Reverse Mathematics of Divisibility in Integral Domains

by

Valentin B. Bura

A thesis
submitted to the Victoria University of Wellington
in fulfilment of the
requirements for the degree of
Master of Science
in Mathematics.

Victoria University of Wellington
2013

Abstract

This thesis establishes new results concerning the proof-theoretic strength of two classic theorems of Ring Theory relating to factorization in integral domains.

The first theorem asserts that if every irreducible is a prime, then every element has at most one decomposition into irreducibles; the second states that well-foundedness of divisibility implies the existence of an irreducible factorization for each element.

After introductions to the Algebra framework used and Reverse Mathematics, we show that the first theorem is provable in the base system of Second Order Arithmetic RCA_0, while the other is equivalent over RCA_0 to the system ACA_0.

Acknowledgments

Foremost thanks are due to my supervisor, A/Professor Noam Greenberg, for suggesting the topic and directing its development. Collaborating with him was a privilege and a first-rate learning opportunity: his great deal of patience, thoughtful advice, pedagogical foresight and mathematical intuition have guided my steps through this first research project.

Professor Rod Downey influenced my journey as a graduate student in Mathematics.

Dr Peter Donelan and Dr BD Kim were available for discussion and had suggestions. Dr Dillon Mayhew supervised my research for a period of time.

Dr David Diamondstone and Dr Dan Turetski, the postdocs working in Computability at SMSOR, have helped the development of my ideas.

I was inspired by many of my past lecturers in Logic, including Professor Cris Calude at Auckland, Dr Colin Bailey, Professor Rob Goldblatt and Professor Edwin Mares in Wellington.

I have benefited from the friendship and fruitful exchange of ideas with Ahmad Abdul-Ghaffar, Valentina Baccetti, Amanda Cameron, Dr Carolyn Chun, Mohammed Daher, Henry Macdonald, Joel Miller and Zheng Jingwei.

My thoughts turn towards the multitude of people from which I have learned during my formative years. I mention here three of my high-school teachers: Mioara Enache and Ioan Lepãdatu, who have fostered my mathematical abilities, and Gilbert Danciu, who has instilled in my mind the desire to succeed in academic research.

On a personal note, I thank my parents, Lucian and Raluca, for their continuous encouragement and their support on multiple levels, key ingredients in my ability to pursue a higher education.

Contents

Chapter 1

Introduction

The program of Reverse Mathematics was introduced by Harvey Friedman in his 1974 address to the International Congress of Mathematicians in Vancouver. It is a program in Mathematical Logic with deep philosophical import, redefining one of the pillars of the Foundations of Mathematics, namely Proof Theory.

1.1 Background

Reverse Mathematics is a study of the foundations of ordinary Mathematics, and this involves both reasoning within a given proof system and "going backwards from the theorems to the first principles". The main question it poses is "which set-existence axioms are needed to prove the theorems of non-set-theoretic Mathematics?" It stands in intimate connection with Computability Theory, since a certain notion of effectiveness provides a foundation to these types of investigations.

The results the logician focuses on are, in a sense, already known to be true if one considers the larger proof framework of ZFC Set Theory. It is not the 'truth' of results that one seeks to establish, but the more philosophically adequate notion of 'relative truth'. We come to a better understanding of what this means if we try to restrict our attention to different programs in the Philosophy of Mathematics, ranging from Constructive Mathematics to Impredicativism.

The process is carried out in subsystems of Second Order Arithmetic,

where one takes a base system as proving grounds and then proves that a certain theorem is equivalent to a stronger set of axioms, over the base system. Like any equivalence, this proof is done in two parts: first, a direct proof is formulated that the theorem follows from the axioms, and then a 'reversal' step is appended, in which it is shown that the axioms follow if we are to assume the theorem.

In the words of S. S. Wainer, reviewing Friedman's survey, two main themes can be identified straight away: first, that "the 'proper' axioms to use in proving particular fundamental theorems of mathematics often turn out to be (provably) equivalent to those theorems", and second that "stronger axioms are needed to provide explicit definitions of hard-to-define sets of integers than merely to prove their existence".

Friedman introduced several axioms for arithmetic sets. RCA, the base system, which is too weak for most proofs but strong enough for most definitions, consists of basic axioms for arithmetic manipulations, a restricted induction scheme and a comprehension scheme for computable properties. Hence, provability in this system is equivalent to effectiveness.

ACA is the Arithmetic Comprehension axiom system, KL consists of RCA (recursive comprehension axioms) plus König's Lemma, SLUB consists of RCA plus the axiom "every bounded sequence of reals has a l.u.b.". SBW is the sequential Bolzano-Weierstrass system. The above systems are all equivalent.

