)) = \max\{h(h(x)), h^{-1}(h(x))\} + 1$, and so satisfies $p(h(x)) \geq x + 1$. Again, this implies that it consists of a single unbounded positive orbital. □

Theorem 5.4. *Every element of $Aut_c(\mathbb{Q})$ is a commutator.*

Proof. Fix $f \in \mathrm{Aut}_c(\mathbb{Q})$. By Lemma 5.3, there is a $p \in \mathrm{Aut}_c(\mathbb{Q})$ such that both p and pf consist of a single unbounded positive orbital. Therefore, by the effectivization of Theorem 5.1, there is an $h \in \mathrm{Aut}_c(\mathbb{Q})$ such that $pf = h^{-1}ph$ and so $f = p^{-1}h^{-1}ph = [p, h]$. □

Theorem 5.5. *There is an $f \in Aut_c(\mathbb{Q})$ such that for all $h \in Aut_c(\mathbb{Q})$, $f \neq [f, h]$.*

Proof. The requirements for this theorem are the D_n and R_n requirements of Theorem 3.1 plus

$$P_e : \varphi_e \in \mathrm{Aut}_c \to f^2 \neq \varphi_e^{-1} f \varphi_e.$$

To satisfy P_e, it suffices to make sure that for some n and q, $f^{2n}(q) \neq \varphi_e^{-1}(f^n(\varphi_e(q)))$.

As in Section 3, we construct f without injury. We require the global properties from Theorem 3.1, and for the first time, we use the fact that each interval $(3e, 3(e + 1))$ consists of either exactly one positive orbital or exactly two positive orbitals.

Lemma 5.6. *Assume f has the global properties from Theorem 3.1. If $f^2 = h^{-1}fh$, then h must map each interval $(3n, 3(n+1))$ bijectively onto itself.*

Proof. Write $f^2 = h^{-1}fh$ as $hf^2 = fh$. For any a such that $f(a) = a$, we have $h(f^2(a)) = h(a)$, and so $f(h(a)) = h(a)$. Consider $h(0) = q$. Either $q < 0$, $q = 0$, or $q = 3n$ for some $n \geq 1$. Suppose $q < 0$ and fix any x such that $0 < x < 3$ and $q < h(x) < 0$. Then $f(h(x)) = h(x)$, but $f^2(x) > x$, so $h(f^2(x)) > h(x)$, which gives a contradiction. It is not hard to see that $q = 3n$ for $n \geq 1$ also leads to a contradiction. Therefore, $h(0) = 0$. Continuing by induction, we get $h(3n) = 3n$ for all n. Since h is an automorphism, it must map each $(3n, 3(n+1))$ bijectively onto itself. □

Consider the situation when f has two orbitals in $(0,3)$, say $(0,r)$ and $(r,3)$. The boundary point r must be irrational, since a rational boundary point between two positive orbitals would be mapped to itself, violating the global properties for f.

Lemma 5.7. *Assume f is as in the last paragraph. If $f^2 = h^{-1}fh$, then h must map $(0,r)$ bijectively onto itself and $(r,3)$ bijectively onto itself.*

Proof. For a contradiction, suppose first $x \in (0,r)$ and $h(x) \in (r,3)$. Fix any $y \in (r,3)$. Since h preserves order and $h(3) = 3$, we know $h(x) < h(y) < 3$. Since $h(x)$ and $h(y)$ are in the same f-orbital, there is an n such that $f^n(h(x)) > h(y)$. Therefore, $f^{2n}(x) = h^{-1}(f^n(h(x))) > y$, which contradicts the fact that x and y are in different f-orbitals. A similar argument applies when $y \in (r,3)$ and $h(y) \in (0,r)$. □

As with the proofs in Sections 3 and 4, we use the interval $(3e, 3(e+1))$ with the witnesses $3e+1$ and $3e+2$ to meet P_e, and we present the construction on $(0,3)$. Unlike the proof of Theorem 4.1, where we could assume that $1 < \varphi_0(1) < f(1)$ and $2 < \varphi_0(2) < 2$, our current opponent has considerably more freedom in defining $\varphi_0(1)$ and $\varphi_0(2)$. However, Lemma 5.6 does tell us that we can ignore P_0 unless $\varphi_0(1)$ and $\varphi_0(2)$ converge to numbers in $(0,3)$. Also, Lemma 5.7 gives us a new strategy to beat P_0. If $\varphi_0(1)$ and $\varphi_0(2)$ converge to numbers which we can guarantee are in the same f-orbital without collapsing 1 and 2 in the same f-orbital, then we do so and win P_0.

