Computability Theory, Reverse Mathematics, and Ordered Fields

Oscar Louis Levin, Ph.D.

University of Connecticut, 2009

The effective content of ordered fields is investigated using tools of computability theory and reverse mathematics. Computable ordered fields are constructed with various interesting computability theoretic properties. These include a computable ordered field for which the sums of squares are reducible to the halting problem, a computable ordered field with no computable set of multiplicatively archimedean class representatives, and a computable ordered field every transcendence basis of which is immune. The question of computable dimension for ordered fields is posed, and answered for archimedean fields, fields with finite transcendence basis, and some fields with infinite pure transcendence basis. Several results from the reverse mathematics of ordered rings and fields are extended.

Computability Theory, Reverse Mathematics, and Ordered Fields

Oscar Louis Levin

B.S. Mathematics, University of Northern Colorado, Greeley, CO, 2004

B.A. Philosophy, University of Northern Colorado, Greeley, CO, 2004

M.S. Mathematics, University of Connecticut, Storrs, CT, 2006

A Dissertation

Submitted in Partial Fullfilment of the

Requirements for the Degree of

Doctor of Philosophy

at the

University of Connecticut

2009

APPROVAL PAGE

Doctor of Philosophy Dissertation

Computability Theory, Reverse Mathematics, and Ordered Fields

Presented by

Oscar Louis Levin, B.S., B.A., M.S.

Major Advisor

_____

D. Reed Solomon

Associate Advisor

_____

Manuel Lerman

Associate Advisor

_____

Evarist Giné

University of Connecticut

2009

ACKNOWLEDGEMENTS

First and formost, thanks to the best adviser anyone could wish for. Reed, you are amazing - I could not have done this without you. Thanks to Asher for many an enlightening conversation and word of encouragement. Thanks to Russell Miller for your insight and suggestions. To my fellow stooges, Matt and Tyler, thank you for learning computability theory with me, and thank you to Joe, for first teaching us this fascinating subject. Shanna, thank you for delaying the puggle for another year and all around being wonderful. And finally, thanks to my family for your continuous love and support.

TABLE OF CONTENTS

1. Introduction 1

1.1 Ordered Fields 2

1.2 Computable Ordered Fields 8

1.3 Summary of Results 11

2. Building Computable Ordered Fields 14

2.1 Simple Examples 14

2.2 Archimedean Fields 15

2.2.1 Making an infinite transcendence basis computable 20

2.3 Non-Archimedean Fields 25

2.3.1 Coding into Multiplicatively Archimedean Classes 29

3. Computable Dimension 44

3.1 Finite Transcendence Degree 45

3.2 Infinite Transcendence Degree 51

3.3 The Archimedean Case 60

4. Transcendence Bases 63

4.1 Non-Computable Transcendence Bases 63

4.2 Immune Transcendence Bases 69

5. Reverse Mathematics of Ordered Fields 73

5.1 Background 73

5.2 Extending Partial Orders to Full Orders 76

5.3 Further Extensions 85

Bibliography 88

Chapter 1

Introduction

Many theorems of algebra assert the existence of an object: there exists a real root of every odd degree rational polynomial, every vector space has a basis, every formally real field can be ordered, etc. One might ask how complicated it is to find these objects that we know must exist. That is, to what extent are these theorems *effective*. In the last century, it has become clear that computable algebra is a powerful tool in addressing these questions. Using the notion of a *computable function* from computability theory, it is possible to precisely define what it means for an algebraic structure to be presented effectively. With such a presentation in hand, we can investigate what properties of the structure are also effective, and if they are not, to what extent does the effectiveness fail.

This program of investigation has been very successful for a wide variety of algebraic structures, including groups, rings, boolean algebras, graphs, and linear orders (for a survey, see [3]). Often results for one class of structures can be transferred to another, although not always. Perhaps surprisingly, the large number of results known for groups cannot be easily transferred to fields. Indeed,

there are many open questions in computably algebra regarding fields, and these seem to be quite hard to answer. This current work looks to make inroads on this front, by considering the possibly simpler case of *ordered* fields.

1.1 Ordered Fields

Before considering any computability theory, let us quickly review some classical definitions and results from the theory of ordered fields. For a more comprehensive introduction, see the chapter 6 in [10], chapter 11 in [11], or [17].

Definition 1.1.1. Let F be a field. An *ordering* on F is a linear order $\leq$ (i.e., a total, transitive, antisymmetric binary relation) such that for all $a, b, c \in F$,

1. $a \leq b \Longrightarrow a + c \leq b + c$, and
2. $a \leq b,\ 0 \leq c \Longrightarrow ac \leq bc$.

F is *orderable* if there is an ordering $\leq$ on F. An *ordered field* is a pair $(F, \leq)$.

Alternatively, we could define the set of non-negative elements in a field.

Definition 1.1.2. Let F be a field. A *positive cone* of F is a subset P of F satisfying,

1. For all $x, y \in P$, both $x + y \in P$ and $x \cdot y \in P$
2. If $x \in P$ and $-x \in P$ then $x = 0$
3. For all $x \in F$, either $x \in P$ or $-x \in P$.

It is easy to check that if we write $a \leq b$ provided $b - a \in P$, then $\leq$ is an order on F. Thus we will freely switch between calling $\leq$ and P orderings on a field, as is convenient. Additionally, we will often refer to F or (F, P) as an ordered field instead of $(F, \leq)$. Note that our definition has $0 \in P$, as in [17], although in [10] and [11] this is not the case. If $0 \notin P$, then the order defined by P is strict, i.e., $a < b$ provided $b - a \in P$.

For any field F with an ordering P, the set of squares in F, which we denote by F^2, is a subset of P, as $x^2 = (-x)^2$ and either x or $-x$ is in P. Since P is closed under addition, the set of elements of F which are sums of squares, denoted by S_F, is also a subset of P. Also, since $1 \in P$, we immediately see that -1 is not a sum of squares in F.

Definition 1.1.3. A field F is *formally real* (or simply *real*) provided -1 is not a sum of squares in F.

So every ordered field is formally real. The converse is also true:

Theorem 1.1.4 (Artin-Schrier)**.** Let F be a field. Then F is formally real if and only if F is orderable.

Note that for any formally real field, $\sum a_i^2 = 0$ implies $a_i = 0$. Since 1 is a square, we will thus never have $1 + 1 + \cdots + 1 = 0$, so every formally real field, and as such ever ordered field, has characteristic 0.

Given a formally real field F, the algebraic closure of F is no longer real since $x^2 + 1 = 0$ has a root in the algebraic closure, making -1 a square. If we

consider a maximal algebraic extension of a real field which is still real, we get a real closure.

Definition 1.1.5. A field F is *real closed* if F is formally real and no algebraic extension of F is formally real.

Definition 1.1.6. A real closure R_F of a field F is a real closed field which is algebraic over F.

Every formally real field has a real closure, although it need not be unique. However, if we consider ordered fields, uniqueness is guaranteed:

Theorem 1.1.7 (Artin-Schreier)**.** Any ordered field (F, P) has a unique (up to isomorphism) real closure.

Real closed fields are particularly nice for a variety of reasons. They admit a unique ordering: P is exactly the squares (every sum of squares in a real closed field is itself a square). In a real closed field R, every polynomial of odd degree with coefficients in R has a root in R. Also, $R(\sqrt{-1})$ is necessarily the algebraic closure of R. Real closed fields are also nice from a model theory point of view: the theory of real closed fields (in the language of ordered rings) is a complete, decidable theory. This implies that any two real closed field are elementarily equivalent. Since the real numbers, as an ordered field, are a real closed field, this says that any real closed field shares all the first order algebraic and order-theoretic properties of $\mathbb{R}$ (this is called the "Tarski-Principle").

Another nice property we will make heavy use of is that it is possible to determine the number of roots of a given polynomial in a real closed field. There are multiple ways to do this. One way is to use the fact that the theory of real closed fields is complete and decidable. Alternatively, we can appeal to the purely algebraic Sturm's Theorem, which we now discuss in more detail.

Theorem 1.1.8 (Sturm's Theorem)**.** Let $p(x)$ be any polynomial with coefficients in a real closed field R. Then there is a sequence of polynomials

$$p_0(x), p_1(x), \ldots, p_n(x)$$

such that if $p(\alpha) \neq 0$ and $p(\beta) \neq 0$, then the number of distinct roots of $p(x)$ in the interval $[\alpha, \beta]$ is $V_\alpha - V_\beta$, where V_γ denotes the number of variations in sign of $\{p_0(\gamma), p_1(\gamma), \ldots, p_n(\gamma)\}$.

The polynomials $p_0(x), p_1(x), \ldots, p_n(x)$ can be found effectively. In fact, $p_0(x) = p(x)$, $p_1(x) = p'(x)$ and for $i \geq 2$, $p_i(x)$ is the negative remainder after dividing $p_{i-1}(x)$ by $p_{i-2}(x)$. Since we will be concerned with computable real closed fields, we will be able to calculate $p_i(\gamma)$ for any γ in R and $i = 0, \ldots, n$. Thus we will be able to effectively find V_γ, and as such, the number of roots of $p(x)$ between any α and β which are not roots of $p(x)$. What's more, as there is a bound (due to Cauchy) on the roots of a given polynomial, this allows us to effectively determine the total number of roots of a given polynomial. (For a detailed discussion of Sturm's Theorem, and its proof, see [10].)

The real closure of a field is an algebraic extension, but we will also consider field extensions which are not algebraic. Recall that for any field F (ordered or otherwise) a set $S \subseteq F$ is *algebraically dependent* if for some $n \in \mathbb{N}$ there is a nonzero polynomial $p \in \mathbb{Q}[x_1, \ldots, x_n]$ and distinct $s_1, \ldots, s_n \in S$ such that $p(s_1, \ldots, s_n) = 0$. S is *algebraically independent* if it is not algebraically dependent. A maximal algebraically independent set in F is call a *transcendence basis* for F over $\mathbb{Q}$. The *transcendence degree* of a field F is the cardinality of some transcendence basis for F. Every non-algebraic extension field of $\mathbb{Q}$ has a transcendence basis over $\mathbb{Q}$, and all transcendence bases of a given field have the same cardinality, so these are well defined (see [9]). One can also prove that for any field F, if F is an extension of $\mathbb{Q}$ and has a transcendence basis S, then F is algebraic over the field $\mathbb{Q}(S)$. The field $\mathbb{Q}(S)$ is a *purely transcendental* extension of $\mathbb{Q}$, with a *pure transcendence basis* S. Note that every purely transcendental extension has a pure transcendence basis, but also has transcendence bases which are not pure. (All of this also works for extensions of arbitrary fields instead of $\mathbb{Q}$, but we will only need to consider this simplest of cases.)

Finally, we consider the possibility of infinite elements in an ordered field.

Definition 1.1.9. For any element a in an ordered field F, define the *absolute value of* a by

$$|a| = \begin{cases} a & \text{if } 0 \leq a \\ -a & \text{if } a < 0 \end{cases}$$

Definition 1.1.10. An ordered field F is *archimedean* if for all $a \in F$ there is some $n \in \mathbb{N}$ such that $|a| \leq n$.

If an ordered field is not archimedean, then it contains infinite elements. In this case we would like to say how various infinite elements are related. For ordered groups this is done by considering the archimedean classes. Two nonzero elements x and y, are *archimedean equivalent* if there is some $n \in \mathbb{N}$ such that $|x| \leq n|y|$ and $|y| \leq n|x|$. This is the only case needed for groups, since the only operation is addition. With multiplication, it is possible for elements in different archimedean classes to be even "farther apart." We will say that elements x and y are *multiplicatively archimedean equivalent* if $|x| \leq |y|^n$ and $|y| \leq |x|^n$, where n is some positive integer if $|x|, |y| > 1$ or some negative integer if $0 < |x|, |y| < 1$. For example, if x is infinite, then x and x^2 are not archimedean equivalent - they are in different archimedean classes. But x and x^2 are in the same multiplicatively archimedean class. For an infinite element y to be multiplicatively archimedean above x, it must be that y is greater than any power of x. We modify the usual notation for archimedean equivalence as follows:

Notation 1.1.11. $x \approx_a y$ means x and y are (additively) archimedean equivalent. $x \ll_a y$ means x is (additively) archimedean below y, i.e., $x < y$ and x and y are in different (additively) archimedean classes. $x \approx_m y$ means x and y are multiplicatively archimedean equivalent. $x \ll_m y$ means x is multiplicatively archimedean below y.

These definitions will be made precise when they are needed. Note though that there is no difference between an archimedean field and a multiplicatively archimedean field. That is, if the ordered field has no elements (additively) archimedean above the natural numbers, then there is no element multiplicatively archimedean above the natural numbers either.

1.2 Computable Ordered Fields

Now we turn to questions of computability. We assume familiarity with the basic ideas from computability theory (otherwise, see [19]). Intuitively, an ordered field will be computable if the operations $+$ and $\cdot$ are computable, and the relation $\leq$ is computable. While this is often enough for us, we will now be more precise. We work in the language of ordered rings, so a field F will have a domain $|F|$ and there will be binary function symbols $+_F$ and $\cdot_F$, a binary relation $\leq_F$, and distinguished elements 0_F and 1_F. For F to be a *computable* ordered field, $|F|$ will be a computable subset of $\mathbb{N}$, with $+_F$ and $\cdot_F$ partial computable functions from $F \times F$ to F, and $\leq_F \subseteq F \times F$ a computable relation. Additionally, we are given the elements 0_F and 1_F computably, although these can always be found uniformly by searching through the elements of the field. Of course we want F to be an ordered field, so the usual ordered field axioms must be satisfied. There will be times when we want to consider fields (or rings) without an order, and in these cases, we simply drop $\leq_F$ from our language, and restrict the axioms accordingly.

Note that since the domain of F is a subset of $\mathbb{N}$, computable ordered fields (and in general all computable algebraic structures) are necessarily countable.

Elements of fields have both additive and multiplicative inverses, and our definition would not be very good if subtraction and division were not computable functions as well. But these are computable in any computably ordered field. To compute a^{-1} in F, we can simply search through all elements of $|F|$ until we find some b so that $a \cdot b = 1_F$. Since F is a field, such a b will eventually be found, and we can set $b = a^{-1}$. Similarly for $-a$.

Ordered fields necessarily have characteristic 0, so the rationals $\mathbb{Q}$ are contained in every ordered field. If F is a computable ordered field, we can locate any given rational q. That is, we can determine which element of the domain of F corresponds to q. If $q = a/b$ where a and b are integers, we simply compute the sum of 1_F with itself a times, and divide that by the sum of 1_F with itself b times. However, while it is possible to find any rational in F, the subfield of F isomorphic to $\mathbb{Q}$ need not be computable. Given an element $a \in F$, there may be no algorithm which determines whether or not a is rational. The rationals do form a computably enumerable (c.e.) subset of F, but there is no way to know when an element is *not* a rational, unless the field were presented in a particularly nice way.

This brings us to the distinction between a computable field and a computable copy (or presentation) of that field. Consider the example $\mathbb{Q}(\sqrt{2})$ with

the standard order. To see that this field is computable we must give a computable subset $|F|$ of $\mathbb{N}$, computable functions $+_F$ and $\cdot_F$, a computable relation $\leq_F$ and elements 0_F and 1_F so that $F = (|F|, +_F, \cdot_F, 0_F, 1_F, \leq_F)$ is an ordered field, and in fact the ordered field $\mathbb{Q}(\sqrt{2})$ (so really, there is a field isomorphism $\varphi : |F| \to \mathbb{Q}(\sqrt{2})$). In other words, we must produce a *computable copy* of the field. We could, for example, take $|F| = \mathbb{N}$, let the even number in $\mathbb{N}$ be rationals (relative to some fixed enumeration of $\mathbb{Q}$), let $1 \in \mathbb{N}$ be $\sqrt{2}$, and close under the field operations (in some well defined way) with the remaining odd numbers in $\mathbb{N}$. Of course we could have done this differently, and then we would have a different computable copy. So a field is computable if and only if there is at least one computable copy of the field. In what follows, when speaking of a computable field, we will either mean a particular computable copy of the field, or the isomorphism class of the field. In general, we will be as precise as the discussion requires.

One topic which specifically involves the computable copies of fields is computable dimensions. Two computable copies of a given ordered field are both isomorphic to the field, so isomorphic to each other. However, there is no guarantee that this isomorphism is computable. The computable dimension of F counts the number of computable copies of F, up to *computable isomorphism*. If a field has computable dimension 1, then every computable copy of F is computably isomorphic, so in some sense which computable copy we consider doesn't matter. Such fields are called *computably categorical*. A big open question in the study of

computable fields is which fields are computably categorical. This is known for algebraically closed fields, as well as real closed fields. In both cases, the field is computably categorical if and only if the transcendence degree of the field is finite. Further, if the transcendence degree is infinite, then the computable dimension is infinite (see [13] and [16]). Little is known beyond these two simplest of examples. There are fields with infinite transcendence degree which are computably categorical (see [15]), and fields with finite transcendence degree which are not (see [4] or [14]). It is unknown whether there are any fields with finite transcendence degree greater than 1.