WKL (the weak König's Lemma system, for binary trees) is equivalent to SHB (sequential Heine-Borel system) and to the reflection principle "if a statement is true there is a structure in which it holds" (it has a model), which can also be viewed as a soundness statement. The second theme is illustrated by the fact that whereas ACA is clearly sufficient to explicitly define non-recursive sets, WKL is not.

Even though it deals with Constructivism, Reverse Mathematics differs from this school of thought because it assumes the framework of Classical Logic and does not make the radical ontological commitments of intuitionists.

However, from this perspective, Reverse Mathematics is the answer to those who are not prepared to make the full set-existence commitments that a working mathematician makes: the big five subsystems correspond

roughly to Bishop's Constructive mathematics, Hilbert's Finitistic reductionism, Weyl's and Feferman's Predicativism, Friedman's and Simpson's Predicative reductionism, and to Impredicativism respectively.

1.2 Effective and Reverse Algebra

Effective Algebra incorporates both Computable Algebra and Constructive Algebra. Good surveys of the latter are found in [1, 16].

The systematic study of computability in the framework of Ring Theory started in the fifties and sixties with [7, 8, 20, 21].

The work of Fröhlich and Sheperdson in [7, 8] assumed a less rigorous foundation for computable sets, while Rabin in [20, 21] and Mal'cev in [14] developed the modern concept of a computable structure by using an analogue of the Gödel numbering of logical syntax.

The focus of [7] was effective factorization of polynomials, extending on the work of Van der Waerden ([29]) and Kneser([12]). In particular, [29] has discussed the problem of carrying out certain field theoretical procedures effectively, in a "finite number of steps", and it was shown that there can be no general algorithm for splitting polynomials over an explicitly given field K, more precisely that such an algorithm would lead to a general procedure for deciding whether arbitrarily given properties of positive integers are instantiated. (A splitting algorithm for a field K decides the irreducibility of a polynomial over $K[x]$.) In [29] it was defined an "explicitly given" field as one whose elements are uniquely represented by distinguishable symbols with which one can perform the operations of addition, multiplication, subtraction and division in a finite number of steps, and Fröhlich and Sheperdson assume the same framework.

In [7, 8] it was constructed an explicit field for which there is no splitting algorithm, and explicit fields K, $\bar{K}$ such that $\bar{K}$ is a simple non separable extension of K, and K has a splitting algorithm but $\bar{K}$ does not. In addition to this, they show there exist isomorphic "explicitly given fields", one of which possesses a splitting algorithm but the other does not, and that a computable field with a splitting algorithm has a computable algebraic closure that is unique up to computable isomorphism.

In [20, 21] Rabin develops the notion of what it means for an algebraic

structure to be "computable" by defining an indexing of a set S as an injective mapping $i\colon S \to \omega$ such that $i(S)$ is a recursive subset of ω. Several results are then proved, including the fact that the algebraic closure T of any computable field K is computable, and the natural embedding of K into T is computable.

Mal'cev ([14]), working on the same framework based on Gödel numbering, focused on effective universal algebras.

A historical note on Computability in Ring Theory is found in [26].

Reverse Algebra (Reverse Mathematics in the context of Algebra) is intimately related to Computable Algebra and debuted with the seminal paper by Friedman et al. "Countable Algebra and set existence axioms" ([6]). Several equivalences are proved over RCA_0. It is shown that WKL_0 is equivalent to the following statements: every countable field has a unique algebraic closure; every countable formally real field is orderable; every countable formally real field has a real closure; every countable commutative ring has a prime ideal. It is shown that ACA_0, is equivalent to the statements: every countable field is isomorphic to a subfield of its algebraic closure; every countable ordered field is isomorphic to a subfield of its real closure; every countable field has a transcendence base; every countable vector space has a basis; every countable abelian group has a torsion subgroup; every countable abelian group has a unique divisible hull; every countable commutative ring (or countable integral domain) has a maximal ideal. Finally, it is shown that ATR_0 is equivalent to the statement: every countable reduced abelian group has a system of Ulm invariants which determine it up to isomorphism, and that $\Pi^1_1 - CA$ is equivalent to the statement: every countable abelian group is the direct sum of a divisible group and a reduced group.

Subsequently, weaker theories have been investigated to allow for equivalences with RCA_0 to be proven; some equivalences are: every finitely generated vector space over a countable field has a basis (Friedman quoted by [11]); a polynomial over a countable field has finitely many roots, such a polynomial has an irreducible factor, the ring of polynomials over a countable field is a unique factorization domain ([25]) and a principal ideal domain, every countable Euclidean domain is a unique factorization domain, if R is a countable unique factorization domain, so is $R[x]$ ([22]).

For a treatment of Reverse Algebra we refer the reader to [24].