Construction:

Stage 0**:** Set $f^{-1}(1) = 1/2$, $f(1) = 5/4$, $f^{-1}(2) = 7/4$, and $f(2) = 5/2$. Set $m_1 = p_1 = m_2 = p_2 = 1$.

Stage $s+1$**:** Assume we have not met P_0 yet and the induction hypotheses from Theorem 3.1 hold.

Case $s = 3n$**:** Proceed exactly as in stage $s+1$ when $s = 3n$ in Theorem 3.1.

Case $s = 3n+1$**:** Proceed exactly as in stage $s+1$ when $s = 3n+1$ in Theorem 3.1.

Case $s = 3n+2$**:** If either $\varphi_{0,s}(1)$ or $\varphi_{0,s}(2)$ fails to converge, then go to the next stage. If both computations converge, check if $0 < \varphi_0(1) < \varphi_0(2) < 3$. If not, then φ_0 cannot conjugate f^2 and f, so proceed to the next stage. Otherwise, we need to actively diagonalize to meet P_0. Choose the first subcase which applies.

Subcase 1: Assume $f^{m_1}(1) < \varphi_0(1)$. To win P_0, it suffices (by Lemma 5.7) to guarantee that $(0,3)$ has two orbitals such that 1 is in the bottom orbital and $\varphi_0(1)$ is in the top orbital. There are two possibilities: if $\varphi_0(1) < f^{-p_2}(2)$, then set $f(\varphi_0(1)) = f^{-p_2}(2)$ (guaranteeing

that $\varphi_0(1)$ is in the same orbital as 2), and if $f^{-p_2}(2) \leq \varphi_0(1)$, then do nothing (since $\varphi_0(1)$ is already in the same orbital as 2). In either case, proceed to the next stage, noting that the induction hypotheses still hold. After this point, skip all diagonalization stages.
Subcase 2: Assume subcase 1 does not apply, and $\varphi_0(2) < f^{-p_2}(2)$. We win P_0 by making sure $(0,3)$ has two orbitals with 2 in the top orbital and $\varphi_0(2)$ in the bottom orbital. Again, there are two possibilities: if $f^{m_1}(1) < \varphi_0(2)$, then set $f^{m_1+1}(1) = \varphi_0(2)$ (guaranteeing that $\varphi_0(2)$ is in the same orbital as 1), and if $\varphi_0(2) \leq f^{m_1}(1)$, then do nothing (since $\varphi_0(2)$ is already in the same orbital as 1). In either case, proceed to the next stage, noting that the induction hypotheses still hold. After this point, skip all diagonalization stages.
Subcase 3: Assume that $\varphi_0(1) \leq f^{m_1}(1)$ and $f^{-p_2}(2) \leq \varphi_0(2)$. To reduce the number of possibilities in this subcase, we extend f as follows.

1. Pick y such that $f^{m_1}(1) < y < f^{-p_2}(2)$. Set $f^{m_1+1}(1) = y$ and reset m_1 to $m_1 + 1$.
2. If $\varphi_0(2) > f^{m_2}(2)$, then pick x such that $\varphi_0(2) < x < 3$. Set $f^{m_2+1}(2) = \varphi_0(2)$, $f^{m_2+2}(2) = x$, and reset m_2 to $m_2 + 2$.
3. If $\varphi_0(1) < f^{-p_1}(1)$, then set $f^{-p_1-1}(1) = \varphi_0(1)$ and reset p_1 to $p_1 + 1$.

The point of extending f in this manner is that we can now assume that there are integers i and j with $-p_1 \leq i < m_1$ and $-p_2 \leq j < m_2$ such that

$$f^i(1) \leq \varphi_0(1) < f^{i+1}(1) \text{ and } f^j(2) \leq \varphi_0(2) < f^{j+1}(2).$$

There are four possibilities to consider. Our action in each of these possibilities will violate the induction hypotheses. Therefore, after this stage, we continue the construction with the *alternate continuation* given in Theorem 3.1.
Subcase 3(a): Assume that $\varphi_0(1) = f^i(1)$ and $f^j(2) < \varphi_0(2)$. The crucial observation here is that $f^j(2) < \varphi_0(2) < f^{j+1}(2)$ implies that regardless of how f is extended to an automorphism

$$\forall k \in \mathbb{Z}\, (f^k(2) \neq \varphi_0(2)). \tag{1}$$

If we make $f^{2k}(1) = 2$ for some k, then $\varphi_0(f^{2k}(1)) = \varphi_0(2)$. But, $f^k(\varphi_0(1)) = f^{k+i}(1) = f^{i-k}(2)$, which by Equation (1) cannot be equal to $\varphi_0(2)$.