1.3 Summary of Results

In chapter 2, we consider how to build computable ordered fields, and give examples of different ways to do this. One method of construction will allow us to build computable ordered fields for which F^2 and S_F (the squares in F and the set of sums of squares) are not computable. In fact, we show that either set can be as complicated as possible - the sets can compute the halting problem. Another method of construction will allow us to build a computable, non-archimedean ordered field with infinite transcendence degree. We will be able to build these fields so that c.e. linear orders, or the halting problem, can be coded into the infinite multiplicatively archimedean classes. Additionally, we will build a computable archimedean field with infinite transcendence degree which is purely transcenden-

tal and has a computable pure transcendence basis. This field will be useful in chapters 3 and 4.

Chapter 3 takes up the question of computable dimension. We will prove that computable ordered fields with finite transcendence degree are computably categorical (in fact, computably stable). This shows a major distinction between computable fields and computable ordered fields, since as we have mentioned, there are computable fields of finite transcendence degree which are not computably categorical. The case for ordered fields of infinite transcendence degree will be considered briefly, and we will show that in the simplest case these computable ordered fields have infinite transcendence degree. More specifically, we will show that any computable, purely transcendental archimedean field with an infinite computable pure transcendence basis has infinite computable dimension. Finally, we show that computable archimedean ordered fields, like real closed and algebraically closed fields, must either be computably categorical or have infinite computable dimension.

Chapter 4 will investigate how complicated transcendence bases can be in a computable ordered field. We will produce a computable ordered field in which every transcendence basis computes the halting problem. Additionally, we will build a computable ordered field in which every transcendence basis is immune. Both fields will be isomorphic to the computable archimedean field with computable pure transcendence basis built in chapter 2.

Finally, in chapter 5, we will change perspectives and consider questions of effectiveness in the theory of ordered fields from the viewpoint of reverse mathematics. We will expand on the work of Friedman, Simpson, and Smith in [5]. They showed the theorem that a field is formally real if and only if the field is orderable is equivalent to weak König's Lemma. We will prove similar equivalences for theorems about how partial orders on rings and fields can be extended to full orders on the ring or field, or to full orders on extension fields. The background for the reverse mathematics will be introduced at the beginning of the chapter.

Chapter 2

Building Computable Ordered Fields

In the chapters that follow, we shall consider various properties of computable ordered fields. First though, let us consider how such computable ordered fields arise.

2.1 Simple Examples

Recall that an ordered field F is computable if the field operations (addition and multiplication) as well as the order relation are computable. With this definition, it is easy to see that the rationals, with their natural order, form a computable ordered field. Similarly, if we take any finite algebraic extension of $\mathbb{Q}$, as long as the extension field is an ordered field, it will be computable. (There are of course algebraic extensions of $\mathbb{Q}$ which are not formally real, so cannot be ordered. These will be computable fields, without any order.) Further, if we form the real closure of an ordered field, we will arrive at a computable ordered field.

Theorem 2.1.1 (Madison [12])**.** Given any computable ordered field F, the real

closure R_F of F, with its unique order extending the order of F, is a computable ordered field.

2.2 Archimedean Fields

A useful method of constructing a computable ordered field is to build it inside of a real closed field. Consider the field $\mathbb{Q}(\sqrt{p}_i)_{i\in\mathbb{N}}$, where p_i is the ith prime. For each p_i, we can either insist that $\sqrt{p_i}$ is positive, or that it is negative. Thus there are $2^{\aleph_0}$ many distinct orderings of the field. So there are (uncountably) many orderings of the field which are not computable. However, with the standard ordering (as a subset of $\mathbb{R}$), the field is a computable ordered field.

Proposition 2.2.1. $F = \mathbb{Q}(\sqrt{p_i})_{i\in\mathbb{N}}$ with the standard ordering is a computable ordered field.

Proof. We will represent elements of the field as natural numbers. In order to define addition, multiplication and the order relation, we will build a computable injection $\alpha : \mathbb{N} \to R_{\mathbb{Q}}$, such that the range of α is exactly F. Once such an α is constructed, it will be possible to compute the sum or product of two elements as follows: for $m, n \in \mathbb{N}$, we define $m +_F n = \alpha^{-1}(\alpha(m) + \alpha(n))$ and $m \cdot_F n = \alpha^{-1}(\alpha(m) \cdot \alpha(n))$. That is, to compute the sum or product of two elements, we find their image under α, compute their sum or product in the real closure of $\mathbb{Q}$, then find the pre-image of the result. Similarly, we say $m \leq_F n$ exactly when $\alpha(m) \leq \alpha(n)$.

We build such an α in stages, so that by stage s, we have defined α on all natural numbers less than s. We fix an enumeration of $\mathbb{Q}$. At stage $s = 0$, define $\alpha(0) = 0_{\mathbb{Q}}$, and at stage $s = 1$, define $\alpha(1) = 1_{\mathbb{Q}}$. At all subsequent stages, define $\alpha(s)$ in one of six possible ways:

$s = 6k$: Set $\alpha(s)$ to be the least element in the enumeration of $\mathbb{Q}$ not already in the range of α.

$s = 6k + 1$: Set $\alpha(s)$ to be $\sqrt{p_{k+1}}$.

$s = 6k + 2$: Set $\alpha(s)$ to be $\alpha(m) + \alpha(n)$ for the lexicographically-least pair (m, n) for which m, n are in the range of α but $\alpha(m) + \alpha(n)$ is not.

$s = 6k + 3$: Set $\alpha(s)$ to be $\alpha(m) \cdot \alpha(n)$ for the lexicographically-least pair (m, n) for which m, n are in the range of α but $\alpha(m) \cdot \alpha(n)$ is not.

$s = 6k + 4$: Set $\alpha(s)$ to be $-\alpha(m)$ for the least m such that m is in the range of α but $-\alpha(m)$ is not.

$s = 6k + 5$: Set $\alpha(s)$ to be $\alpha(m)^{-1}$, for the least m such that m is in the range of α but $\alpha(m)^{-1}$ is not.

If at any of the latter four stages there is no (m, n) or m satisfying the condition, then simply define $\alpha(s)$ to be the least element in the enumeration of $\mathbb{Q}$ not already in the range of α. Defined in this way, α is clearly a computable function, and is injective. Also, the range of α contains every rational and each

$\sqrt{p_i}$ for $i \in \mathbb{N}$, and is closed under addition, multiplication, and inverses of each. Thus the range of α is precisely F as a subfield of $R_{\mathbb{Q}}$. *QED*

Using this method of building ordered fields, we can build fields which have certain computability-theoretic properties. For example, it is possible to build an ordered field such that the set of squares (denoted F^2) is not computable. In fact, the set of squares can be as complicated as the halting problem (which we always denote by K).

Theorem 2.2.2. There is a computable ordered field F such that $K \leq_1 F^2$.

Proof. We will take $F = \mathbb{Q}(\sqrt{p_i})_{i \in K}$, with the standard ordering. To show that F is computable, we define a computable injection $\alpha : \mathbb{N} \to R_{\mathbb{Q}}$ whose range is F. To define α, we proceed as in the proof above, alternately assigning $\alpha(s)$ to be a rational, a sum or product of elements already in the range of α, additive or multiplicative inverse of an element already in the range of α, or $\sqrt{p_i}$ for $i \in K$. This last assignment is accomplished by waiting for a new element to be enumerated into K and then proceeding. Thus the range of α will contain all rationals as well as $\sqrt{p_i}$ for all $i \in K$, and will be closed under addition and multiplication, so the range will be exactly F. Therefore F is computable. Finally, note that $K \leq_1 F^2$, since $i \in K$ if and only if $\sqrt{p_i} \in F$ if and only if p_i is a square in F. *QED*

Alternatively, we can code K into the set of elements which are sums of

squares. Recall, we let S_F be the set of all elements of F which are sums of squares.

Theorem 2.2.3. There is a computable ordered field F such that $K \leq_1 S_F$.

Proof. This time take $F = \mathbb{Q}(\sqrt{p_i}, \sqrt[4]{p_j})_{i\in\mathbb{N}, j\in K}$, with the standard ordering. To see that F is computable, we again build a computable injection $\alpha : \mathbb{N} \to R_{\mathbb{Q}}$ with F equal to the range of α. To build α, alternately define $\alpha(s)$ to be a rational, $\sqrt{p_i}$, $\sqrt[4]{p_j}$ for $j \in K$ (by waiting for the next element of K to appear), and sums, products, additive inverses, and multiplicative inverses of elements already in the range of α. To see that $K \leq_1 S_F$, note that while every positive rational is a sum of squares, $\sqrt{p_j}$ is a sum of squares if and only if $\sqrt[4]{p_j}$ is in F. As this occurs exactly when $j \in K$, we can effectively determine K using S_F. *QED*

Remark 2.2.4. In both the previous constructions, note that the order played no role. Indeed we could ignore the order completely to construct computable fields in which the squares, or sums of squares, compute K. Also, note that K is the best we can do, in both cases, as both F^2 and S_F are Σ^0_1 sets:

$$x \in F^2 \iff \exists y(y^2 = x)$$

$$x \in S_F \iff \exists n \exists y \left(y = \langle a_1, \ldots, a_n \rangle \wedge \sum_{i=1}^{n} a_i^2 = x \right).$$

One might wonder whether our coding of K into F^2 or S_F was purely a function of our construction method. Might there be another way to present these

ordered fields in which the squares or sums of squares were less complicated? This is not the case.

Corollary 2.2.5. There is a computable ordered field F such that $K \leq_1 F^2$ in every computable copy of F, as well as a computable ordered field F' such that $K \leq_1 S_{F'}$ in every computable copy of F'.

Proof. Let $F = \mathbb{Q}(\sqrt{p_j})_{j\in K}$ and $F' = \mathbb{Q}(\sqrt{p_i}, \sqrt[4]{p_j})_{i\in\mathbb{N},j\in K}$ as above. Now regardless of the computable copy, we have the 1 element of these fields. Thus it is a simple matter to locate p_j, as it is $1+1+\cdots+1$ with p_j summands. To determine whether $j \in K$, we can simply ask whether this element found to be p_j is in F^2. Similarly, we have $\sqrt{p_i} \in F'$ for all i, so we can search through the elements of F' until we find some c such that $c^2 = p_i$ and $c \geq 0$. Then c corresponds to the positive square root of p_i. We can then ask whether c is in $S_{F'}$ and the answer will tell us whether $i \in K$. *QED*

Remark 2.2.6. If we do not insist that the fields in the above corollary are ordered, then the fields constructed without the orders are still Turing equivalent to the halting problem. Particularly, when searching for a square root of p_i in F', we can find both roots (as they are both in F') and then ask whether either is in $S_{F'}$. We thus have a *tt*-reduction (instead of a 1-reduction, as in the ordered case) from F^2 or $S_{F'}$ to K.

In all of the ordered fields we have constructed so far, we have used the same

technique to verify that the field is computable. The process can be generalized, which will be useful later.

Theorem 2.2.7. Let F be a computable ordered field and E a subfield of F. Suppose $E = \mathbb{Q}(S)$ for some infinite c.e. $S \subseteq F$, such that for any $a \in S$, $a \notin \mathbb{Q}(S \setminus \{a\})$. Then E is a computable ordered field, and S is a computable subset of E.

Proof. The construction of a computable copy of E is as before: we build a computable injection $\alpha : \mathbb{N} \to F$ with range $\mathbb{Q}(S)$. That S is a computable subset of E follows from the fact that in the construction, we will define $\alpha(s)$ to be an element of S exactly at stages where $s = 6k + 1$ for some k. The condition that $a \notin \mathbb{Q}(S \setminus \{a\})$ for any $a \in S$ guarantees that no element of S will be the image of any natural number which is not 1 mod 6 - we don't put an element of S into the range of α when closing under the field operations. *QED*

2.2.1 Making an infinite transcendence basis computable

So far, all examples of computable ordered fields have been algebraic extensions of the rationals. This need not be the case. However, dealing with transcendental elements can complicate matters. Specifically, it is more complicated to effectivly define the order on the field. There are exactly two orders which can be placed on $\mathbb{Q}(\sqrt{2})$ - one in which $\sqrt{2} > 0$ and one in which $\sqrt{2} < 0$. However, there are uncountably many orderings of $\mathbb{Q}(t)$, each corresponding to a lower cut of

the rationals (in addition to non-archimedean orders). Thus while it is a simple matter to see that $\mathbb{Q}(t)$ is a computable field, viewing elements as formal quotients of polynomials in t, to build the field as a computable *ordered* field is more challenging.

One way to accomplish this is to identify t with a real number known to be transcendental. To see how this works, let us show that $\mathbb{Q}(e^a)$ for $a \in \mathbb{Q}$ is a computable ordered field.

Proposition 2.2.8. If $a \in \mathbb{Q}$, the ordered field $\mathbb{Q}(e^a)$ under the standard ordering is a computable ordered field.

Proof. If $a = 0$, then $e^a = 1$, so $\mathbb{Q}(e^a) = \mathbb{Q}$, obviously a computable ordered field. If $a \neq 0$, then e^a is transcendental. Thus $\mathbb{Q}(e^a) \cong \mathbb{Q}(t)$ (as fields). As a field, $\mathbb{Q}(t)$ is clearly computable. Elements are simply quotients of polynomials in t, and adding and multiplying the polynomials can be carried out in the usual way. To form $\mathbb{Q}(t)$ as an ordered field (in fact the ordered field $\mathbb{Q}(e^a)$) we must define a computable order relation.

This is accomplished by effectively giving a Cauchy sequence $\langle q_i \rangle_{i \in \mathbb{N}}$ of rationals for each element of $\mathbb{Q}(e^a)$ such that $|q_k - q_{k+i}| < 2^{-k}$ for all k and i. With such a sequence we can effectively determine whether $l = \lim q_i \neq 0$ is positive or negative. We look through the sequence until we find a q_k such that $|q_k| > 2^{-k}$. There must be such a q_k because $l \neq 0$ and for each k, $|q_k - l| \leq 2^{-k}$, so as soon as q_k is closer to l than to 0, $|q_k| > 2^{-k}$. But since $|q_k - l| \leq 2^{-k}$ and $|q_k| \geq 2^{-k}$,

it must be that the sign of q_k is the same as l, so we can determine whether l is positive or negative. (In general, it is not possible to decide whether a sequence of this sort converges to zero, but we will give 0 the constant 0 sequence, and all other sequences will converge to some non-zero element of $\mathbb{Q}(e^a)$.)

Now if we have such sequences for x and y in $\mathbb{Q}(t)$, then we can find similarly nice sequences for $x+y$, $x\cdot y$, $-x$ and x^{-1}. Thus to show that $\mathbb{Q}(e^a)$ is a computable ordered field, all we must do is to give such a sequence whose limit is e^a.

We use the Taylor approximation of e^x about 0. Let

$$P_n(x) = \sum_{k=0}^{n} \frac{x^k}{k!}.$$

Then by Taylor's Theorem, we have

$$|e^x - P_n(x)| \leq \frac{M}{(n+1)!} x^{n+1}$$

where M is the maximum value of e^x on the interval between 0 and x. In particular, we can easily calculate an acceptable rational M by finding some natural number $m > x$ and taking

$$M = \max\{3^m, 3\}$$

To define the Cauchy sequence for e^a, we can then take a subsequence of $\{P_n(a)\}_{n\in\mathbb{N}}$ so that the error terms are bounded correctly. That is, we take the sequence

$$\left\{ P_{n_k}(a) \;\middle|\; \frac{Ma^{n+1}}{(n+1)!} < 2^{-k} \right\}.$$

Such a subsequence can be found for any $a \in \mathbb{Q}$, so $\mathbb{Q}(e^a)$ is a computable ordered field. *QED*

Using the technique outlined in the above proof, we can easily see that $\mathbb{Q}(e^a, e^b)$ is a computable ordered field for any rationals a and b with $\{e^a, e^b\}$ algebraically independent. In fact, we could adjoin an infinite number of reals of the form e^a in this fashion. Further generalizing, we get the following.

Theorem 2.2.9. Let F be a computable ordered field contained in $\mathbb{R}$. If there is a set $\{a_0, a_1, \ldots\} \subset F$ such that $\{e^{a_0}, e^{a_1}, \ldots\}$ is algebraically independent over F, then $\widehat{F} = F(e^{a_i})_{i \in \mathbb{N}}$ under the standard ordering is a computable ordered field.

Proof. We present the field as $F(x_0, x_1, \ldots)$, so that addition and multiplication are automatically computable functions. To define a computable order, we associate with each element of $F(x_0, x_1, \ldots)$ a Cauchy sequence of elements of F as described in the proof of Proposition 2.2.8. To see that we can do this effectively, we must show that we can produce such a sequence for each x_i uniformly in i. In fact, we want the sequence for x_i to converge to e^{a_i}. We get the sequences for e^{a_i} by taking appropriate subsequences of $\{P_n(a_i)\}_{n \in \mathbb{N}}$. Since $a_i \in F$, $P_n(a_i)$ is an element of F, and can be found since F is computable. We can find an appropriate subsequence using Taylor's Theorem to compute a bound for $|e^{a_i} - P_n(a_i)|$ for each n. *QED*

For this theorem to be applicable, we must have a way of knowing that

$\{e^{a_0}, e^{a_1}, \ldots\}$ is algebraically independent. This is given to us by the Lindermann-Weierstrass Theorem:

Theorem 2.2.10 (Lindermann-Weierstrass)**.** If $a_0, a_1, \ldots, a_n$ are algebraic numbers that are linearly independent over $\mathbb{Q}$, then

$$e^{a_0}, e^{a_1}, \ldots, e^{a_n}$$

are algebraically independent over $\mathbb{Q}$.