1.3 Results

Our problems relate to two well-known equivalent characterizations for Unique Factorization Domains. Either one of these characterizations is employed as a definition, while the other is showed to be equivalent. The two characterizations are:

$$\text{ACCP } \& \text{ AP-domain} \tag{I}$$
$$\text{Atomic } \& \text{ U-UFD} \tag{II}$$

Characterization I invokes the Ascending Chain Condition on Principal Ideals (ACCP), which is equivalent to the statement "the divisibility relation is well-founded". It also invokes the property of being an AP-domain, by which every irreducible is a prime. Hence, the first characterization reads:

The divisibility relation is well-founded and every irreducible is a prime.

Characterization II invokes the property of being Atomic, which requires every element of the ring to have an irreducible factorization, and the property of being an U-UFD, which stipulates that any element which admits an irreducible factorization has a unique such factorization, up to units and order of the factors. So this reads:

Every element has *exactly one* factorization into irreducibles.

The equivalence is not hard to prove, and we state it here as the first theorem:

Theorem 1.1. *Let R be an integral domain. The following are equivalent:*

1. *R is an AP domain which satisfies the ACCP;*
2. *R is an Atomic U-UFD.*

These two characterizations hint towards two other classic theorems of Ring Theory. We will use these two theorems as objects of study and we will provide their strength relative to the five subsystems of Second Order Arithmetic used in Reverse Mathematics. The theorems depict two different implications. The first one links irreducibles, primes and unique factorizations:

Theorem 1.2. *If an integral domain is AP, then it is an U-UFD.*

As expected, the second theorem links ACCP and Atomicity:

Theorem 1.3. *If an integral domain satisfies the ACCP, then it is Atomic.*

Given the equivalence between the characterizations and the above implications, it is somewhat surprising that neither of the two converses hold, as shown in [10, 2]. Hence the situation is, in some sense, asymmetrical. This relationship is depicted below by Figure 1.1.

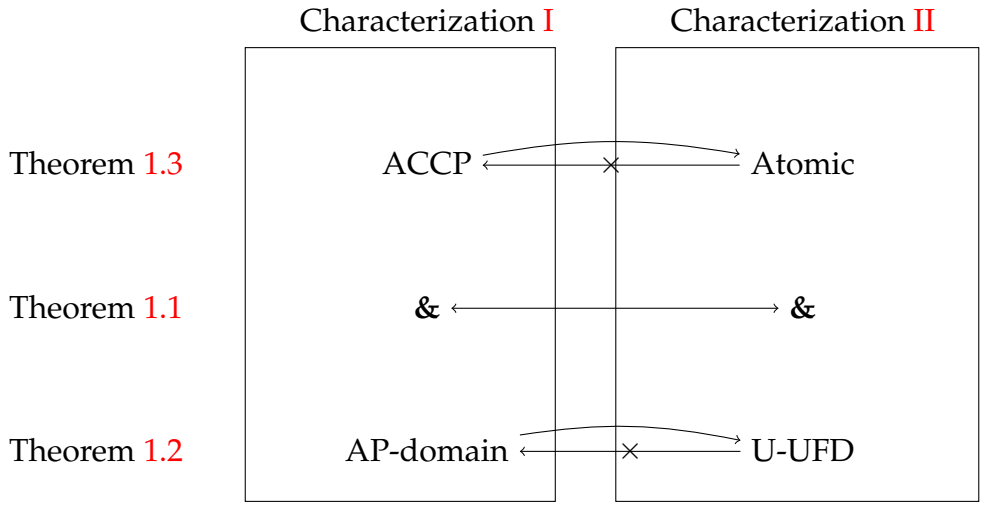


Figure 1.1: The logical structure of our main problems

It is perhaps less surprising that theorems 1.2 and 1.3 exhibit different proof-theoretic strengths. This can be easily seen by examining their standard proofs: while the proof of the second holds effectively, the proof of the first one requires the Halting Set as an oracle. It is these novel facts that the present work establishes.

More precisely, we give an involved proof that theorem 1.3 is equivalent to ACA_0 over RCA_0 while also giving an argument that theorem 1.2 is provable in RCA_0.

Chapter 2 introduces the notions of Algebra we will make use of in our treatment of UFDs. Chapter 3 provides a short introduction to Computability Theory and Reverse Mathematics and presents some results concerning Effective Algebra that will be useful in the next Chapter. Finally, Chapter 4

focuses on our main results. A brief conclusion is formulated at the end of Chapter 4.

Chapter 2

Elements of Algebra

This chapter sets up the framework of Abstract Algebra we will be interested in, which concerns the theory of commutative rings. Some of the material presented here is standard, but we include it in order to lay a foundation to our inquiry. Other parts of this chapter are more specialized and form prerequisites of Chapter 4, in which our results are presented.

In the Chapters concerning Algebra the capital letters P, Q, R, S will denote rings, small letters will usually denote elements of rings, maps will be referenced by greek letters φ, ψ, η, sets will be referenced by capitals I, J, K and the letters f, g, h will be reserved for polynomials.