To make $f^{2k}(1) = 2$ for some k, we act as follows. If $m_1 + p_2 + 1$ is even, then set $f^{m_1+1}(1) = f^{-p_2}(2)$ (thus making $f^{m_1+p_2+1}(1) = 2$). If $m_1 + p_2 + 1$ is odd, then pick a point x such that $f^{m_1}(1) < x < f^{-p_2}(2)$ and set $f^{m_1+1}(1) = x$ and $f(x) = f^{-p_2}(2)$ (thus making $f^{m_1+p_2+2}(1) = 2$).
Subcase 3(b): Assume $f^i(1) < \varphi_0(1)$ and $f^j(2) = \varphi_0(2)$. We perform exactly the same action as in subcase 3(a). The verification that this successfully diagonalizes is essentially the same as subcase 3(a).
Subcase 3(c): Assume that we have $\varphi_0(1) = f^i(1)$ and $\varphi_0(2) = f^j(2)$. Our strategy is again to make $f^{2k}(1) = 2$, for some k, to obtain

$$\varphi_0(f^{2k}(1)) = \varphi_0(2) = f^j(2) = f^{2k+j}(1) \text{ and } f^k(\varphi_0(1)) = f^{k+i}(1).$$

As long as k is chosen such that $k+j \neq i$, we will win P_0. Pick points $x_1, \dots, x_l$ such that $f^{m_1}(1) < x_1 < \dots < x_l < f^{-p_2}(2)$, $m_1 + l + p_2 + 1$ is even, and $((m_1 + l + p_2 + 1)/2) + j \neq i$. Set $f^{m_1+1}(1) = x_1$, $f(x_n) = x_{n+1}$ for $1 \leq n < l$ and $f(x_l) = f^{-p_2}(2)$. We have made $f^{m_1+l+p_2+1}(1) = 2$ as desired.
Subcase 3(d): Assume $f^i(1) < \varphi_0(1)$ and $f^j(2) < \varphi_0(2)$. Extend f so that $f^{m_1-i-1}(\varphi_0(1))$ and $f^{-p_2-j}(2)$ are defined. Notice that

$$f^{m_1-1}(1) < f^{m_1-i-1}(\varphi_0(1)) < f^{m_1}(1) \text{ and } f^{-p_2}(2) < f^{-p_2-j}(\varphi_0(2)) < f^{-p_2+1}(2).$$

Therefore, we have extended f as far as possible to maintain the induction hypotheses. Our goal is to make $f^{2k}(1) = 2$, so that $\varphi_0(f^{2k}(1)) = \varphi_0(2)$, and to guarantee that $f^n(\varphi_0(1)) \neq \varphi_0(2)$ for any n.

If $m_1 + p_2 + 1$ is even, then set $f^{m_1+1}(1) = f^{-p_2}(2)$, which makes $f^{m_1+p_2+1}(1) = 2$. Pick points x, y such that $f^{m_1}(1) < x < f^{-p_2}(2)$ and $f^{-p_2}(2) < y < f^{-p_2-j}(\varphi_0(2))$. Set $f^{m_1-i}(\varphi_0(1)) = x$ and $f(x) = y$. We have

$$f^{-p_2}(2) < f^{m_1-i+1}(\varphi_0(1)) < f^{-p_2-j}(\varphi_0(2)).$$

When f is extended to an automorphism, we will have $f^{-p_2-j-1}(\varphi_0(2)) < f^{-p_2}(2)$, which shows that $f^n(\varphi_0(1)) \neq \varphi_0(2)$ for any n.