Now since $\{\sqrt{2}, \sqrt{3}, \sqrt{5}, \ldots, \sqrt{p_i}, \ldots\}$ is a linearly independent set of algebraic numbers, the theorem tells us that $\{e^{\sqrt{2}}, e^{\sqrt{3}}, \ldots, e^{\sqrt{p_i}}, \ldots\}$ is algebraically independent over $\mathbb{Q}$. But then the set is also algebraically independent over $\mathbb{Q}(\sqrt{p_i})_{i\in\mathbb{N}}$. Putting this all together, we get the following.

Proposition 2.2.11. There is a computable ordered field with infinite transcendence degree.

Proof. Let $E = \mathbb{Q}(\sqrt{p_i})_{i\in\mathbb{N}}$. Then E is a computable ordered field by Proposition 2.2.1. By the Lindermann-Weierstrass Theorem, $\{e^{\sqrt{p_i}} \mid i = 1, \ldots, n\}$ is algebraically independent over $\mathbb{Q}$, and so also over E, for each n. Now let $F = \mathbb{Q}(\sqrt{p_i}, e^{\sqrt{p_i}})_{i\in\mathbb{N}}$. Then F has infinite transcendence degree, and by Theorem 2.2.9 is a computable ordered field. *QED*

In the following chapters, we will prove results about a particularly nice class of computably ordered fields, of which the following proposition guarantees existence.

Proposition 2.2.12. There exists a computable, archimedean ordered, purely transcendental extension of $\mathbb{Q}$ with an infinite computable pure transcendence basis.

Proof. We take our field to be $E = \mathbb{Q}(e^{\sqrt{p_i}})_{i\in\mathbb{N}}$, with the ordering of the reals. Let $F = \mathbb{Q}(\sqrt{p_i}, e^{\sqrt{p_i}})_{i\in\mathbb{N}}$, as in Proposition 2.2.12. Since $S = \{e^{\sqrt{p_i}} \mid i \in \mathbb{N}\}$ is a computable subset of F and is algebraically independent (so $a \notin \mathbb{Q}(S \setminus \{a\})$ for any $a \in S$), by Theorem 2.2.7 we see that E is a computable ordered field with computable pure transcendence basis S. Clearly E is purely transcendental and archimedean. *QED*

2.3 Non-Archimedean Fields

We now turn to the task of building non-archimedean ordered fields. The fields will always be of the form $\mathbb{Q}(t_i)_{i\in I}$ for some set I of natural numbers. We will represent elements simply as formal quotients of polynomials in the variables t_i, and as such addition and multiplication will automatically be computable functions. We will need to work to ensure that the order relation is computable. The difficulties arise in trying to describe how to determine which of two elements is larger, and in succinctly describing how the elements are ordered (which is necessary for the sake of building ordered fields with interesting computability-theoretic properties). To simplify this process, we will work almost entirely with computable ordered rings, and then take the field of fractions as our computable ordered field. Thus

we must first verify that it is possible to move from a computable ordered ring to the ring's field of fractions to get a computable ordered field.

Lemma 2.3.1. If A is any computable ordered ring, then there is a uniform procedure to pass from A to its computable ordered field of fractions.

Proof. Given a presentation of A, we present F as formal quotients of the non-zero elements of A. Addition and multiplication are performed in the standard way, and since these operations are computable in A, they are computable functions on F. Presented in this way, there are many elements which are equal, so we must verify that equality is a computable relation. Given $a/b, c/d \in F_A$, where $a, b, c, d \in A$, we note that

$$\frac{a}{b} = \frac{c}{d} \text{ if and only if } ad = cb,$$

and since A is computable, we can decide whether $ad = cb$. Similarly, to determine whether $a/b < c/d$, we note

$$\frac{a}{b} < \frac{c}{d} \iff (ad < bc \wedge bd > 0) \vee (ad > bc \wedge bd < 0).$$

QED

Example 2.3.2. $\mathbb{Q}[t]$, such that $n < t$ for all natural numbers n is a computable ordered ring. Elements are simply polynomials in the variable t, and are added and multiplied as such. Given $a, b \in \mathbb{Q}[t]$, we can determine whether $a < b$ by checking the sign of the coefficient of the highest degree term of $b - a$. By taking

the field of fractions, we see that $\mathbb{Q}(t)$, ordered such that $n < t$ for all natural numbers n, is a computable ordered field.

Example 2.3.3. $\mathbb{Q}[t_0, t_1]$, such that $n < t_0$ and $t_0^n < t_1$ for all $n \in \mathbb{N}$, is a computable ordered ring. Elements are polynomials in the variables t_0 and t_1, so addition and multiplication are automatically computable. To determine whether $a < b$ for a given a and b in the ring, we again determine whether $b - a$ is positive. This is done by writing $b - a$ in the form

$$p_0(t_0) + p_1(t_0)t_1 + \cdots + p_{n-1}(t_0)t_1^{n-1} + p_n(t_0)t_1^n$$

where $p_0(t_0), \ldots, p_n(t_0)$ are all polynomials in $\mathbb{Q}[t_0]$. Then $b - a$ is positive exactly when $p_n(t_0)$ is positive. We can determine whether $p_n(t_0)$ is positive exactly as in Example 2.3.2.

Taking the field of fractions, we find that $\mathbb{Q}(t_0, t_1)$ with the order defined by $n < t_0$ and $t_0^n < t_1$ for all $n \in \mathbb{N}$ is a computable ordered field.

In this example, we were able to get away with a relatively simple description of the order on the ring: t_0 is archimedean above 1 and t_1 is archimedean above every power of t_0. If we keep the transcendental elements spread out as much as possible in this way, we can get a computable ordered field with infinitely many infinite algebraically independent elements:

Example 2.3.4. $\mathbb{Q}(t_i)_{i \in \mathbb{N}}$ with the order defined by $n < t_0$ and $t_i^n < t_j$ for all $n \in \mathbb{N}$ and $i < j$ is a computable ordered field.

In the examples above, the key step in verifying that the ring was computable was to give a procedure to determine the sign of an element. This was done by noting that the sign of

$$p = a_0 + a_1 t_i + \cdots + a_n t_i^n$$

was determined by the sign of a_n. Let us be a little more careful about stating this fact, as it will be needed in the more complicated proofs below. Recall that $x \ll_a y$ means $n|x| < |y|$ for all $n \in \mathbb{N}$.

Lemma 2.3.5. Let A be an ordered ring which embeds into $\mathbb{Q}[t_i]_{i\in\mathbb{N}}$ with all t_i infinite (i.e., $1 \ll_a t_i$). Let $a, b, t \in A$, and suppose $t > 0$, $a \ll_a t$, and $a + bt \neq 0$. Then the sign of $a + bt$ is identical to the sign of b.

Consequently, if $p = a_0 + a_1 t + \cdots + a_n t^n$ with $a_0, \ldots, a_n \ll_a t$ and $p \neq 0$, then the sign of p is identical to the sign of a_n.

Proof. Note that A contains no infinitesimal elements. In particular, there is some $n \in \mathbb{N}$ such that $\frac{1}{n} < |b|$. Suppose first that $b > 0$ but contrary to stipulation, $a + bt < 0$. Since $bt > 0$, we must have that $a < 0$. In fact, we have $bt < |a|$. But $\frac{1}{n}t < bt$, so $t < n|a|$, contradicting the hypothesis that $a \ll_a t$. Conversely, suppose $b < 0$ but $a + bt > 0$. Since $bt < 0$, we must have $a > 0$, and in fact $|a| > |bt|$. But then again, $|a| > |b|t > \frac{1}{n}t$, contradicting the hypothesis. Therefore, $a + bt > 0$ if and only if $b > 0$, as required.

To see that the sign of p is the sign of a_n, note that if $a_0, \ldots, a_n \ll_a t$,

then $a_i t^k \ll_a t^{k+1}$ for all $i \in \{0, \ldots, n-1\}$ and $k \in \mathbb{N}$. Thus $a_i t^k \ll_a t^n$ for all $i \in \{0, \ldots, n-1\}$, $k \leq n$, and as such

$$a_0 + a_1 t + \cdots + a_{n-1} t^{n-1} \ll_a t^n.$$

Now we can apply the first half of the lemma with $a = a_0 + \cdots + a_{n-1} t^{n-1}$, $b = a_n$ and $t = t^n$. *QED*

2.3.1 Coding into Multiplicatively Archimedean Classes

Definition 2.3.6. We say two elements x and y in an ordered ring A are *multiplicatively archimedean equivalent* (written $x \approx_m y$) provided either

- $|x|, |y| > 1$ and there is some $n \in \mathbb{Z}^+$ such that $|x| \leq |y|^n$ and $|y| \leq |x|^n$, or
- $0 < |x|, |y| < 1$ and there is some $n \in \mathbb{Z}^-$ such that $|x| \leq |y|^n$ and $|y| \leq |x|^n$.

Definition 2.3.7. We say y is *multiplicatively archimedean above* x or x is *multiplicatively archimedean below* y (written $x \ll_m y$) provided $|x| < |y|$ and x is not multiplicatively archimedean equivalent to y.

Clearly, $\approx_m$ is an equivalence relation. The multiplicatively archimedean classes of an ordered ring A are the equivalence classes under $\approx_m$. When we code into the multiplicatively archimedean classes, we will only code into the infinite classes - those classes whose members are infinite.

Let $\mathrm{Arch}^\times(A) = \{(x, y) \in A \times A \mid x \approx_m y\}$. We wish to see how complicated the relation can be for a computable ordered field.

Theorem 2.3.8. There is a computable ordered field F for which $\mathrm{Arch}^{\times}(F)$ is Turing equivalent to the halting problem.

Proof. For any computable ordered field F, checking whether a given pair (x, y) is in $\mathrm{Arch}^{\times}(F)$ is clearly Σ^0_1 so $\mathrm{Arch}^{\times}(F)$ is computable from K. We must build an ordered field F such that $K \leq_T \mathrm{Arch}^{\times}(F)$. In fact, we build a computable ordered ring A with this property such that the field of fractions of A is the required F.

Fix an enumeration $\{K_s\}_{s\in\mathbb{N}}$ of K for which exactly one element enters K_s at each $s \geq 2$ (so $K_0 = K_1 = \emptyset$). We will take A to be the ordered ring $\mathbb{Q}[t_i, u_i]_{i\in\mathbb{N}}$ where $u_n = t_n^s$ for exactly $n \in K_s \setminus K_{s-1}$. We specify that the ring is ordered such that $t_i \ll_a u_i \ll_m t_{i+1}$ for all $i \in \mathbb{N}$, with all t_i and u_i infinite. We claim that this describes a computable ordered ring.

Elements of A will simply be formal polynomials in the variables t_i and u_i, added and multiplied in the usual way (so addition and multiplication are computable). To show that A is a computable ordered ring, we must show that $\leq$ is a computable relation. Also, since our representation of A allows different looking elements to be equal, we must verify that we can tell when two elements are in fact equal. All of this will be accomplished if we can give an algorithm to determine the sign (positive, negative, or zero) of a given polynomial $p \in A$. By the index of a polynomial p, we shall mean the largest n such that either t_n or u_n (or both) appear in p. We show the existence of such an algorithm by induction on the index of p.

If the index of p is 0, then we can write p as

$$p = a_0 + a_1 u_0 + a_2 u_0^2 + \cdots + a_n u_0^n$$

where $a_0, a_1, \ldots, a_n$ are all polynomials in $\mathbb{Q}[t_0]$, of degree no more than (say) m. The first thing we do is to check whether $0 \in K_m$. If so, then we find the $\widehat{m} \leq m$ such that $t_0^{\widehat{m}} = u_0$ and make the proper substitutions in p so that $a_0, \ldots, a_n$ have degree less than $\widehat{m}$. Then we rewrite the new p in the proper form (i.e., $p = a_0 + \cdots + a_n u_0^n$ for the new $a_0, \ldots, a_n$). If $0 \notin K_m$, then we leave p untouched. Now we can simply inspect p (the new version or the original, as the case may be) to decide the sign of p. The only way for p to be equal to 0 is for each of $a_0, \ldots, a_n$ to be 0. Because we reduced p as needed, we have $t_0^k \ll_a u_0$, where k is the highest power of t_0 appearing in any of $a_0, \ldots, a_n$. Thus $a_0, \ldots, a_n \ll_a u_0$, so by Lemma 2.3.5, we will have $p > 0$ exactly when $a_n > 0$. We will have $a_n > 0$ exactly when the coefficient of the highest power of t_0 in a_n is positive. Clearly, all this can be checked computably.

Now suppose the index of p is j and we have algorithms to find the sign of any polynomial of index less than j. Again, write

$$p = a_0 + a_1 u_j + a_2 u_j^2 + \cdots + a_n u_j^n.$$

Here $a_0, \ldots, a_n$ can each be written as a polynomial in the variable t_j, with coefficients polynomials in t_i, and u_i for $i < j$. That is, the coefficients of t_j in each $a_0, \ldots, a_n$ have index less than j. Suppose m is the largest power of t_j to appear

in any of $a_0, \ldots, a_n$. Reduce p as needed (if $j \in K_m$, ensure that the largest power of t_j is less than $\widehat{m}$ for $j \in K_{\widehat{m}}$). With p properly reduced, the sign of p will be exactly the sign of a_n (again by Lemma 2.3.5, since $a_0, \ldots, a_n \ll_a u_j$). We write

$$a_n = b_0 + b_1 t_j + \cdots + b_l t_j^l.$$

The sign of a_n will be exactly the sign of b_l, which is a polynomial of index less than j. Thus we can find the sign of b_l effectively (by the inductive hypotheses), so we can find the sign of p.

Thus A is a computable ordered field. Since t_n and u_n are in the same multiplicatively archimedean class if and only if $n \in K$, we see that $K \leq_T \mathrm{Arch}^\times(A)$. Passing to F, the field of fractions of A, we still have that t_n and u_n are multiplicatively archimedean equivalent in F if and only if they were in A, so we conclude $K \leq_T \mathrm{Arch}^\times(F)$. *QED*

In a similar way, we can code any c.e. linear order into the multiplicatively archimedean classes of a computable ordered field.

Definition 2.3.9. A *c.e. linear order* is a countable linear order L for which there is a computably enumerable set $\leq_L \subset \mathbb{N} \times \mathbb{N}$ such that the relation $\approx_L$ defined by $m \approx_L n$ if and only if $m \leq_L n$ and $n \leq_L m$ is an equivalence relation, and L is isomorphic to $(\mathbb{N}/\approx_L, \leq_L)$.

The relation $\leq_L$ is reflexive, transitive, and total, but need not be antisymmetric (if it were, it would be a linear order). The idea here is that there is a

copy of the linear order, with elements represented by natural numbers, for which the $\leq$ relation is c.e. However, given two elements m and n, we can of course wait around for the enumeration of $\leq_L$ to give us an answer: either $m \leq_L n$ or $n \leq_L m$, so we can computably decide which of $m <_L n$ or $n <_L m$ does *not* hold (note the strict inequalities). What we cannot necessarily computably determine is whether $m \approx_L n$, since if m and n do not represent the same element of L, we would wait forever to be told otherwise.

To code such a linear order into the infinite multiplicatively archimedean classes of a field, we will specify the order of the infinite elements as we discover the order of L. So if the enumeration of $\leq_L$ says that $m \leq_L n$, we will make $t_m \leq_F t_n$. Then if it turns out that $m <_L n$ (so $n \leq_L m$ is never enumerated), then we will have $t_m \ll t_n$. If, on the other hand, $n \leq_L m$ is eventually enumerated, say at stage s, then we will set $t_m^s = t_n$, so that t_m and t_n are in the same multiplicatively archimedean class. We will need to be slightly more careful than this, since multiple elements of L can collaps at a single stage, but the basic strategy is the same: set $t_m \leq_F t_n$ if $m \leq_L n$ and then if m and n collaps to the same element of L, make sure that t_m and t_n are in the same class.

Actually we will build, like last time, a computable ordered ring A, and then pass to the field of fractions. For this to work, we need to know that doing so does not create any new infinite multiplicatively archimedean classes.

Lemma 2.3.10. Let A be an ordered ring isomorphic to $\mathbb{Q}[t_i]_{i\in\mathbb{N}}$ ordered so that

$t_i^n < t_j$ for all $i < j \in \mathbb{N}$ and $n \in \mathbb{N}$. Then the field of fractions $F \cong \mathbb{Q}(t_i)_{i\in\mathbb{N}}$ of A has the same infinite multiplicatively archimedean classes as A.

Proof. For each n, let A_n be the subring of A isomorphic to $\mathbb{Q}[t_0, \ldots, t_n]$. We will show by induction on n, that A_n has the same multiplicatively archimedean classes as its field of fractions F_n. This will be sufficient, since any $p/q \in F$, there is some n so that $p/q \in F_n$. Then if p/q is infinite, it will be multiplicatively archimedean equivalent to some infinite $a \in A_n$, so p/q cannot be in an infinite multiplicatively archimedean class which is not already in A. In all that follows, assume without loss of generality that p and q both positive. Note that if q is finite then q is rational, so then $p/q \in A$. Thus we also assume that p and q are infinite.