If $m_1 + p_2 + 1$ is odd, then pick four points v, w, x, y such that $f^{m_1}(1) < v < w < x < f^{-p_2}(2)$ and $f^{-p_2}(2) < y < f^{-p_2-j}(\varphi_0(2))$. Set $f^{m_1+1}(1) = w$ and $f(w) = f^{-p_2}(2)$, so that $f^{m_1+p_2+2}(1) = 2$. Set $f^{m_1-i}(\varphi_0(1)) = v$, $f(v) = x$, and $f(x) = y$. The verification that this succeeds is as above.
End of Construction

Lemma 5.8. *P_0 is satisfied.*

Proof. Assume $\varphi_0(1)$ and $\varphi_0(2)$ converge. If either number is not in $(0, 3)$, then Lemma 5.6 shows that P_0 is satisfied. If both numbers are in $(0, 3)$, then we must eventually consider one of the subcases when $s = 3n + 2$. In the first two subcases, the numbers 1 and 2 remain in distinct orbitals by Lemma 3.3, while either $\varphi_0(1) \in \text{orbital}(2)$ or $\varphi_0(2) \in \text{orbital}(1)$. Therefore, P_0 is satisfied by Lemma 5.7. In the third subcase, we verified that P_0 was satisfied in the construction. □

This completes the proof of Theorem 5.5. □

Corollary 5.9 (Morozov and Truss, [5]). *There are $f, g \in Aut_c(\mathbb{Q})$ such that f and g are conjugate in $Aut(\mathbb{Q})$ but not in $Aut_c(\mathbb{Q})$.*

As noted in the introduction, the proof of Corollary 5.9 in [5] builds f and g for which the Turing degrees of the orbital structures for f and g are different. We can strengthen this result as follows.

Corollary 5.10. *There are $f, g \in Aut_c(\mathbb{Q})$ such that f and g are conjugate in $Aut(\mathbb{Q})$, f and g are not conjugate in $Aut_c(\mathbb{Q})$, and the Turing degrees of the orbital structures of f and g are equal. In fact, f and g can be chosen to have the same orbitals.*

Proof. For any automorphism f (regardless of computational properties), f and f^2 have the same orbitals and therefore are conjugate in $\mathrm{Aut}(\mathbb{Q})$. Let f be as in Theorem 5.5. Rewriting $f \neq [f, h]$ as $f^2 \neq f^h$, it is clear that the functions f and $g = f^2$ satisfy Corollary 5.10. □

6 Normal subgroups

The standard proof that $\mathrm{Aut}(\mathbb{Q})$ contains exactly three nontrivial normal subgroups, $B(\mathbb{Q})$, $L(\mathbb{Q})$, and $R(\mathbb{Q})$, relies heavily on both the fact that $\mathrm{Aut}(\mathbb{Q})$ is divisible and the fact that if two elements in $\mathrm{Aut}(\mathbb{Q})$ have isomorphic orbital structures then they are conjugate. In this section, we show that $B_c(\mathbb{Q})$, $L_c(\mathbb{Q})$, and $R_c(\mathbb{Q})$ are the only nontrivial normal subgroups in $\mathrm{Aut}_c(\mathbb{Q})$. As with Theorem 5.4, our proof must differ from the classical proof.

Theorem 6.1. *$B_c(\mathbb{Q})$, $L_c(\mathbb{Q})$, and $R_c(\mathbb{Q})$ are the only nontrivial normal subgroups in $Aut_c(\mathbb{Q})$.*

The rest of this section is devoted to the proof of Theorem 6.1. To see these three subgroups are normal in $\mathrm{Aut}_c(\mathbb{Q})$, suppose $r \in \mathbb{Q}$ is such that $f(q) = q$ for all $q \geq r$ and let $h \in \mathrm{Aut}_c(\mathbb{Q})$ be arbitrary. Let $q' = h^{-1}(r)$. Then, for any $x \geq q'$, we have $h(x) \geq r$ and so $h^{-1}(f(h(x))) = x$. The verification when $f(q) = q$ for all $q \leq s$ is similar.

For the remainder of this section, we assume that all automorphisms mentioned are computable.

The task of showing these are the only normal subgroups in $\mathrm{Aut}_c(\mathbb{Q})$ can be broken into four pieces. First, we show that if $f \in \mathrm{Aut}_c(\mathbb{Q})$ is not in these subgroups, then the normal closure of f is all of $\mathrm{Aut}_c(\mathbb{Q})$. Second, we show that if $f \in L_c(\mathbb{Q}) \setminus R_c(\mathbb{Q})$, then the normal closure of f is $L_c(\mathbb{Q})$. Third, we show that if $f \in R_c(\mathbb{Q}) \setminus L_c(\mathbb{Q})$, then the normal closure of f is $R_c(\mathbb{Q})$. Finally, we show that if $f \in B_c(\mathbb{Q})$, then the normal closure of f is $B_c(\mathbb{Q})$.

Definition 6.2. We say that f has positive orbitals which are **cofinal as** $x \to +\infty$ (as $x \to -\infty$, respectively) if for every $n \in \mathbb{N}$, there is an $x \in \mathbb{Q}$ such that $x > n$ ($x < -n$, respectively) and $f(x) > x$. We say f has positive orbitals which are **cofinal in both directions** if f has positive orbitals which are cofinal as $x \to +\infty$ and as $x \to -\infty$.

Lemma 6.3. *Let $f \in Aut_c(\mathbb{Q})$ have positive orbitals which are cofinal in both directions. Then there is a $g \in Aut_c(\mathbb{Q})$ such that $f^g f$ consists of a single unbounded positive orbital.*

Proof. Choose a sequence of rationals z_n for $n \in \mathbb{Z}$ such that $f(z_{2i}) = z_{2i+1}$ for all i, the sequence z_{2i} is unbounded in both directions, and $n < m$ implies $z_n < z_m$. Such points can be chosen effectively by our assumption on f.

Define g effectively such that $g([z_n, z_{n+1}]) = [z_{n+1}, z_{n+2}]$ for all $n \in \mathbb{Z}$. Notice that $g^{-1}(f(g(f(z_{2i})))) = z_{2i+2}$. Therefore, $f^g f$ maps each interval $[z_{2i}, z_{2i+2}]$ onto $[z_{2i+2}, z_{2i+4}]$ and hence consists of one unbounded positive orbital. □

Lemma 6.4. *Let $f \in Aut_c(\mathbb{Q})$ be such that $f \notin R_c(\mathbb{Q})$, f has positive orbitals as $x \to +\infty$, but f does not have positive orbitals as $x \to -\infty$. Then, there is a $g \in Aut_c(\mathbb{Q})$ in the normal closure of f such that g has positive orbitals cofinal in both directions.*

Proof. By the conditions on f, we can effectively pick points z_i for $i \in \mathbb{Z}$ such that

1. z_i are cofinal in both directions,
2. for $i \geq 0$, $z_i < f(z_i) < f^{-1}(z_{i+1}) < z_{i+1}$,
3. $z_{-1} < f^{-1}(z_{-1}) < f^{-1}(z_0) < z_0$, and
4. for $i < 0$, $z_{i-1} < f^{-1}(z_{i-1}) < f(z_i) < z_i$.

By an effective back-and-forth argument, define $\alpha \in \mathrm{Aut}_c(\mathbb{Q})$ such that

1. for $i \geq 0$, the interval $(z_i, f(z_i))$ is a single positive α-orbital,
2. for $i < 0$, the interval $(f(z_i), z_i)$ is a single negative α-orbital, and
3. $\alpha(x) = x$ for all other x.

Set $g(x) = \alpha^{-1} f^{-1} \alpha f(x)$, and notice that g is in the normal closure of f. It is straightforward to check that for all $i \geq 0$, $(f^{-1}(z_i), z_i)$ is a positive g-orbital and $(z_i, f(z_i))$ is a negative g-orbital. Also, for $i < 0$, $(f(z_i), z_i)$ is a positive g-orbital and $(z_i, f^{-1}(z_i))$ is a negative g-orbital. At all other points, $g(x) = x$. Therefore, g meets the requirements of the lemma. □

Using Lemmas 6.3 and 6.4, we can show that for any $f \in \mathrm{Aut}_c(\mathbb{Q})$, if $f \notin L_c(\mathbb{Q}) \cup R_c(\mathbb{Q})$, then the normal closure of f is all of $\mathrm{Aut}_c(\mathbb{Q})$. Applying Lemma 6.4, we can assume without loss of generality that f has positive orbitals which are cofinal in both directions. By Lemma 6.3, there is a g is the normal closure of f which consists of a single unbounded positive orbital. Consider any $h \in \mathrm{Aut}_c(\mathbb{Q})$. By Lemma 5.3, there is a p such that both p and ph consist of single positive unbounded orbitals. But, by the effectivization of Theorem 5.1, both p and ph are in the normal closure of f, and hence h is in the normal closure of f, as required.