First consider the base case, $n = 0$. We have $A_0 \cong \mathbb{Q}[t_0]$, and $F_0 \cong \mathbb{Q}(t_0)$. Let p/q be an infinite element of F_0, with $p, q \in A_0$. Since $\mathbb{Q}$ is a field, we know $\mathbb{Q}[t_0]$ is a Euclidean domain. Thus there are polynomials m and r in $\mathbb{Q}[t_0]$ such that

$$p = mq + r,$$

with the degree of r strictly less than the degree of q. In F_0 then, we have

$$\frac{p}{q} = m + \frac{r}{q}$$

But $r/q < 1$ since the degree of q is greater than the degree of r. Thus if p/q is infinite, then it is in the same archimedean class as m, an element of A_0. So every

infinite element of F_0 is in the same archimedean class as an infinite element of A_0, so A_0 and F_0 have the same multiplicatively archimedean classes.

So suppose that we know that F_m has the same multiplicatively archimedean classes as A_m for all $m < n$. Consider some infinite $p/q \in F_n$, with p and q in A_n. If both p and q do not contain t_n, then $p/q \in F_m$ for some $m < n$, so by induction p/q is multiplicatively archimedean equivalent to some element of A_n as $A_m \subseteq A_n$. So suppose that p contains t_n. (Since p/q is infinite, we have $p > q$, so it cannot be that q contains t_n but p does not.) If q does *not* contain t_n, then $q^2 < p$, so

$$\left(\frac{p}{q}\right)^2 = \frac{p^2}{q^2} > \frac{p^2}{p} = p > \frac{p}{q}.$$

Thus p/q is in the same multiplicatively archimedean class as $p \in A_n$.

Finally suppose that both p and q contain an instance of t_n. Write p and q as polynomials in t_n with coefficients in A_{n-1}:

$$p = a_0 + a_1 t_n + a_2 t_n^2 + \cdots + a_k t_n^k$$

$$q = b_0 + b_1 t_n + b_2 t_n^2 + \cdots + b_{k'} t_n^{k'}$$

Since $p > q$, we have that $k \geq k'$. We consider the two cases.

Case 1 $k > k'$. Because $t_n^{k'-1} \ll_a t_n^{k'}$, and because each of $b_0, \ldots, b_{k'}$ is multiplicatively archimedean below t_n,

$$b_0 + b_1 t_n + \cdots b_{k'-1} t_n^{k'-1} < b_{k'} t_n^{k'}$$

(since $q > 0$, we know $b_{k'} t_i^{k'} > 0$). Thus for any $j \in \mathbb{N}$,

$$q^j = b_{k'}^j t_n^{jk'} + s(t_n) < b_{k'}^j t_n^{jk'} + t_n^{jk'} < t_n^{jk'+1}.$$

(Here $s(t_n)$ is some polynomial such that the largest exponent on any t_n is less than jk'.) Also, it is easy to see that $p^j > t_n^{jk-1}$, as

$$p^j = a_k^j t_n^{jk} + \widehat{s}(t_n) > t_n^{jk-1}.$$

Now since $k > k'$, we have $k \geq k'+1$ so $3k \geq 3k'+3$, and thus $3k-1 > 3k'+1$. So letting $j = 3$ in the above gives,

$$\left(\frac{p}{q}\right)^3 > \frac{t_n^{3k-1}}{t_n^{3k'+1}} > t_n \approx_m p,$$

so p/q is multiplicatively archimedean equivalent to p.

Case 2 $k = k'$. Consider p and q as elements in $F_{n-1}[t_n]$, which is a Euclidean domain since F_{n-1} is a field. Thus there are m and r in $F_{n-1}[t_n]$ such that

$$p = mq + r,$$

with the degree (in t_n) of r less than that of q. What's more, the degree (in t_n) of m is zero, since the degrees of p and q are equal. Then in F_n, we have

$$\frac{p}{q} = m + \frac{r}{q}.$$

But $r/q < 1$, so if p/q is infinite, then $p/q \approx_m m$. But m is an element of $F_{n-1}[t_n]$, with degree zero, so in fact an element of F_{n-1}. Thus by the inductive

hypothesis, m is multiplicatively archimedean equivalent to some $a \in A_{n-1}$. So p/q is multiplicatively archimedean equivalent to an element of A_n, as required.

QED

In the above proof, since we went on induction on n where A_n was a subring isomorphic to $\mathbb{Q}[t_0, \ldots, t_n]$, we arrive at the following corollary, which is what we will actual use in the proof of the theorem below.

Corollary 2.3.11. If A is an ordered ring isomorphic to $\mathbb{Q}[t_0, \ldots, t_n]$ for some n, ordered as in Lemma 2.3.10, then the field of fractions of A has the same infinite multiplicatively archimedean classes as A.

Now to the main theorem.

Theorem 2.3.12. Given a c.e. linear order L, there is a computable ordered field F such that any set of infinite multiplicatively archimedean representatives is isomorphic (as a linear order) to L.

Proof. We build a computable ordered ring A such that any set of infinite multiplicatively archimedean representatives is isomorphic (as a linear order) to L. We will take $A = \mathbb{Q}[t_i]_{i \in \mathbb{N}}$ with $t_i^n = t_j$ for some i, j, and n, as determined below. Elements of A are simply formal polynomials in the variables $t_0, t_1, \ldots$, and are added and multiplied accordingly. We will give a procedure to determine the sign of any element of A. This will define a computable order on A, as well as say that we can computably tell when two elements of A are equal.

We describe the ordering on A in stages, and will be able to determine the sign of $p \in A$ at stage s if s is at least as large as both the degree of p and the largest i such that t_i appears in p. Here and for the rest of the proof, by the degree of p we mean the maximum sum of exponents in individual summands of p (e.g, the degree of $t_0^2 t_1 + t_2^2$ is 3). Fix an enumeration of the order on L. We will use $l_0, l_1, \ldots$ to speak of the elements of L. At any stage s, we will be able to write down how the elements $l_0, l_1, \ldots l_s$ are ordered (or equal). We will form a list L_s of the form

$$l_{i_0} * l_{i_1} * l_{i_2} * \cdots * l_{i_s}$$

where $*$ is either $\leq_L$ or $\approx_L$, as appropriate. This list will tell us how the infinite elements of A are ordered. As long as we see $l_i \leq_L l_{i+1}$, we will specify that $t_i \leq_A t_{i+1}$, and in fact that $n t_i^s \leq t_{i+1}$ (at stage s, and for all $n \in \mathbb{N}$), so that $t_i^s \ll_a t_{i+1}$. If $l_i \not\approx_L l_{i+1}$, then this will ensure that $t_i \ll_m t_{i+1}$. On the other hand, if we discover at stage s that $l_i \approx_L l_{i+1}$, then we will set $t_i^s = t_{i+1}$. Then $t_i \approx_m t_{i+1}$. (Note: throughout this proof, $\ll_a$, $\ll_m$, $\approx_a$ and $\approx_m$ all refer to the ordering on A.)

At stage $s = 0$, we have $L_s = l_0$, and we say $1 \ll_a t_0$. We clearly can determine the sign of any $p \in A$ which has degree 0. At stage $s = 1$, we run the enumeration of $\leq_L$ until we see either $L_1 = l_0 \leq_L l_1$ or $L_1 = l_1 \leq_L l_0$. In the first case, we say $t_0 \ll_a t_1$, in the latter case we say $1 \ll_a t_1 \ll_a t_0$. We claim that we can determine the sign of any $p \in A$ with degree 1 or less, and with only t_0 and

t_1 appearing in p. We write p as a polynomial in t_{i_1}, where l_{i_1} is the right-most entry in L_1. So

$$p = a_0 + a_1 t_{i_1}$$

where a_0, a_1 are polynomials in t_{i_0} of degree 1 or less. Since $t_{i_0} \ll_a t_{i_1}$, the sign of p will be the sign of a_1. We can write $a_1 = b_0 + b_1 t_{i_0}$ were $b_0, b_1 \in \mathbb{Q}$. The sign of a_1 will then be b_1. Thus we can determine the sign of p.

The procedure for general s will be similar, except that we might need to reduce p if some of the l_{i_j}'s are L-equivalent. At the start of stage s, we have

$$L_{s-1} = l_{i_0} * l_{i_1} * \cdots * l_{i_{s-1}}$$

where each $*$ is either $\leq_L$ or $\approx_L$. To form L_s, we run the enumeration of $\leq_L$ until we see where l_s should fit into L_{s-1}. While running this procedure, we may see $l_{i_j} \leq_L l_{i_k}$ for some $k \leq j \leq s-1$, in which case each $*$ between l_{i_k} and l_{i_j} will become a $\approx_L$ (if it was not already). Once we know where l_s should go, we write

$$L_s = l_{i_0} * l_{i_1} * \cdots * l_{i_j} * l_s *_s l_{i_{j+1}} * \cdots * l_{i_{s-1}}$$

and we insist that $*_s$ is $\leq_L$ and not $\approx_L$, or that l_s is the right most element of the list. (That is, if l_s appears between elements which are L-equivalent, then we list l_s on the far right of the list of elements which are L-equivalent.) Finally, we re-index the elements of the list, adding 1 to the sub-index of all elements $l_{i_{j+1}}$ to $l_{i_{s-1}}$ and setting l_s to $l_{i_{j+1}}$. (This just lets us write $L_s = l_{i_0} * \cdots * l_{i_s}$.)

In defining L_s, we possibly changed some of the $*$ in L_{s-1} from $\leq_L$ to $\approx_L$. Whenever such a change is made, we must act to ensure that the corresponding elements of A are in the same multiplicatively archimedean class. So if, at stage s, we see $l_{i_j} \leq_L l_{i_{j+1}}$ become $l_{i_j} \approx_L l_{i_{j+1}}$, then we set $t^s_{i_j} = t_{i_{j+1}}$. Note that we only do this for consecutive elements of L_s, although even if more than two elements collapse down to become equivalent at a stage, we will have the desired result. For example, if we see $l_{i_{j+3}} \leq_L l_{i_j}$ and we currently have $l_{i_j} \leq_L l_{i_{j+1}} \leq_L l_{i_{j+2}} \leq_L l_{i_{j+3}}$, we will now have $l_{i_j} \approx_L l_{i_{j+1}} \approx_L l_{i_{j+2}} \approx_L l_{i_{j+3}}$, and will set $t^s_{i_j} = t_{i_{j+1}}$, $t^s_{i_{j+1}} = t_{i_{j+2}}$, and $t^s_{i_{j+2}} = t_{i_{j+3}}$. But then $t^{s^3}_{i_j} = t_{i_{j+3}}$, so we still have that t_{i_j} and $t_{i_{j+3}}$ are in the same multiplicatively archimedean class.

For the j such that $l_{i_j} \leq_L l_{i_{j+1}}$ in L_s (elements between which $\leq_L$ did *not* change into $\approx_L$), we specify that $t^s_{i_j} \ll_a t_{i_{j+1}}$. This works towards the possibility that l_{i_j} and $l_{i_{j+1}}$ will never be L-equivalent, ensuring that in that case $t_{i_j} \ll_m t_{i_{j+1}}$. Note that by making $t^s_{i_j} \ll_a t_{i_{j+1}}$, we get that $a \ll_a l_{i_{j+1}}$ for all polynomials a in the variables $t_{i_0}, \ldots, t_{i_j}$ of degree no more than s. For suppose a were such a polynomial. As we have $t_{i_0} \ll_a t_{i_1} \ll_a \cdots \ll_a t_{i_j}$, any summand in a must be less than $nt^s_{i_j}$ for some n (here it is important that the sum of the exponents in any summand is no more than s, which holds because the degree is no more than s). Thus $a < n't^s_{i_j}$ for some n', and as such $a \ll_a t_{i_{j+1}}$.

Now let us argue that at this stage we can determine the sign of any $p \in A$ with degree no more than s and with no t_j with $j > s$ appearing in p. We proceed

by induction on k, where t_{i_k} is the right-most element of L_s to appear in p. For $k = 0$, we have $p = a_0 + a_1 t_{i_0} + \cdots + a_n t_{i_0}^n$ for some $n \leq s$, and each of $a_0, a_1, \ldots a_n$ contain only rationals. Now $p = 0$ if and only if $a_0 = a_1 = \cdots = a_n = 0$, and if not, then the sign of p is simply the sign of a_n. Thus for $k = 0$ we can determine the sign of p. Now suppose that we can determine the sign of any p of degree no more than s which contains only $t_{i_{k-m}}$ for $m \geq 1$. We determine the sign of p in two steps:

Step 1. Inspect L_s to see how l_{i_k} relates to $l_{i_{k-1}}$. If $l_{i_{k-1}} \leq_L l_{i_k}$, then let $q = p$ and skip to step 2. However, if $l_{i_{k-1}} \approx_L l_{i_k}$, then we must reduce p. Find the left-most element l_{i_j} in L_s such that $l_{i_j} \approx_L l_{i_k}$. Find the stage s' at which we first discovered $l_{i_j} \approx_L l_{i_{j+1}}$ and rewrite p so that p does not contain any occurrences of $t_{i_j}^n$ for any $n \geq s'$. That is, if p contains $t_{i_j}^{as'+b}$ for some a and some $b < s'$, substitute in $t_{i_j}^b t_{i_{j+1}}^a$ (which is equal, since we set $t_{i_j}^{s'} = t_{i_{j+1}}$). Then repeat with $t_{i_{j+1}}$ and $t_{i_{j+2}}$, and so on all the way up through $t_{i_{k-1}}$ and t_{i_k}. Call the result of all these substitutions the polynomial q. Note that the degree of q is no more than the degree of p.

Step 2. Write

$$q = a_0 + a_1 t_{i_k} + \cdots + a_n t_{i_k}^n$$

where $a_0, a_1, \ldots, a_n$ are polynomials of degree no more than s which contain only $t_{i_{k-m}}$ for $m \geq 1$. Because we reduced p to q (if we needed to) in step 1, we know that $a_0, \ldots, a_n \ll_a t_{i_k}$. Then $q = 0$ just in case each $a_j = 0$, and otherwise the

sign of q is the sign of a_n, by Lemma 2.3.5. Since a_n does not contain t_{i_k}, there is an algorithm for determining its sign, by the inductive hypothesis. Thus we can find the sign of q, which is the same as the sign of p.

We have built A so that it is a computable ordered ring for which any set of infinite multiplicatively archimedean representatives is isomorphic to L. To get the field F with this same property, we simply pass to the field of fractions. For this to work, we must know that the multiplicatively archimedean classes of F and A coincide. We appeal to Corollary 2.3.11. Given any $p/q \in F$ with $p, q \in A$, we can consider the subring A' of A which only contains the variables in p and q. This is (classically) isomorphic to $\mathbb{Q}[x_0, \ldots, x_n]$ for some n. Then by Corollary 2.3.11, A' will have the same multiplicatively archimedean classes as its field of fractions, which contains p/q. So p/q will be in the same multiplicatively archimedean class as an element of A. This works for any p and q, so F and A have the same multiplicatively archimedean classes, as needed. *QED*

With this result in hand, we can take results known about linear orders and translate them to results about ordered fields. For instance:

Theorem 2.3.13 (Feiner (1970))**.** There is a c.e. linear order L which is not computable.

Applying this to our theorem, we get:

Corollary 2.3.14. There is a computable ordered field for which there is no com-

putable set of multiplicatively archimedean representatives (in any computable copy of the field).

Proof. Take the linear order L from Theorem 2.3.13. Build a field F as in Theorem 2.3.12. Then if there were a presentation of the field F which had a computable set of multiplicatively archimedean representatives, the presentation would have a computable set of *infinite* multiplicatively archimedean representatives. This is because we can check whether a particular representative is greater than the representative for the multiplicatively archimedean class containing the natural numbers greater than 1. The set of infinite multiplicatively archimedean representatives is isomorphic to L. So we would have a computable presentation of L, a contradiction. *QED*

This can be restated as:

Corollary 2.3.15. There is a computable ordered field F such that $\mathrm{Arch}^{\times}(F)$ is not computable for any computable copy of F.

Proof. The same field as in Corollary 2.3.14 works. If $\mathrm{Arch}^{\times}(F)$ were computable, we could define a computable set of infinite multiplicatively archimedean representatives $\{b_0, b_1, \ldots\}$ as follows. Suppose $F = \{a_0, a_1, \ldots\}$. Let b_0 be a_i where i is the least such that $2 < a_i$ and $2 \not\approx_m a_i$ (this guarantees that a_i is infinite). In general, we take b_j to be a_i where i is least such that $2 < a_i$, $2 \not\approx_m a_i$ and a_i is not in the same multiplicatively archimedean class of any of $b_0, b_1, \ldots, b_{j-1}$. *QED*

Chapter 3

The Computable Dimension of Ordered Fields

In the previous chapter, we saw how to construct computable ordered fields with various properties. In doing so, we always gave a very concrete presentation of the field. Now we turn to the question of how different computable copies of the same ordered field can be related. We will see that for a large class of ordered fields, the particular computable copy of the field does not affect the computability-theoretic properties of the field. That is, for these computable ordered fields, we can computably move between computable copies. We will also see that there are computable ordered fields for which this is not the case.

To make these notions precise, we recall some definitions from computable model theory.

Definition 3.0.1. The *computable dimension* of a computable structure $\mathcal{A}$, written $\operatorname{comp\,dim}(A)$, is the number of distinct computable copies (presentations) of the structure, up to computable isomorphism.

Definition 3.0.2. A computable structure $\mathcal{A}$ is *computably categorical* if every

computable structure $\mathcal{B}$ isomorphic to $\mathcal{A}$ is computably isomorphic to $\mathcal{A}$. That is, if $\operatorname{comp\,dim}(\mathcal{A}) = 1$.