We next consider automorphisms $f \in L_c(\mathbb{Q}) \setminus R_c(\mathbb{Q})$.

Definition 6.5. If $f \in L_c(\mathbb{Q}) \setminus R_c(\mathbb{Q})$, then we say a real r is the **upper boundary** for $\mathrm{supp}(f)$ if $\mathrm{supp}(f) \cap [r, +\infty) = \emptyset$ and for any rational $q < r$, $\mathrm{supp}(f) \cap (q, r) \neq \emptyset$.

The case we are most interested in is when the upper boundary r is a rational. In this case, $f(r) = r$.

Lemma 6.6. *If $f \in L_c(\mathbb{Q}) \setminus R_c(\mathbb{Q})$, then there is a $g \in L_c(\mathbb{Q})$ in the normal closure of f such that g has positive orbitals which are cofinal as $x \to -\infty$ and the upper boundary of supp(g) is a rational point.*

Proof. Without loss of generality, we can assume that f has positive orbitals as $x \to -\infty$. Pick points z_i for $i \in \mathbb{N}$ such that $z_i \to -\infty$ as $i \to \infty$ and $z_{i+1} < f(z_{i+1}) < f^{-1}(z_i) < z_i$ for all i. By an effective back-and-forth argument, define $\alpha(x)$ such that each interval $(z_i, f(z_i))$ is a positive α-orbital and $\alpha(x) = x$ for all x not in an interval of this type. Set $g(x) = \alpha^{-1} f^{-1} \alpha f(x)$ and notice that g is in the normal closure of f. As in Lemma 6.4, it is straightforward to check that g has positive orbitals which are cofinal as $x \to -\infty$ and the upper boundary of g is $f(z_0)$. □

Lemma 6.7. *If $f \in L_c(\mathbb{Q}) \setminus R_c(\mathbb{Q})$ has positive orbitals which are cofinal as $x \to -\infty$ and has a rational upper boundary point, then there is a $g \in L_c(\mathbb{Q})$ in the normal closure of f such that g consists of a single positive orbital (which is unbounded as $x \to -\infty$) and has a rational upper boundary point.*

Proof. The proof is similar to that of Lemma 6.3. □

Lemma 6.8. *If $h \in L_c(\mathbb{Q})$, then there is a $p \in L_c(\mathbb{Q})$ such that both p and ph consist of single positive orbitals (which are unbounded as $x \to -\infty$) and have rational upper boundary points.*

Proof. Fix any rational number r such that r is greater than all the numbers in $\mathrm{supp}(h)$. Define $p(x)$ as follows. On the interval $[r+2, +\infty)$, p is the identity. p maps the interval $(r, r+2)$ as a single positive orbital onto the interval $(r+1, r+2)$. On the interval $(-\infty, r]$, $p(x) = \max(h(x), h^{-1}(x)) + 1$. Notice that since $p(r) = r+1$, the intervals $(-\infty, r]$ and $(r, r+2)$ join together in a single positive p-orbital. Therefore, p has a single positive orbital which is unbounded as $x \to -\infty$ and p has the rational upper boundary point $r+2$. Furthermore, since h is the identity on all numbers bigger than r, ph has exactly the same orbital structure as p. Therefore, we have met the requirements of the lemma. □

We are now in a position to show that for any $f \in L_c(\mathbb{Q}) \setminus R_c(\mathbb{Q})$, the normal closure of f is all of $L_c(\mathbb{Q})$. Applying Lemmas 6.6 and 6.7, there is a g in the normal closure of f which consists of a single positive orbital which is unbounded as $x \to -\infty$ and g has a rational upper boundary point. For any $h \in L_c(\mathbb{Q})$, by Lemma 6.8, there is a p such that both p and ph have the same orbital structure as g. Applying the effectivization of Theorem 5.1, g must be conjugate to both p and ph, and therefore, h is in the normal closure of g.

A similar argument shows that if $f \in R_c(\mathbb{Q}) \setminus L_c(\mathbb{Q})$, then the normal closure of f is all of $R_c(\mathbb{Q})$. It remains to show that if $f \in B_c(\mathbb{Q})$, then the normal closure of f is all of $B_c(\mathbb{Q})$.

Definition 6.9. We say that the orbital structure of f consists of **two orbitals separated by a rational point** if there are rationals $q < r < s$ such that (q, r) and (r, s) are both f-orbitals, and f is the identity on all other points.