Slightly stronger than computably categorical is computably stable:

Definition 3.0.3. A computable structure $\mathcal{A}$ is *computably stable* if for every computable structure $\mathcal{B}$ classically isomorphic to $\mathcal{A}$, every isomorphism $f : \mathcal{A} \to \mathcal{B}$ is in fact a computable isomorphism.

For a wide variety of algebraic structures, the computable dimension is known. For instance, it is known that if $\mathcal{A}$ is an algebraically closed field, or a real closed field, then the computable dimension of $\mathcal{A}$ is either 1 or ω. In fact, the computable dimension is 1 precisely when the field has finite transcendence degree.

3.1 Finite Transcendence Degree

We will show that every computable ordered field with finite transcendence degree is computably stable. We begin by verifying the same result for computable real closed fields.

Lemma 3.1.1. Any computable real closed field with finite transcendence degree is computably stable.

Proof. Let $R = \{a_0, a_1, \ldots\}$ be a computable real closed field with finite transcendence degree. Let $\widehat{R}$ be a computable real closed field isomorphic to R via

the (classical) isomorphism f. Without loss of generality, assume $\{a_0, \ldots, a_{k-1}\}$ is a transcendence basis for R and that a_k is the multiplicative identity. Then $\{f(a_0), \ldots, f(a_{k-1})\}$ is a transcendence basis for $\widehat{R}$ and $f(a_k)$ is the multiplicative identity in $\widehat{R}$. Let $E = \mathbb{Q}(a_0, \ldots, a_{k-1}) \subseteq R$. We will show that f is in fact a computable isomorphism.

Note first that we can computably determine $f(t)$ for any $t \in E$. This is possible since we know the finite information $f(a_0), \ldots, f(a_{k-1})$ and $f(a_k)$. Every other element t of E is some arithmetic combination (sum, difference, product, or quotient) of these finitely many elements. Once we find what combination gives us t, we can form that same combination in $\widehat{R}$, using the fact that f is an isomorphism. Now suppose $p(x)$ is a polynomial in $E[x]$, say

$$p(x) = c_0 + c_1 x + \cdots + c_n x^n.$$

Since $c_0, \ldots, c_n$ are in E, we can effectively find the polynomial

$$\widehat{p}(x) = f(c_0) + f(c_1)x + \cdots + f(c_n)x^n$$

in $f(E)[x]$.

Now to compute $f(t)$ for $t \in R$, we first search and find a polynomial $p(x) \in E[x]$ such that $p(t) = 0$. There must be one since R is algebraic over E. Once found, we determine the number of roots of $p(x)$ which lie in R (which is the same as the number of roots of $\widehat{p}(x)$ which lie in $\widehat{R}$). This can be done either by using Sturm's theorem, or the completeness of the theory of real closed fields.

Once we know the number of roots of $p(x)$, we simply search through R to find all of them. Using the computable order on R, we find m such that there are exactly m roots of $p(x)$ less than t. Next, we search through $\widehat{R}$ to find all the roots of $\widehat{p}(x)$, and specifically find the root $\widehat{t}$ which is greater than exactly m other roots. Since f is an isomorphism, it must be that $f(t) = \widehat{t}$, which we have now found. *QED*

Every ordered field has a unique (up to isomorphism) real closure. If F is a computable ordered field, then there is a computable presentation R_F of its real closure, and a computable embedding from F to R_F. We will use this to prove our result, but we need to know that isomorphisms behave nicely when we pass to real closures. The next lemma is purely algebraic.

Lemma 3.1.2. Let F and $\widehat{F}$ be ordered fields and $f : F \to \widehat{F}$ be an isomorphism. Let R and $\widehat{R}$ be real closures of F and $\widehat{F}$ respectively. Then f extends to a unique isomorphism $g : R \to \widehat{R}$.

Proof. Define g as follows. First, for every $a \in F$, let $g(a) = f(a)$. Now let a be an element of $R \setminus F$. Since R is an algebraic extension of F, there is a polynomial $p(x) \in F[x]$ such that $p(a) = 0$. Say $p(x) = c_0 + c_1x + \cdots + c_nx^n$, and define $\widehat{p}(x) = f(c_0) + f(c_1)x + \cdots + f(c_n)x^n$. Let $a_0 < a_1 < \cdots < a_m$ be the roots of $p(x)$ in R and let $b_0 < b_1 < \cdots < b_m$ be the roots of $\widehat{p}(x)$ in $\widehat{R}$. Define $g(a_i) = b_i$ for $i = 0, \ldots, m$. Note that there really must be the same number of roots of $p(x)$ in R as there are roots of $\widehat{p}(x)$ in $\widehat{R}$. This can be shown using Sturm's Theorem,

which gives the number of roots of a polynomial in a real closure as a function of the number of sign changes in a certain sequence of polynomials. Since f is an isomorphism, the number of sign changes in the sequence for $p(x)$ will be the same as the number of sign changes in the sequence for $\widehat{p}(x)$.

Clearly g is an isomorphism. Moreover, since any isomorphism extending f must send the roots of a polynomial $p(x)$ to roots of $\widehat{p}(x)$, and in the correct order, we see that g is unique. *QED*

We are now ready to prove the main result of this section.

Theorem 3.1.3. Any computable ordered field with finite transcendence degree is computably stable.

Proof. Let F and $\widehat{F}$ be computable ordered fields with finite transcendence degree such that $f : F \to \widehat{F}$ is an isomorphism. Let R and $\widehat{R}$ be computable copies of the real closures of F and $\widehat{F}$ respectively such that the embeddings $\psi : F \hookrightarrow R$ and $\widehat{\psi} : \widehat{F} \hookrightarrow \widehat{R}$ are computable. By Lemma 3.1.2, there is an isomorphism $g : R \to \widehat{R}$ which extends f. By Lemma 3.1.1, we know that g is in fact a computable isomorphism.

Now to compute $f(t)$ for $t \in F$, we simply find $\psi(t)$, and then $g(\psi(t))$. Since g extended f, we know that $g(\psi(t)) = \widehat{\psi}(f(t))$. But now we can just search through $\widehat{F}$ to find an element $\widehat{t}$ such that $\widehat{\psi}(\widehat{t}) = g(\psi(t))$. Thus we can compute $f(t)$ for any $t \in F$, so f is a computable isomorphism. Since f was arbitrary, we see that F is computably stable. *QED*

To summarize, Theorem 3.1.3 goes through because we can non-uniformly match up transcendence bases of the two fields, and after that everything is determined. Each element a is defined by a polynomial $p(x)$ of which it is a root, along with the number of roots of $p(x)$ in the real closure that are smaller than a. The polynomial can be searched for, and the number of smaller roots can be determined algebraically. Thus corresponding roots can be effectively matched up, so we can effectively determine the isomorphism.

Realizing that every element of the field can be defined with a formula using a finite number of parameters (the transcendence basis), leads us to a quicker proof of a stronger result. We will show that any computable ordered field with finite transcendence degree is relatively computably categorical.

Definition 3.1.4. A computable structure $\mathcal{A}$ is *relatively computably categorical* if for every structure $\mathcal{B}$ which is classically isomorphic to $\mathcal{A}$, there is an isomorphism $f : \mathcal{A} \to \mathcal{B}$ which is computable from $\mathcal{B}$.

To prove the result, we will appeal to a theorem of Ash, Knight, Manasse, and Slaman, and independently Chisholm (see [1] or [2]). We need only the simplest case of the theorem.

Theorem 3.1.5 (Ash-Knight-Manasse-Slaman, Chisholm)**.** A structure $\mathcal{A}$ is relatively computably categorical if and only if it has a Σ^0_1 Scott family.

A structure $\mathcal{A}$ has a Σ^0_1 Scott family if there is a finite sequence $\bar{a} \in \mathcal{A}$ and a Σ^0_1 family of existential formulas $\varphi_i(x, \bar{a})$ such that

1. Every $b \in \mathcal{A}$ satisfies $\varphi_i(x, \bar{a})$ for at least one i.

2. If two elements $b, c \in \mathcal{A}$ satisfy the same φ_i, then there is an automorphism of F taking $b \mapsto c$ which fixes $\bar{a}$.

Lemma 3.1.6. Let F be a computable ordered field with finite transcendence degree. Then F has a Σ^0_1 Scott family.

Proof. Let $\bar{a} = \langle a_0, a_1, \ldots, a_{n-1} \rangle$ be a transcendence basis for F. Let $E = \mathbb{Q}(a_0, \ldots a_n) \subseteq F$. We now enumerate a family of formulas $\varphi_{i,j}$ as follows. For each polynomial $p_i \in E[x]$, and each $j \leq \deg(p_i)$, we let $\varphi_{i,j}(x, \bar{a})$ be the formula which says that p_i has k roots and x is the jth-least of these k roots. Here k is the actual number of roots of p_i (which can be found computably, using Sturm's Theorem, for example). Since we are allowed parameters $\bar{a}$ in the formula, such $\varphi_{i,j}$ exist for all i and all $j \leq \deg(p_i)$.

We claim that the family of all such $\varphi_{i,j}$ is a Σ^0_1 Scott family for F. First, note that the collection is clearly Σ^0_1, since we provided an effective enumeration of the formulas (the polynomials p_i can be effectively enumerated). Also, the formulas are all existential. Now for any $b \in F$, b is the root of some polynomial $p(x) \in E[x]$, and that polynomial is p_i for some i. Further, there must be some number j of roots of $p(x)$ less than b, so b satisfies $\varphi_{i,j}$. Thus condition (1) is satisfied. Condition (2) is satisfied trivially, since for every $\varphi_{i,j}$, there is no more than one $b \in F$ which satisfies $\varphi_{i,j}$. Therefore $\{\varphi_{i,j}\}$ is a Σ^0_1 Scott family for F. *QED*

Combining Lemma 3.1.6 with Theorem 3.1.5, we immediately arrive at:

Theorem 3.1.7. Let F be a computable ordered field with finite transcendence degree. Then F is relatively computably categorical.

Before leaving the finite transcendence degree case, it is worth pointing out that these results relied heavily on the fact that our fields are ordered. Indeed, there are computable algebraic fields which are not computably categorical (see [4] for the original proof, or [14]). When the fields in question are ordered, it is possible to distinguish the roots of a given polynomial. An automorphism of a field must send each root of a polynomial to a root of that same polynomial. When the field is not ordered, "different" roots can be exchanged. But with an order on the field, we are able to distinguish roots, and it is no longer possible to send the least root of $p(x)$ to the second least root of $p(x)$.

3.2 Infinite Transcendence Degree

For computable real closed fields, if the field has infinite transcendence degree, then the computable dimension is infinite. We wish to extend this result to the larger class of computable ordered fields with infinite transcendence degree. We will see that in at least the simplest of cases, this is possible.

Theorem 3.2.1. Let F be a computable archimedean field which is a purely transcendental extension of $\mathbb{Q}$ with infinite transcendence degree, for which there

is a computable pure transcendence basis $\mathcal{B}$. Then the computable dimension of F is ω.

Remark 3.2.2. There are fields such as these. See Proposition 2.2.12.

Before giving a proof of the theorem, let us say a little about the general approach. What we will actually demonstrate is that given a suitable computable ordered field F, we can construct a copy $\widehat{F}$ of F in such a way that there is no computable isomorphism between F and $\widehat{F}$. Since F and $\widehat{F}$ need to be classically isomorphic, there must be *some* isomorphism between them. We will construct an isomorphism, but it will be Δ^0_2, and not computable. To ensure that there is no computable isomorphism from F to $\widehat{F}$, we will diagonalize against all partial computable functions. That is, for each partial computable function φ_e, we will wait for $\varphi_e(x)\downarrow = y$ for some particular x, and if y looks like it could be the image of x under a ordered field isomorphism, we will "redefine" y so that φ_e cannot be an isomorphism. Verifying that we can redefine such a y, without losing the computability of $\widehat{F}$ or the fact that $\widehat{F}$ is isomorphic to F, will be the challenging part of the proof.

In our particular case, since we are assuming that F is archimedean, we are helped tremendously by the fact that if $f : F \to \widehat{F}$ is an isomorphism, then f is unique (since F embeds into $\mathbb{R}$, so every $x \in F$ is determined by a Dedekind cut). Thus, since we are building f to be a Δ^0_2 isomorphism, to diagonalize against a partial computable φ_e we need only insist that $\varphi_e(x) \neq f(x)$ for some x. The

x we will use for this diagonalization will be an element of the computable pure transcendence basis. Since any two elements of the pure transcendence basis will be algebraically independent, it will be possible to redefine $f(x)$ in the case that $\varphi_e(x) = f(x)$. Since $F = \mathbb{Q}(\mathcal{B})$ where $\mathcal{B}$ is the computable pure transcendence basis, we will be able to construct $\widehat{F}$ by specifying which elements are in $f(\mathcal{B})$, and then closing under the field operations. This would need to be modified if F were not a purely transcendental extension of the rationals.

Successfully constructing such an $\widehat{F}$ will demonstrate that F cannot be computably categorical - i.e., $\operatorname{comp\,dim}(F) > 1$. However, since F is isomorphic to $\widehat{F}$ via a Δ_2^0 isomorphism, this is enough to demonstrate that $\operatorname{comp\,dim}(F) = \omega$. For this, we appeal to a theorem of Goncharov:

Theorem 3.2.3 (Goncharov [7])**.** If a countable structure $\mathcal{A}$ has two computable copies $\mathcal{A}_1$ and $\mathcal{A}_2$ which are Δ_2^0 isomorphic but not computably isomorphic, then the computable dimension of $\mathcal{A}$ is ω.

The proof of Theorem 3.2.1 rests heavily on our ability to redefine the Δ_2^0 isomorphism as we construct it. This algebraic result will also be useful in Chapter 4, so we will take care of it as a separate lemma. In what follows we will use the following piece of notation: by $p(\bar{b})_c^{b_i}$ we will mean the result of replacing all occurrences of b_i in $p(\bar{b})$ with c.

Lemma 3.2.4. Let A be any finite subset of an archimedean field F and let $B = \{b_0, b_1, \ldots, b_n\} \subseteq A$. Suppose that for each $a \in A$, there is a quotient of

rational polynomials $p_a(\bar{x})$ containing at most the variables $x_0, \ldots, x_n$ such that $a = p_a(\bar{b})$ where $\bar{b} = \langle b_0, b_1, \ldots, b_n \rangle$. Then for each $b_i \in B$, there is a rational c close enough to b_i so that for all $a' \neq a$,

$$p_a(\bar{b}) < p_{a'}(\bar{b}) \text{ if and only if } p_a(\bar{b})^{b_i}_c < p_{a'}(\bar{b})^{b_i}_c.$$

Proof. Let A and B be as in the statement of the lemma. Fix $b_i \in B$. For each $a \in A$, consider the function $f_a(x) = p_a(\bar{b})^{b_i}_x$. This is simply the quotient of two polynomials in a single variable x with coefficients from $\mathbb{Q}(B)$. As such, there is some $E \subseteq F$ containing b_i on which $f_a : E \to F$ is a continuous function. Now for any $a \in A$, let a_1 and a_2 be such that $a_1 < a < a_2$ and a is the only element of A between a_1 and a_2. Consider the interval

$$I_a = \left(\frac{a_1 + a}{2}, \frac{a + a_2}{2} \right) \cap f_a(E).$$

Now I_a is an open set (in the subspace topology on $f_a(E)$), and since f_a is continuous, $f_a^{-1}(I_a)$ is open and contains b_i. Similarly for each of the finitely many $a \in A$. Let

$$I = \bigcap_{a \in A} f_a^{-1}(I_a).$$

This is the intersection of finitely many open sets, so open. Also, I contains b_i, so I must contain an interval about b_i. Take c to be any rational in this interval.

This c so selected satisfies the lemma. To see this, note that by the choice of c, we have $f_a(c) \in I_a$. Since $f_a(c) = p_a(\bar{b})^{b_i}_c$, it follows that

$$p_a(\bar{b}) < p_{a'}(\bar{b}) \text{ if and only if } p_a(\bar{b})^{b_i}_c < p_{a'}(\bar{b})^{b_i}_c$$

for all a and a' in A. *QED*

We are now ready to prove our theorem.

Proof of Theorem 3.2.1. Let $F = \{a_0, a_1, \ldots\}$ with a pure transcendence basis $\{a_{i_0}, a_{i_1}, \ldots\}$. We will build a computable copy $\widehat{F} = \{b_0, b_1, \ldots\}$ of F along with a Δ^0_2 isomorphism $f : \widehat{F} \to F$. The construction will run in stages, so that by the end of stage s we will have defined $\widehat{F}_s \subset \widehat{F}$ and $f_s : \widehat{F}_s \to F$. We will take $\widehat{F} = \bigcup_s \widehat{F}_s$ and $f = \lim_s f_s$. Through the construction, we will satisfy the following requirements for all i, e, and s:

P_i: $\lim_s f_s(b_i)$ exists.

R_i: $\exists j\, (f(b_j) = a_i)$.

Q_s: For all $x, y, z \in \widehat{F}_s$,

$f_s(x) + f_s(y) = f_s(z)$ if and only if $f_{s+1}(x) + f_{s+1}(y) = f_{s+1}(z)$,

$f_s(x) \cdot f_s(y) = f_s(z)$ if and only if $f_{s+1}(x) \cdot f_{s+1}(y) = f_{s+1}(z)$, and

$f_s(x) < f_s(y)$ if and only if $f_{s+1}(x) < f_{s+1}(y)$.

D_e: $\varphi_e \neq f^{-1}$.

Satisfying the P_i and R_i requirements will ensure that f is a well defined bijection (our construction will be such that each f_s is an injection). We will define addition, multiplication, and the order relation on $\widehat{F}$ by $x + y = f^{-1}(f(x) + f(y))$,

$x \cdot y = f^{-1}(f(x) \cdot f(y))$, and $x < y$ if and only if $f(x) < f(y)$. Thus f will in fact by an isomorphism.

Satisfying Q_s for each s will ensure that addition, multiplication, and the order relation will be computable: to decide whether $x < y$, wait until x and y are in $\widehat{F}_s$, then ask whether $f_s(x) < f_s(y)$. This can be answered, since F is a computable ordered field, and we will know

$$x < y \iff f(x) < f(y) \iff f_s(x) < f_s(y).$$

Similarly, to find $x+y$ or $x \cdot y$, we just wait until x and y are in $\widehat{F}_s$. Our construction will put $f_s(x) + f_s(y)$ and $f_s(x) \cdot f_s(y)$ in the range of f_{s+1}, so we will have

$$x + y = z \iff f(x) + f(y) = f(z) \iff f_{s+1}(x) + f_{s+1}(y) = f_{s+1}(z)$$

$$x \cdot y = z \iff f(x) \cdot f(y) = f(z) \iff f_{s+1}(x) \cdot f_{s+1}(y) = f_{s+1}(z).$$

But we can compute $f_{s+1}(x)+f_{s+1}(y)$ and $f_{s+1}(x)\cdot f_{s+1}(y)$ since F is a computable field, and then search through $\widehat{F}_{s+1}$ until we find the element z for which $f_{s+1}(z)$ is the correct sum or product.

Satisfying D_e for each e will ensure that $\widehat{F}$ is not computably isomorphic to F. This works because F and $\widehat{F}$ are archimedean, so any isomorphism between them is unique. But f will be that isomorphism, so making $\varphi_e \neq f^{-1}$ for any e will say that f^{-1} (and as such f) is not computable.

So meeting all requirements will give us the desired result. Now on to the construction. It will be useful to label each element of $\widehat{F}$ with a quotient of rational

polynomials in some finite number of variables $x_0, x_1, \ldots$. We will do this in such a way that if $p_i(\bar{x})$ is the label for b_i, then $f(b_i) = p_i(\bar{a})$ where $\bar{a} = \langle a_{i_1}, a_{i_2}, \ldots, a_{i_n} \rangle$. Since F is a purely transcendental extension of $\mathbb{Q}$, such a labeling is possible. As the construction proceeds, f_s will need to be redefined on some elements, and in doing so, we will change the label of those elements. The labels will tell us how to safely redefine f_s.

Construction: At stage $s = 0$, let $F_0 = \{b_0, b_1, b_2\}$ and define f_0 so that $f_0(b_0) = 0_F$, $f_0(b_1) = 1_F$ and $f_0(b_2) = a_{i_0}$. Give b_0, b_1, and b_2 labels 0, 1 and x_0 respectively. At stage s for $s \geq 1$, first try to meet a requirement D_e:

1. Check if there is some $e < s$ for which $\varphi_{e,s}(a_{i_e}) \downarrow = b_j$ and $f_{s-1}(b_j) = a_{i_e}$. If there is no such e, let $f_s(b_i) = f_{s-1}(b_i)$ for all $b_i \in \widehat{F}_s$ and go to step 5. If there is such an e, pick the least one and continue to step 2:

2. Search for and find a rational c not already in the range of f_{s-1} close enough to a_{i_e} in the sense of Lemma 3.2.4. (More precisely, we take A and B in the lemma to be the range of f_{s-1} and the elements of the pure transcendence basis for F already in the range, respectively. The lemma guarantees that such a c can be found.) Define $f_s(b_j) = c$ and relabel b_j with simply c.

3. For each $b_k \in \widehat{F}_{s-1}$ with label $p_k(\bar{x})$, define $f_s(b_k) = p_k(\bar{a}')$, where

$$\bar{a}' = \langle a_{i_0}, \ldots, a_{i_{e-1}}, c, a_{i_{e+1}}, \ldots, a_{i_n} \rangle.$$

Relabel b_k with $p'_k(\bar{x})$, where p'_k is the result of replacing every occurrence of x_{i_e} in $p_k(\bar{x})$ with c (so $p'_k(\bar{a}) = p_k(\bar{a}')$).

4. For each $b_k \in \widehat{F}_{s-1}$ such that $f_{s-1}(b_k) \neq f_s(b_k)$, take k' least such that $b_{k'}$ is not already in the domain of f_s and define $f_s(b_{k'}) = f_{s-1}(b_k)$. Label $b_{k'}$ with $p_k(\bar{x})$ (the old label of b_k.)

Next, define a little more of f:

5. For each $b_i, b_j \in \widehat{F}_{s-1}$, if any of $f_s(b_i) + f_s(b_j)$, $f_s(b_i) \cdot f_s(b_j)$, $-f_s(b_i)$, or $f_s(b_i)^{-1}$ are not already in the range of f_s, define f_s on b_k to be that element, where k is least such that b_k is not already in the domain of f_s. Label b_k accordingly (i.e., if we defined $f_s(b_k)$ to be $f_s(b_i) + f_s(b_j)$, then label b_k with $p_i(\bar{x}) + p_j(\bar{x})$, and similarly for the other cases).

6. For the least k such that b_k is not already in the domain of f_s, set $f_s(b_k) = a_{i_s}$. Label b_k with x_{i_s}.

7. Let $\widehat{F}_s$ be the domain of f_s.

This completes the construction.

Verification: We verify that each requirement is met. The construction actively worked to satisfy the D_e requirements. For each e such that $\varphi_e(a_{i_e}) \downarrow$, either $\varphi_e(a_{i_e}) \neq f_s^{-1}(a_{i_e})$, in which case D_e is satisfied, or else we immediately act to satisfy D_e by defining f_{s+1} so that $f_{s+1}(f_s^{-1}(a_{i_e})) \neq a_{i_e}$. The only stage s for

which $f_{s+1}^{-1}(a_{i_e}) \neq f_s^{-1}(a_{i_e})$ is one for which we act to meet D_e, so if we ever act to meet D_e, we will succeed and D_e will be satisfied thenceforth.

To see that we satisfy P_i for each i, we consider for which s it happens that $f_s(b_k) \neq f_{s+1}(b_k)$. The only time in the construction when we redefine f is when acting to meet D_e for some e. We define $f_{s+1}(b_k)$ in terms of the label for b_k, but replacing the variable x_{i_e} with a rational c. If the label for b_k does not contain x_{i_e}, then we have $f_{s+1}(b_k) = f_s(b_k)$. If the label does contain x_{i_e}, then we do have $f_{s+1}(b_k) \neq f_s(b_k)$. However, we will only have this situation once for each x_{i_e}, since we only act to meet D_e once. Since the label for b_k contains only finitely many variables, we will have $f_{s+1}(b_k) \neq f_s(b_k)$ for only finitely many s. Thus P_i is satisfied for all i.

Similarly, each requirement R_i is met. By the construction, for every $a_i \in F$, there is some stage s at which a_i is in the range of f_s. This is because we put all rationals into the range, and all elements of the pure transcendence basis into the range, and then close under the field operations. We must check though that $\lim_s f_s^{-1}(a_i)$ exists for each $a_i \in F$. The only time $f_s^{-1}(a_i) \neq f_{s+1}^{-1}(a_i)$ is when we change f in acting to meet D_e for some e. If $f_s^{-1}(a_i)$ changes for the sake of the requirement D_e, then it must have been that the label for $f_s^{-1}(a_i)$ contains x_{i_e}. Since we need only act to meet D_e at most once for each e, and since there are only finitely many e for which x_{i_e} occurs in the label for $f_s^{-1}(a_i)$, we see that there are only finitely many stages s for which $f_s^{-1}(a_i) \neq f_{s+1}^{-1}(a_i)$. Thus R_i is satisfied

for all i.

Finally, we consider requirement Q_s. Fix $x, y, z \in \widehat{F}_s$. Let $p_x(\bar{x})$, $p_y(\bar{x})$, and $p_z(\bar{x})$ be the labels of each at stage s. Now $p_x(\bar{a}) + p_y(\bar{a}) = p_z(\bar{a})$ if and only if $p_x(\bar{a}') + p_y(\bar{a}') = p_z(\bar{a}')$ (since we are simply substituting a rational in for the variable x_{i_e} in each term). But by the construction and how we defined our labeling, we have that $f_s(x) = p_x(\bar{a})$, $f_s(y) = p_y(\bar{a})$, and $f_s(z) = p_y(\bar{a})$. Also, since for any k, $p_k(\bar{a}') = p'_k(\bar{a})$, we have that $f_{s+1}(x) = p_x(\bar{a}')$, $f_{s+1}(y) = p_y(\bar{a}')$, and $f_{s+1}(z) = p_z(\bar{a}')$. Thus

$$f_s(x) + f_s(y) = f_s(z) \iff p_x(\bar{a}) + p_y(\bar{a}) = p_z(\bar{a}) \iff$$

$$\iff p_x(\bar{a}') + p_y(\bar{a}') = p_z(\bar{a}') \iff f_{s+1}(x) + f_{s+1}(y) = f_{s+1}(z).$$

Similarly

$$f_s(x) \cdot f_s(y) = f_s(z) \iff f_{s+1}(x) \cdot f_{s+1}(y) = f_{s+1}(z).$$

That $f_s(x) < f_s(y)$ if and only if $f_{s+1}(x) < f_{s+1}(y)$ follows from Lemma 3.2.4. We picked c close enough to a_{i_e} precisely so that this would hold. This completes the verification, and the proof. *QED*

3.3 The Archimedean Case

We have seen that computable ordered fields with finite transcendence degree have computable dimension 1, while at least some computable ordered fields with infinite transcendence degree have computable dimension ω. But are these the

only possibilities? That is, are there any computable ordered fields with finite computable dimension greater than 1? We will see that this is not possible, at least when considering archimedean fields.

Theorem 3.3.1. Let F be a computable archimedean field. Then F is Δ^0_2 categorical.

Proof. Let $f : F \to \widehat{F}$ be the unique isomorphism from F to $\widehat{F}$. Since F is archimedean, every element of F is uniquely determined by the set of rationals below it. Since f is an isomorphism, for any $x \in F$ and rational a, we have $f(a) < f(x)$ if and only if $a < x$. However, for every rational a, we can computably determine $f(a)$. Thus given $x \in F$ and $y \in \widehat{F}$, we can computably determine the truth of $a < x \leftrightarrow f(a) < y$, for any rational a. We have

$$f(x) = y \iff \forall a(a \in \mathbb{Q} \to (a < x \leftrightarrow f(a) < y))$$
$$\iff \forall a(a \notin \mathbb{Q} \vee (a < x \leftrightarrow f(a) < y)).$$

Since $a \notin \mathbb{Q}$ is Π^0_1, we see that $f(x) = y$ is Π^0_1, so certainly Δ^0_2.

QED

Corollary 3.3.2. If F is a computable archimedean field, then the computable dimension of F is either 1 or ω.

Proof. Let F be a computable archimedean field, and let $\widehat{F}$ be a computable field which is classically isomorphic to F. By Theorem 3.3.1, the unique isomorphism

from F to $\widehat{F}$ is Δ^0_2. If the isomorphism is computable, then the computable dimension of F is 1 (since $\widehat{F}$ was arbitrary). If the isomorphism is not computable, then there are two copies of F (namely F and $\widehat{F}$) which are Δ^0_2 isomorphic but not computably isomorphic. Thus by Goncharov's Theorem (3.2.3), the computable dimension of F is ω. *QED*

Chapter 4

The Transcendence Bases of Computable Ordered Fields

In this chapter we will consider how complicated transcendence bases can be in computable ordered fields.

4.1 Non-Computable Transcendence Bases

We will produce a presentation of a computable ordered field which has no computable transcendence basis. In fact, we will be able to do more. It is possible to construct a computable archimedean field such that every transcendence basis computes the halting problem.

Theorem 4.1.1. There is a computable archimedean field for which every transcendence basis computes K.

The proof is similar to that of 3.2.1, although there are enough differences that we will give the full proof.

Proof. Let F be a computable archimedean field, purely transcendental over $\mathbb{Q}$, with a computable pure transcendence basis (for instance, as in Proposition

2.2.12). For ease of notation, let $F = \{a_0, a_1, \ldots\}$ and let $\{a_{i_0}, a_{i_1}, \ldots\}$ be a computable pure transcendence basis of F. We will build a computable ordered field $\widehat{F}$ and a Δ^0_2 isomorphism $f : \widehat{F} \to F$. We will use $\{b_0, b_1, \ldots\}$ for the elements of $\widehat{F}$. We approximate $\widehat{F}$ with finite $\widehat{F}_s$ at stage s, and approximate f with $f_s : \widehat{F}_s \to F$, so that $\widehat{F} = \bigcup_s \widehat{F}_s$ and $f = \lim_s f_s$. For the construction, we also fix a computable enumeration K_s of K so that $K_{s+1} \setminus K_s$ contains at most one element.

As in the proof of Theorem 3.2.1, we will satisfy requirements:

P_i: $\lim_s f_s(b_i)$ exists.

R_i: $\exists j (f(b_j) = a_i)$.

Q_s: For all $x, y, z \in \widehat{F}_s$,

$f_s(x) + f_s(y) = f_s(z)$ if and only if $f_{s+1}(x) + f_{s+1}(y) = f_{s+1}(z)$,

$f_s(x) \cdot f_s(y) = f_s(z)$ if and only if $f_{s+1}(x) \cdot f_{s+1}(y) = f_{s+1}(z)$, and

$f_s(x) < f_s(y)$ if and only if $f_{s+1}(x) < f_{s+1}(y)$.

Doing so will ensure that $\widehat{F}$ is isomorphic to F and that $\widehat{F}$ is computable. Instead of the requirement that $f^{-1} \neq \varphi_e$ for any e, we will have the requirement:

D_n: If $\{b_{i_0}, \ldots, b_{i_{n-1}}\}$ is algebraically independent, then $K \upharpoonright n = K_m \upharpoonright n$ where $m = \max\{i_0, \ldots, i_{n-1}\}$.

If we meet D_n for each n, then any transcendence basis $\{b_{i_0}, b_{i_1}, \ldots\}$ of $\widehat{F}$ will compute K, as follows. To determine whether $x \in K$, consider any x elements of the

transcendence basis, say $\{b_{i_0}, \ldots, b_{i_{x-1}}\}$. Then calculate $m = \max\{i_0, \ldots, i_{x-1}\}$ and enumerate K for m stages. Since $\{b_{i_0}, \ldots, b_{i_{x-1}}\}$ is algebraically independent, and D_x was satisfied, we have $K\restriction x = K_m\restriction x$. But K_m is computable, so we can ask whether $x \in K_m$. Whatever the answer, that will be the answer as to whether $x \in K$.

As before, at each stage s of the construction we will label each $b_i \in \widehat{F}_s$ with $p_i(\bar{x})$, a quotient of rational polynomials in variables $\{x_0, x_1, \ldots, x_s\}$. Our labeling will satisfy $f_s(b_i) = p_i(\bar{a})$ where $\bar{a} = \langle a_{i_0}, \ldots, a_{i_s}\rangle$. Such a labeling is possible since F is a purely transcendental extension of $\mathbb{Q}$.

Construction: We initially set $\widehat{F}_0 = \{b_0, b_1, b_2\}$, $f_0(b_0) = 0_F$, $f_0(b_1) = 1_F$, and $f_0(b_2) = a_{i_0}$. We give b_0, b_1, and b_2 the labels 0, 1, and x_0 respectively. At any stage s of the construction, we define take the following steps:

1. Compute K_{s+1}. If $K_{s+1} \setminus K_s = \emptyset$ or if $K_{s+1} \setminus K_s = \{n\}$ for $n > s$, let $f_{s+1}(b_i) = f_s(b_i)$ for all $b_i \in F_s$, and do not change the labels of any of those b_i. Then skip to step 3. Otherwise, proceed to step 2.

2. We have $K_{s+1} \setminus K_s = \{n\}$ with $n \leq s$. We will redefine $f_{s+1}(b_j)$ to be rational for those b_j such that $f_s(b_j)$ is among $a_{i_n}, a_{i_{n+1}}, \ldots a_{i_s}$. Set $m = n$, and $f_{s_m} = f_s$. Then as long as $m \leq s$, do the following:

   (a) Let b_j be such that $f_s(b_j) = a_{i_m}$. Search for a rational c_m not already in the range of f_{s_m} close enough to a_{i_m} in the sense of Lemma 3.2.4.

(More precisely, we take A and B in the lemma to be the range of f_{s_m} and the the elements of the pure transcendence basis for F already in the range, respectively. The lemma guarantees that such a c_m can be found.) Set $f_{s_{m+1}}(b_j) = c_m$. Relabel b_j with c_m.

(b) For each $b_k \in \mathrm{dom}(f_{s_m})$ with a label $p_k(\bar{x})$, define $f_{s_{m+1}}(b_k) = p_k(\bar{a}')$, where $\bar{a}'$ is the result of replacing each a_{i_m} in $\bar{a}$ with the rational c_m found above. Relabel b_k with $p'_k(\bar{x})$, where p'_k is the results of replacing every occurrence of x_{i_m} in $p_k(\bar{x})$ with c_m (so $p'_k(\bar{a}) = p_k(\bar{a}')$).