Lemma 6.10. *If $f \in B_c(\mathbb{Q})$ is not the identity, then there is a $g \in B_c(\mathbb{Q})$ in the normal closure of f such that the orbital structure of g consists of two orbitals separated by a rational point. Furthermore, the labels of the two nontrivial g-orbitals are different.*

Proof. Without loss of generality, we can assume there is a point z such that $z < f(z)$. Fix such a z. Define α effectively such that $(z, f(z))$ is a single positive α-orbital, and $\alpha(x) = x$ for all points outside this interval. Let $g(x) = \alpha^{-1} f^{-1} \alpha f(x)$. It is straightforward to check that $(f^{-1}(z), z)$ is a positive g-orbital, $(z, f(z))$ is a negative g-orbital, and $g(x) = x$ for all points outside these intervals. Therefore, g meets the requirements of the lemma. □

Lemma 6.11. *For any $h \in B_c(\mathbb{Q})$, there is a $p \in B_c(\mathbb{Q})$ such that the orbital structures of both p and ph consist of two orbitals separated by a rational point. Furthermore, the labels on the nontrivial orbitals for both p and ph are different.*

Proof. Fix rational numbers $q < r$ such that $\text{supp}(h)$ lies in the interval (q, r). Define an automorphism $p(x)$ effectively such that

1. p restricted to $[r + 2, +\infty)$ is the identity,
2. p maps $(r, r + 2)$ onto $(r + 1, r + 2)$ as a single positive orbital,
3. for $x \in [q, r]$, $p(x) = \max(h(x), h^{-1}(x)) + 1)$,
4. p maps $(q - 1, q)$ onto $(q - 1, q + 1)$ as a single positive orbital,
5. $p(q - 1) = q - 1$,
6. p maps $(q - 2, q - 1)$ onto $(q - 2, q - 1)$ as a single negative orbital, and
7. p restricted to $(-\infty, q - 2]$ is the identity.

Because $p(q) = q+1$ and $p(r) = r+1$, the intervals $(q-1, q)$, $[q, r]$ and $(r, r+2)$ join together in a single positive p-orbital. Therefore, the orbital structure of p consists of two orbitals separated by the rational point $q - 1$. Furthermore, the lower orbital is negative and the higher orbital is positive.

Since h is the identity outside of (q, r), it is clear that ph has the same orbital structure as p, and so we have fulfilled the requirements of the lemma. □

We can now finish the proof of Theorem 6.1. Suppose $f \in B_c(\mathbb{Q})$ and fix any $h \in B_c(\mathbb{Q})$. By Lemmas 6.10 and 6.11, there is a g in the normal closure of a $p \in B_c(\mathbb{Q})$ such that the orbital structures of g, p^{-1} and $(ph)^{-1}$ are all effectively the same. Therefore, once more applying the effective version of Lemma 5.1, we get that g is conjugate to p^{-1} and $(ph)^{-1}$ and hence h is in the normal closure of f.

References

[1] Glass, A.M.W., *Ordered permutation groups*, Cambridge University Press, Cambridge, 1981.

[2] Glass, A.M.W. and Gurevich, Yuri, The word problem for lattice-ordered groups, *Trans. Amer. Math. Soc.*, **280** (1983), 127-138.

[3] Glass, A.W.M., Gurevich, Y., Holland, W.C. and Shelah, S., Rigid homogeneous chains, *Mathematical Proceedings of the Cambridge Philosophical Society*, **89** (1981), 7-17.

[4] Holland, W.C., The lattice-ordered group of automorphisms of an ordered set, *Michigan Mathematics Journal*, **10** (1963), 399-408.

[5] Morozov, A.S. and Truss, J.K., On computable automorphisms of the rational numbers, *Journal of Symbolic Logic*, to appear.

[6] Simpson, Stephen G., *Subsystems of second order arithmetic*, Springer–Verlag, Heidelberg, 1998.

[7] Soare, Robert I., *Recursively enumerable sets and degrees*, Springer–Verlag, Heidelberg, 1987.

[8] Solomon, Reed, Ordered groups: a case study in reverse mathematics, *Bulletin of Symbolic Logic*, **5**(1) March 1999, 45-58.

[9] Weinberg, E.C., Embedding in a divisible lattice-ordered group, *Journal of the London Mathematics Society*, **42** (1967), 504-506.