(c) For each $b_k \in \mathrm{dom}(f_{s_m})$ such that $f_{s_m}(b_k) \neq f_{s_{m+1}}(b_k)$, take k' least such that $b_{k'}$ is not already in the domain of $f_{s_{m+1}}$ and define $f_{s_{m+1}}(b_{k'}) = f_{s_m}(b_k)$. Label $b_{k'}$ with $p_k(\bar{x})$ (the old label of b_k.)

(d) If $m < s$, increment m and go back to step 2a. If $m = s$, then set $f_{s+1} = f_{s_m}$ and continue to step 3.

Continue as in Theorem 3.2.1:

3. For each $b_i, b_j \in \widehat{F}_s$, if any of $f_{s+1}(b_i) + f_{s+1}(b_j)$, $f_{s+1}(b_i) \cdot f_{s+1}(b_j)$, $-f_{s+1}(b_i)$, or $f_{s+1}(b_i)^{-1}$ are not already in the range of f_{s+1}, define f_{s+1} on b_k to be that element, where k is least such that b_k is not already in the domain of f_{s+1}. Label b_k accordingly (i.e., if we defined $f_{s+1}(b_k)$ to be $f_{s+1}(b_i) + f_{s+1}(b_j)$, then label b_k with $p_i(\bar{x}) + p_j(\bar{x})$, and similarly for the other cases).

4. For the least k such that b_k is not already in the domain of f_{s+1}, define

$f_{s+1}(b_k) = a_{i_{s+1}}$. Label b_k with $x_{i_{s+1}}$.

5. Let $\widehat{F}_{s+1}$ be the domain of f_{s+1}.

This completes the construction.

Verification: We verify that each requirement is met. Each Q requirement is satisfied by the construction, exactly as in the proof of Theorem 3.2.1. To see that we satisfy P_i for each i, consider an s for which $f_{s+1}(b_i) \neq f_s(b_i)$. Then we must have reached step 2 in the construction, so some $n < s$ just entered K. Further, the label for b_i must contain an occurrence of x_{i_m} for some $n \leq m \leq s$, since if it did not, then $\bar{a}' = \bar{a}$ so

$$f_{s+1} = p_i(\bar{a}') = p_i(\bar{a}) = f_s(b_i).$$

After relabeling, the label for b_i will have one or more fewer variables. Thus $f_{s+1} \neq f_s(b_i)$ can happen only finitely many times (at most once for each variable in the original label of b_i). So P_i is satisfied.

To see that each requirement R_i is met, note that since 1_F and every element of the transcendence basis is eventually put into the range of f_s and we close the range under the field operations, each a_i is in the range of f_s for some s. We must argue that $\lim_s f_s^{-1}(a_i)$ exists for each i. The label for $f_s^{-1}(a_i)$ mentions only finitely many x_{i_n}, so let n be largest so that x_{i_n} is in the label for $f_s^{-1}(a_i)$. Let s' be a stage such that $K_{s'} \restriction n = K \restriction n$. Since after stage s', we only change f_s on elements with labels containing x_{i_m} for $m > n$, we will have $f_{s'}^{-1}(a_i) = \lim_s f_s^{-1}(a_i)$. So R_i

is satisfied.

Finally, let us argue that D_n is satisfied for each n. Suppose for some m, $K\restriction n \neq K_m\restriction n$. Then for some $s > m$, there is an $n' \leq n$ such that $K_{s+1}\setminus K_s = \{n'\}$. Then at stage s of our construction, we relabel all $b_i \in F_s$ so that no label contains variables x_j with $j \geq n'$ (each such variable is replaced with a rational). When we move on to the part of the construction where we pick new elements for F_{s+1} and give them labels containing x_j for $j \geq n'$, we use elements b_k for k not yet used. But the construction is such that the smallest available k is much larger than s. So after stage s of the construction, the only variables occurring in any b_k for $k < s$ are x_j for $j < n'$. So any set of n elements b_k with $k < m < s$ must mention fewer than $n < n'$ variables. Thus such a set of n elements is algebraically dependent (each element is in the algebraic span of a set of fewer than n elements). Therefore D_n is satisfied. This completes the verification, and the proof. *QED*

One may wonder if it is possible to get any stronger result along this line. For instance, is there a computable ordered field such that every transcendence basis is Π^0_2 complete? The answer is no. It is relatively easy to see that every computable ordered field contains a transcendence basis which is Π^0_1:

Proposition 4.1.2. Every computable (ordered) field contains a Π^0_1 transcendence basis.

Proof. Let F be a computable field (or ordered field). Without loss of generality, assume that F has infinite transcendence degree. We will approximate the

transcendence basis in stages, having at stage s a set A_s which contains a transcendence basis for F. We will do so in such a way that $\lim_s A_s = \bigcap_s A_s = A$ is a transcendence basis for F. Also, we will ensure that the complement of A is c.e., so the transcendence basis will be co-c.e., that is, Π^0_1.

Fix an enumeration $\{p_0, p_1, \ldots\}$ of all non-zero polynomials in $\mathbb{Q}[x_0, x_1, \ldots, x_n]$ (for all values of n), as well as an enumeration $\{\bar{a}_0, \bar{a}_1, \ldots\}$ of all tuples (of all sizes) of elements from F. Let $A_0 = F$. To form A_s, check whether $p_i(\bar{a}_j) = 0$ for each $i \leq s$ and $j \leq s$ for which $\bar{a}_j \in A^n_{s-1}$ (for $n = |\bar{a}_j|$). If there is a first $\bar{a}_j = (a_{j_0}, \ldots a_{j_{n-1}})$ for which this is satisfied, let $A_s = A_{s-1} \setminus \{a_{j_{n-1}}\}$. If there is no tuple which makes a polynomial 0, then let $A_s = A_{s-1}$. Now $A = \lim_s A_s$ is clearly a transcendence base for F, and its complement is c.e., as required. *QED*

4.2 Immune Transcendence Bases

Above we built a computable archimedean field for which every transcendence basis computed the halting problem. As such, no transcendence basis of that field is computable. Moreover, since the field contains a co-c.e. transcendence basis, there must be a transcendence basis which is not c.e. We now consider whether it is possible to build a computable archimedean field such that *no* transcendence basis is c.e. In fact, we will show something stronger: that there is a computable archimedean field such that no transcendence basis even contains an infinite c.e. set.

Theorem 4.2.1. There is a computable archimedean field such that every transcendence basis is immune. That is, no transcendence basis contains an infinite c.e. set.

Proof. As in the proof of Theorem 4.1.1, we start with a computable archimedean field F which is a purely transcendental extension of $\mathbb{Q}$ with a computable pure transcendence basis. We then build a copy $\widehat{F}$ such that if W_e is infinite, then the first $e+1$ elements of W_e are algebraically dependent in $\widehat{F}$. Thus W_e can not be contained in any transcendence basis of $\widehat{F}$.

We use the same setup and notation as in the proof of Theorem 4.1.1. Requirements P_i, R_i and Q_s are identical. We replace the requirement D_n with

D_e: If W_e is infinite, then W_e is algebraically dependent.

Clearly satisfying all requirements results in a field with no c.e. transcendence basis.

Construction: We proceed as in the construction in the proof of Theorem 4.1.1, except for the first two steps on the construction at stage s. Instead, we do the following:

1. Check whether there is some $e < s$ for which D_e has not been satisfied, and for which $|W_{e,s}| \geq e+1$. If there is no such e, then set $f_{s+1} = f_s$ and skip to step 3. Otherwise, suppose the first $e+1$ elements of such a W_e are $b_{i_0}, \ldots, b_{i_e}$, with labels $p_{i_0}, \ldots, p_{i_e}$.

2. Let $\{x_{j_0}, \ldots, x_{j_n}\}$ be the set of variables appearing in $p_{i_0}, \ldots, p_{i_e}$. If $n < e$, then D_e is satisfied so set $f_{s+1} = f_s$ and skip to step 3. Otherwise, we have $e < n$. Set $m = e$ and $f_{s_m} = f_s$. As long as $m \leq n$ do the following:

(a) - (c) Same as in the construction in the proof of Theorem 4.1.1.

(d) If $m < n$, increment m and go back to step 2a. If $m = n$, then set $f_{s+1} = f_{s_m}$ and continue to step 3.

3 - 5. Identical to those of Theorem 4.1.1

This completes the construction.

Verification: We check that each requirement is satisfied by the construction. For each e, if W_e is infinite, then there will be a stage s for which $D_{e'}$ is satisfied for all $e' < e$, and for which $W_{e,s}$ contains $e + 1$ many elements. If needed, the construction redefines f_s so that the $e+1$ elements of W_e all have labels with e or fewer distinct variables. Thus the $e+1$ elements of W_e are all in the algebraic span of e or fewer elements of $\widehat{F}$. Therefore, the elements of W_e cannot be algebraically independent, so D_e is satisfied. To see that P_i is satisfied for each i, note that the only $b_k \in \widehat{F}_s$ for which $f_s(b_k) \neq f_{s+1}(b_k)$ are ones whose labels include variables x_i with $i \geq e$ when we attempt to satisfy D_e. Similarly for requirements R_i, we have $f_s^{-1}(a_i) \neq f_{s+1}^{-1}(a_i)$ only when we try to satisfy D_e and the label for a_i contains x_j for $j < e$. So once D_e is satisfied, $f_s(b_k) = f_{s+1}(b_k)$ and $f_s^{-1}(a_i) = f_{s+1}^{-1}(a_i)$ for every b_k and a_i with labels containing only x_j and for $j < e$. Thus P_i and R_i

are met for each i. Requirements Q_s are satisfied as before. This completes the verification, and the proof.

QED

Chapter 5

The Reverse Mathematics of Ordered Fields and Rings

In this chapter we will approach our subject from a slightly different viewpoint - that of reverse mathematics. We begin by giving some background, although the reader entirely unfamiliar with the subject is urged to see [18]. Afterwards, we will give generalizations of some known results.

5.1 Background

Reverse mathematics seeks to classify theorems of ordinary countable mathematics by the strength of the set existence axioms required to prove them. We work in the formal language of second order arithmetic, Z_2, which contains non-logical symbols

$$+,\ \cdot,\ <,\ 0,\ 1,\ \in$$

along with both number and set variables. The axioms of Z_2 posit that these symbols behave in the usual way on the natural numbers and sets of natural numbers, with $\in$ as set membership. In addition to the basic axioms, there is a

full induction scheme

$$(\varphi(0) \wedge \forall n(\varphi(n) \to \varphi(n+1))) \to \forall n\, \varphi(n)$$

for any formula φ, and full comprehension scheme

$$\exists X \forall n(n \in X \leftrightarrow \varphi(n))$$

where φ is any formula not containing X.

In analyzing a theorem of ordinary mathematics from the viewpoint of reverse mathematics, we wish to determine the weakest subsystem of Z_2 in which it is still possible to prove the theorem. We then say that the theorem lies in that subsystem. Perhaps surprisingly, the large majority of theorems lie in a mere five subsystems: RCA_0, WKL_0, ACA_0, ATR_0, and Π^1_1-CA_0. In what follows we will only be concerned with the first three.

RCA_0 is the weakest of these systems, and is used as a "base system," in which to prove the equivalence of theorems and higher subsystems. It consists of the basic axioms of Z_2 along with Σ^0_1 induction and Δ^0_1 comprehension. That is, in the induction and comprehension schemes above, we require that φ is Σ^0_1 and Δ^0_1 respectively. With these restrictions, many theorems of ordinary mathematics can no longer be proved. For example, RCA_0 does not prove:

Lemma 5.1.1 (Weak König's Lemma)**.** Every infinite tree $T \subseteq 2^{<\mathbb{N}}$ contains an infinite path.

Adding weak König's Lemma to RCA_0 as an axiom gives WKL_0, which is strictly stronger than RCA_0. Strictly stronger still is ACA_0, which allows induction and comprehension of any arithmetic formulas (containing any number of number quantifiers, but no set quantifiers).

When dealing with a particular algebraic structure, care must be taken in giving the correct definitions. These definitions are given from within RCA_0, and as such it is important not to assume the existence of sets which might require WKL_0 or ACA_0 to exist. This however is not an issue when giving the definition of a field:

Definitions 5.1.2 (RCA_0)**.** A *field* F is a set $|F| \subseteq \mathbb{N}$ along with binary operations $+_F$ and $\cdot_F$, a unary operation $-_F$, and distinguished elements 0_F and 1_F, all of which obey the usual field axioms. An *ordered field* is a field F together with a binary relation $\leq_F \subseteq |F|^2$ which obey the usual ordered field axioms.

Definition 5.1.3 (RCA_0)**.** A *formally real field* is a field F such that -1 is not a sum of squares in F.

Note that classically, one could define a formally real field as a field which can be ordered, and prove as a theorem that such fields do not have -1 as a sum of squares. This is not the right way to go here though, since weak König's Lemma is required to prove the existence of an ordering in a field for which -1 is not a sum of squares. This and a variety of other results concerning the reverse mathematics of fields were proved by Friedman, Simpson, and Smith in [5]. Highlights include:

Theorem 5.1.4. RCA_0 is sufficeint to prove that every field has an algebraic closure and every ordered field has a unique real closure.

Theorem 5.1.5. The following are equivalent over RCA_0.

1. WKL_0.

2. Every countable, formally real field is orderable.

Theorem 5.1.6. The following are equivalent over RCA_0.

1. ACA_0

2. Every field has a transcendence basis.

In the following sections, we will attempt to extend these kind of results.

5.2 Extending Partial Orders to Full Orders

Let R be a commutative ring. We say that $(R, \leq)$ is a partially ordered ring (p. o. ring) if R is a partially ordered set under $\leq$ and for any $a, b, c \in R$

1. if $a \leq b$, then $a + c \leq b + c$,

2. if $a \leq b$ and $c > 0$, then $ac \leq bc$.

Instead of specifying $\leq$, we will instead consider the set P of all positive elements under $\leq$. We call such a P the *positive cone* of the partial order.

Definitions 5.2.1 (RCA_0)**.** $P \subseteq R$ is a *positive cone for a partial order* on R provided

- $P \cap -P = \{0\}$
- $P + P \subset P$
- $P \cdot P \subset P$.

If P also satisfies

- $P \cup -P = R$

then P is a *positive cone for a full order* on R.

From a positive cone P for a partial (or full) order on R we can define a partial (or full) order on R by $a \leq b$ if and only if $b - a \in P$. From this point forward, we will blur the distinction, and simply refer to a positive cone for a partial (or full) order as a partial order (or full order).

We are interested in conditions which guarantee that a partial order on a ring or field can be extended to a full order. We find such conditions in [6]. First some definitions and notation.

Notation 5.2.2. If R is a ring containing elements $a_0, a_1, \ldots, a_n$, and A is a subset of R, then by $H(A, a_0, \ldots, a_n)$ we mean the semiring generated by $0, A, a_0, \ldots, a_n$ in R. (That is, the result of closing $\{0, A, a_0, \ldots a_n\}$ under addition and multiplication, but not necessarily under additive or multiplicative inverses.)

Definition 5.2.3. A semiring is *conic* provided zero is not the sum of nonzero elements from the semiring.

Now consider the following theorem:

Theorem 5.2.4. A partial order P of a ring R can be extended to a full order of R if and only if P satisfies:

(*) for every finite set $\{a_0, \ldots, a_n\} \subset R$ there are $\varepsilon_0, \ldots, \varepsilon_n \in \{-1, 1\}$ such that

$$H(P, \varepsilon_0 a_0, \ldots, \varepsilon_n a_n)$$

is conic.

The proof given in [6] uses Zorn's Lemma to take the maximal partial order Q extending P which satisfies (*) and shows that Q is in fact a full order on R. We are concerned with whether there is a "simpler" proof. As we will see, the theorem can be proved in WKL_0. But also, over RCA_0, we can prove weak König's Lemma from the theorem. We begin by proving

Lemma 5.2.5. WKL_0 implies Theorem 5.2.4.

Remark 5.2.6. The statement of Lemma 5.2.5 and its proof below are not quite right. The problem is that the set $H(P, \varepsilon_0 a_0, \ldots, \varepsilon_n a_n)$ need not exist in WKL_0 (in general, you need ACA_0 to prove the existence of such semirings). To be completely accurate, we would need to restate Theorem 5.2.4 in the language of second order arithmetic. We would define a function $s(A, n, x)$ by recursion, where

A is (a code for) a finite sequence of elements (the $\varepsilon_i a_i$), so that $s(A, n, x) = 1$ if x is in the set generated by P and A using only n-steps of addition and multiplication, and $s(A, n, x) = 0$ if x is not in that set. The semiring $H(P, A)$ then is then the set of all x for which there is some n so that $S(A, n, x) = 1$. For simplicity, we have omitted this level of detail in the proof below, and in the results that follow. For an example of how this detailed proof would be carried out (in the context of orderable groups) see [20].

Proof of Lemma 5.2.5. We simply give a proof of Theorem 5.2.4 in WKL_0. Let P be a partial order on the ring R. First suppose that P can be extendend to a full order P_1. Then for every finite set $\{a_0, \ldots, a_n\} \subset R$, either $a_i \in P_1$ or $-a_i \in P_1$, for each $i = 0, \ldots, n$. Thus we can choose $\varepsilon_0, \ldots, \varepsilon_n \in \{-1, 1\}$ accordingly, so that $\varepsilon_i a_i \in P_1$ for each $i = 0, \ldots, n$. Then, since $P \subseteq P_1$, we have

$$H(P, \varepsilon_0 a_0, \ldots, \varepsilon_n a_n) \subset H(P_1, \varepsilon_0 a_0, \ldots, \varepsilon_n a_n) = H(P_1).$$

But $H(P_1)$ is just P_1, since any full (or partial) order is already a semiring. Also, since P_1 is a full order, it is conic. Since 0 is not the sum of nonzero elements of P_1, it follows that 0 is not the sum of nonzero elements in $H(P, \varepsilon_0 a_0, \ldots, \varepsilon_n a_n)$, which is to say that $H(P, \varepsilon_0 a_0, \ldots, \varepsilon_n a_n)$ is conic. (Note that this direction of the proof needed only RCA_0.)

Conversely, suppose (*). We will build a infinite tree $T \subseteq 2^{<\mathbb{N}}$ such that every infinite path through T codes a full order on R extending P. By weak König's Lemma, T will have an infinite path, so there will be a full order on R

extending P. Let $R = \{0, a_0, a_1, \ldots\}$ and $P = \{0, p_0, p_1, \ldots\}$. The intuition for building T is that if $\sigma \in T$ then we should have $\sigma(n) = 1$ if and only if a_n is positive.

Construction of T: For each s, we let T_s be the tree of all strings of T with length no more than s. So T_0 consists only of the empty string. Now suppose T_s is defined, and we wish to define $T_{s+1} \supset T_s$. For each $\sigma \in T_s$ with $|\sigma| = s$ we put $\sigma^\frown 0$ and $\sigma^\frown 1$ into T_{s+1} *unless* there are $i, j, k < s$ such that any of the following hold:

(i) $a_i + a_j = a_k$ and $\sigma(i) = \sigma(j) = 1$ but $\sigma(k) = 0$,

(ii) $a_i \cdot a_j = a_k$ and $\sigma(i) = \sigma(j) = 1$ but $\sigma(k) = 0$,

(iii) $a_i = -a_j$ but $\sigma(i) = \sigma(j)$, or

(iv) $a_i = p_j$ but $\sigma(i) = 0$.

Claim: T is infinite. To verify this, suppose T were finite. Then there was a least stage s for which $T_s = T_{s+1}$. Thus for each $\sigma \in T_s$ with $|\sigma| = s$, one of (i) - (iv) holds. In fact, this can be said of every $\sigma \in 2^{<\mathbb{N}}$ of length s. To simplify notation, define for each $\sigma \in 2^{<\mathbb{N}}$ of length s,

$$\sigma_i = \begin{cases} 1 & \text{if } \sigma(i) = 1, \\ -1 & \text{if } \sigma(i) = 0. \end{cases}$$

So then for some $i, j, k < s$, either $\sigma_i a_i + \sigma_j a_j + \sigma_k a_k = 0$ or $\sigma_i a_i \cdot \sigma_j a_j + \sigma_k a_k = 0$ or $\sigma_i a_i + \sigma_j a_j = 0$ or $\sigma_i a_i + p_j = 0$. Let

$$g_\sigma = \prod_{i,j,k<s} (\sigma_i a_i + \sigma_j a_j + \sigma_k a_k)(\sigma_i a_i \cdot \sigma_j a_j + \sigma_k a_k)(\sigma_i a_i + \sigma_j a_j)(\sigma_i a_i + p_j).$$

Then $g_\sigma = 0$ for all $\sigma \in 2^{<\mathbb{N}}$ of length s.

Now when multiplied out, g_σ is the sum of terms of the form $\prod_{i,j<s} p_j^{n_j} (\sigma_i a_i)^{m_i}$. These are non-zero elements of the semiring $H(P, \sigma_0 a_0, \ldots, \sigma_{s-1} a_{s-1})$ so it is *not* conic. But this is true for every $\sigma \in 2^{<\mathbb{N}}$ of length s, so for every choice of $\sigma_0, \ldots, \sigma_{s-1} \in \{-1, 1\}$, contradicting (*). Thus T is infinite.

To conclude, we note that weak Köneg's Lemma guarantees that T contains an infinite path, call it τ. The set

$$P_1 = \{a_i \mid \tau(i) = 1\} \cup \{-a_i \mid \tau(i) = 0\}$$

is clearly a full order on F_1, by the construction of T. Further, $P \subseteq P_1$, as required. This completes the proof.

QED

With this lemma in hand, we proceed to prove the equivalence of Theorem 5.2.4 and WKL_0. While at it, we will also include the following corollary.

Corollary 5.2.7. A ring R can be fully ordered if and only if for every finite set $a_0, \ldots, a_n \in R$ there are $\varepsilon_0, \ldots, \varepsilon_n \in \{-1, 1\}$ such that $H(\varepsilon_0 a_0, \ldots, \varepsilon_n a_n)$ is conic.

Theorem 5.2.8. The following are equivalent over RCA_0:

1. WKL_0.

2. Corollary 5.2.7

3. Theorem 5.2.4.

Proof. Lemma 5.2.5 gives us (1) $\Longrightarrow$ (3). If we let $P = \{0\}$, we immediately see that (3) $\Longrightarrow$ (2). Thus we need only (2) $\Longrightarrow$ (1). Our proof will rely on a theorem of Solomon [20]. He proved (in RCA_0) that WKL_0 is equivalent to the theorem that a group G is orderable if and only if for every finite set $\{a_0, \ldots, a_n\} \subseteq G$ there are $\varepsilon_0, \ldots, \varepsilon_n \in \{-1, 1\}$ such that

$$0_G \notin S(\varepsilon_0 a_0, \ldots, \varepsilon_n a_n),$$

where $S(\varepsilon_0 a_0, \ldots, \varepsilon_n a_n)$ is the semigroup generated by $\varepsilon_0 a_0, \ldots, \varepsilon_n a_n$.

Suppose (2). Let G be a group and consider the ring R_G of elements from G with multiplication defined by $g \cdot h = 0$ for all $g, h \in G$. Note that R_G is a commutative ring, without identity. Suppose that for every finite set $\{a_0, \ldots, a_n\} \subseteq G$ there are $\varepsilon_0, \ldots, \varepsilon_n \in \{-1, 1\}$ such that $0_G \notin S(\varepsilon_0 a_0, \ldots, \varepsilon_n a_n)$. In R_G, consider $H(\varepsilon_0 a_0, \ldots, \varepsilon_n a_n)$. This is the semiring generated by $\varepsilon_0 a_0, \ldots, \varepsilon_n a_n$, but since the product of any two elements is always 0, we need only close under addition. So really, $H(\varepsilon_0 a_0, \ldots, \varepsilon_n a_n)$ is no more than the semigroup generated by $\varepsilon_0 a_0, \ldots, \varepsilon_n a_n$. Since $0 \notin S(\varepsilon_0 a_0, \ldots, \varepsilon_n a_n)$, we have that $H(\varepsilon_0 a_0, \ldots, \varepsilon_n a_n)$ is conic. By (2), this

implies that there is a full order on R_G. But a full order on R_G is also a full order on G, so G is orderable. Thus weak König's Lemma holds. *QED*

If R is in fact a field, there is a simpler condition guaranteeing that a partial order can be extended to a full order: that zero is not a sum of nonzero terms of the form a^2 or pa^2 for $a \in R$ and $p \in P$. This fact is also equivalent to weak König's Lemma.

Theorem 5.2.9. The following are equivalent over RCA_0:

1. WKL_0.
2. If P is a partial order on a field F, then P extends to a full order on F if and only if the sum of nonzero terms of the form a^2 or pa^2 ($a \in F$, $p \in P$) is never zero.

Proof. If we let $P = \{0\}$, then (2) says that F is orderable if and only if F is formally real. By Theorem 5.1.5 this is equivalent to weak König's Lemma, so (2) $\Longrightarrow$ (1). The argument that (1) $\Longrightarrow$ (2) is nearly identical to that in the proof of Theorem 5.2.8. The forwards direction of (2) is provable in RCA_0: if P_1 is a full order extending P, then the sum of nonzero terms of the form a^2 or pa^2 for $a \in F$ and $p \in P_1$ is never zero, and every $p \in P$ is also in P_1. For the backwards direction, we build a infinite tree $T \in 2^{<\mathbb{N}}$ every infinite path in which codes a full order of F extending P. The construction of T is identical to that in the proof of Theorem 5.2.8. The only difference is in the verification that T is infinite.

To verify this, suppose T were finite. Then there was a least stage s for which $T_s = T_{s+1}$. Again, we define for each $\sigma \in 2^{<\mathbb{N}}$ of length s,

$$\sigma_i = \begin{cases} 1 & \text{if } \sigma(i) = 1, \\ -1 & \text{if } \sigma(i) = 0. \end{cases}$$

Since no new nodes were added at stage s of the construction of T, for each $\sigma \in T_s$ of length s there is some $i, j, k < s$ so that either $\sigma_i a_i + \sigma_j a_j + \sigma_k a_k = 0$ or $\sigma_i t_i \cdot \sigma_j a_j + \sigma_k a_k = 0$ or $\sigma_i a_i + \sigma_j a_j = 0$ or $\sigma_i a_i + p_j = 0$. This time let

$$g_\sigma = \prod_{i,j,k<s} (\sigma_i a_i + \sigma_j a_j + \sigma_k a_k)^2 (\sigma_i t_i \cdot \sigma_j a_j + \sigma_k a_k)^2 (\sigma_i a_i + \sigma_j a_j)^2 (\sigma_i a_i + p_j)^2.$$

Then $g_\sigma = 0$ for all $\sigma \in 2^{<\mathbb{N}}$ of length no more than s. Let

$$S = \sum_{\sigma \in 2^{<\mathbb{N}}, |\sigma| = s} g_\sigma.$$

Since each $g_\sigma = 0$, we clearly have $S = 0$. Now what form do the individual terms of S have? Well consider what happens when each g_σ is multiplied out. The result is a sum of terms each having the form $\prod_{i,j<s} p_j^{n_j} (\sigma_i a_i)^{m_i}$. For some of these terms, all the m_i are even. In this case, the term is non-zero and has the form a^2 or pa^2 where $a \in F$ and $p \in P$. Of course there may be other terms in the expansion of g_σ for which some m_i is odd. However, for each of these, the term will be the negative of the corresponding term in the expansion of $g_{\sigma'}$, where $\sigma(j) = \sigma'(j)$ for exactly all $j \neq i$. In S, these terms will cancel out. Thus $S = 0$ is in fact the sum of nonzero terms of the form a^2 or pa^2 where $a \in F$ and $p \in P$. This contradicts our assumption, so we conclude that T is infinite. *QED*

5.3 Further Extensions

We now consider a few generalization of the results from the previous section. One idea is to consider the conditions for when a partial order on a field F can be extended to a full order of a field *extending* F. In [17] we find the following classical result along these lines.

Lemma 5.3.1. Let $F \subset F_1$ be fields. Then a full order P of F extends to a full order P_1 of F_1 if and only if $\sum_{i=1}^{n} p_i x_i^2 = 0$ has no nontrivial solution in F_1, for all $n \in \mathbb{N}$ and $p_1, p_2, \ldots, p_n \in P \setminus \{0\}$.

Note since P is a full order, it contains 1, so $\sum_{i=1}^{n} p_i x_i^2 = 0$ having no nontrivial solutions is equivalent to zero not being the sum of nonzero terms of the form a^2 or pa^2. So this result is very reminiscent of (2) in Theorem 5.2.9. In fact, since P is a partial order on F_1, this result implies (2) of Theorem 5.2.9. Thus the lemma implies weak König's Lemma. Additionally, using an argument nearly identical to the proof of Theorem 5.2.9, we can proof the lemma in WKL_0.

We can strengthen the lemma by allowing P to be a partial order on F (as long as we also take the $p_1, p_2, \ldots p_n \in P \cup \{1\} \setminus \{0\}$, to properly parallel (2) from Theorem 5.2.9). It is easy to check that with this modification, the result is still equivalent to weak König's Lemma. Also, we can allow F to simply embed into F_1 (so $F \hookrightarrow F_1$ instead of $F \subset F_1$). That is:

Lemma 5.3.2. Let $f : F \hookrightarrow F_1$ be a field embedding, let P be a partial order

on F. Then there is a full order P_1 on F_1 such that $f(P) \subset P_1$, if and only if the sum of nonzero terms of the form a^2 or pa^2 ($a \in F_1$, $p \in f(P)$) is never zero.

This is again equivalent to WKL_0 over RCA_0. This is not entirely obvious: in general, the range of a function need not exist, so to prove the lemma, we cannot simply apply Theorem 5.2.9 to F_1 with it's partial order $f(P)$. But this is not necessary. We can build the tree of full orders extending $f(P)$ without knowing $f(P)$. This is done by not extending a $\sigma \in T_s$ of length s if there are $i, j < s$ such that $a_i = f(p_j)$ but $\sigma(i) = 0$. The rest of the proof is analogous to that of Theorem 5.2.9.

To summarize, we have the following theorems.

Theorem 5.3.3. The following are pairwise equivalent over RCA_0:

1. WKL_0.

2. A partial order P on a field F is extendable to a full order if and only if 0 is not the sum of nonzero terms of the form a^2 or pa^2 where $a \in F$ and $p \in P$.

3. A partial order P on a field $F \subseteq F_1$ extends to a full order on the field F_1 if and only if 0 is not the sum of nonzero terms of the form a^2 or pa^2 where $a \in F_1$ and $p \in P$.

4. Let F and F_1 be fields with $f : F \hookrightarrow F_1$, and let P be a partial order on F. Then there is a full order on F_1 containing $f(P)$ if and only if 0 is not the sum of nonzero terms of the form a^2 or pa^2 where $a \in F_1$ and $p \in f(P)$.

Theorem 5.3.4. The following are pairwise equivalent over RCA_0:

1. WKL_0.

2. A full order P on a field $F \subseteq F_1$ extends to a full order on the field F_1 if and only if $\sum_{i=1}^{n} p_i x_i^2 = 0$ has no nontrivial solution in F_1, where $p_0, \ldots, p_n \in P \setminus \{0\}$.

3. A full order P on a field F is extendable to a full order on a field F_1 for which $F \hookrightarrow F_1$ if and only if $\sum_{i=1}^{n} p_i x_i^2 = 0$ has no nontrivial solution in F_1, where $p_0, \ldots, p_n \in P \setminus \{0\}$.

Bibliography

[1] C. Ash, J. Knight, M. Manasse, T. Slaman, *Generic Copies of Countable Structures*, Annals of Pure and Applied Logic, vol. 42, 195-205, North-Holland, 1989.

[2] J. Chisholm, *Effective Model Theory vs. Recursive Model Theory*, Journal of Symbolic Logic, vol. 55, 1168-1191, 1990

[3] R. Downey, *On Presentations of Algebraic Structures*, in Complexity, Logic and Recursion Theory, (A. Sorbi, ed.), Marcel Dekker, Lecture Notes in Pure and Applied Mathematics, vol. 197, 157-206, 1997.

[4] Yu.L. Ershov, *Theorie der Numerierungen*, Zeits. Math. Logik Grund. Math., vol. 23, 289-371, 1977.

[5] H.M. Friedman, S.G. Simpson, R.L Smith *Countable Algebra and Set Existence Axioms* Annals of Pure and Applied Logic, vol. 25, 141-181, 1983.

[6] L. Fuchs, *Partially Ordered Algebraic Systems*, Pergamon Press, 1963.

[7] S.S. Goncharov, *Limit Equivalent Constructivizations*, Mathematical Logic and Theory of Algorithms, Nauka Sibirsk. Otdel., Novosibirsk, 4-12, 1982.

[8] K. Hatzikiriakou, S. G. Simpson, *WKL_0 and Orderings of Countable Abelian Groups*, Contemporary Mathematics, vol. 106, 177-180, 1990.

[9] T.W. Hungerford, *Algebra*, Springer-Verlag, 1974

[10] N. Jacobson, *Lectures in Abstract Algebra: Theory of Fields and Galois Theory* Van Nostrand, 1964

[11] S. Lang, *Algebra*, 3rd ed., Springer-Verlag, 2005

[12] E.W. Madison *A Note on Computable Real Fields*, Journal of Symbolic Logic, vol. 35(2), 239-241, 1970.

[13] G. Metakides, A. Nerode, *Effective Content of Field Theory*, Annals of Mathematical Logic, vol. 17, 289-320, 1979.

[14] R. Miller, **d**-*Computable Categoricity for Algebraic Fields*, to appear in Journal of Symbolic Logic, 2009.

[15] R. Miller, H. Schoutens, *Computably Categorical Fields via Fermat's Last Theorem*, submitted for publication.

[16] A.T. Nurtazin, *Strong and Weak Constructivizations and Enumerable Families*, Algebra and Logic, vol. 13, 177-184, 1974.

[17] A. Prestel, *Lectures on Formally Real Fields*, Lecture Notes in Mathematics, 1093, Springer-Verlag, 1984

[18] S.G. Simpson, *Subsystems of Second Order Arithmetic*, Springer-Verlag, 1998

[19] R.I. Soare, *Recursively Enumerable Sets and Degrees*, Perspectives in Mathematical Logic, Springer-Verlag, 1987.

[20] R. Solomon, *Reverse Mathematics and Fully Ordered Groups* Notre Dame Journal of Formal Logic, vol. 39(2), 157-189, 1998.