We start by defining a ring structure.

Definition 2.1. A *ring* is a nonempty set R endowed with two binary operations, $+$ and $\cdot$, such that for all $a, b, c \in R$ the following conditions hold:
1. $a + b = b + a$ (commutativity of addition);
2. $(a + b) + c = a + (b + c)$ (associativity of addition);
3. $\exists\, 0 \in R$ such that $\forall a \in R, a + 0 = a$ (additive identity);
4. $\forall a \in R \exists - a \in R$ such that $a + (-a) = 0$ (additive inverses);
5. $a \cdot b = b \cdot a$ (commutativity of multiplication);
6. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (associativity of multiplication);
7. $\exists\, 1 \in R$ such that $\forall a \in R, a \cdot 1 = a$ (multiplicative identity);
8. $a \cdot (b + c) = a \cdot b + a \cdot c$ (distributivity).

In the literature, the structure defined above is known as a "commutative

ring with unity". These are precisely the kind of rings we will make use of in the present work, so we have restricted the definition of a ring to only include these objects.

Examples include the integers $\mathbb{Z}$, the integers modulo n, $\mathbb{Z}/n\mathbb{Z}$, and the set $Z[x]$ of all polynomials in the variable x with integer coefficients. We will give a formal treatment of polynomial rings below.

We will write $(R, +_R, \cdot_R, 0_R, 1_R)$ for the ring R, and if it is understood from context, the subscripts will be dropped.

For the treatment of basic Ring Theory, we follow Gallian in [9].

2.1 Divisibility

We begin our treatment of divisibility here.

Definition 2.2. A ring in which there are no non-zero elements a, b such that $a \cdot b = 0$ is called an *integral domain*.

A *unit* is an element $a \in R$ such that there is $b \in R$ with $a \cdot b = 1_R$. The set of units of R is denoted as $R^\times$. In an integral domain, the element a *divides* the element b if there exists c such that $a \cdot c = b$. We write $a \mid b$. Elements a and b of an integral domain D are called *associates* if $a = u \cdot b$ for a unit u. This is equivalent to $a \mid b$ and $b \mid a$, and we will write $a \sim b$. A non-zero element a of an integral domain D is called *irreducible* if it is a non-unit and, whenever $b, c \in D$ with $a = b \cdot c$, then b is a unit or c is a unit. In other words, a is irreducible if a is not a unit and whenever $b|a$, either b and a are associates or b is a unit. A non-zero element a of an integral domain D is called a *prime* if a is not a unit and $a|b \cdot c$ implies $a|b$ or $b|c$. For example, in $\mathbb{Z}$, the irreducible elements are the prime numbers p and their additive inverses $-p$. Non-unit elements which are not irreducible are called reducible.

Proposition 2.3. In an integral domain, every prime is irreducible.

Proof. Suppose p is prime and $p = a \cdot b$. Then, $p \mid ab$, by primeness $p \mid a$ or $p \mid b$. Suppose without loss of generality that $p \mid a$, we have that $p \sim a$, so b must be invertible.

□

The converse does not always hold; we will reserve a special name for a ring in which the converse is true.

Definition 2.4. A ring in which every irreducible is prime is called an *AP domain*.

Definition 2.5. An ideal of a ring R is a non-empty subset I of R such that:

1. $a - b \in I$ whenever $a, b \in I$,
2. $r \cdot a \in I$ whenever $r \in R$ and $a \in I$.

Hence, an ideal generated by I in R has the form:

$$\langle I \rangle = \{r_1 \cdot a_1 + r_2 \cdot a_2 + \cdots + r_k \cdot a_k \mid r_1, r_2 \cdots r_k \in R, a_1, a_2 \cdots a_k \in I\}.$$

A multiset B is a pair (S, m), where S is a set and m is a function $m\colon S \to \omega$. If $s \in S$, $m_s(B) = m(s)$ denotes the multiplicity of s in B. If $S = \{s_1, s_2 \cdots s_k \cdots\}$ with $m_{s_i} = n_i$, we write

$$B = [s_1, s_1 \cdots s_1, s_2, s_2 \cdots s_2, \cdots s_k, s_k \cdots s_k, \cdots],$$

where each s_i appears in B n_i many times.

To formalize the idea of unique factorization, we use the following definition.

Definition 2.6. An irreducible (prime) factorization of p in the ring Q is a finite multiset of irreducible (prime) elements $B = [p_i \mid i \leq n]$ in Q, such that $p \sim \prod_{i=1}^{n} p_i$.

We say B is a subset of B' up to association if there exists an injective function $f\colon B \to B'$ such that if $f(p) = p'$, then $p \sim p'$. If f is a bijection we say B and B' are equal up to association and write $B \sim B'$.

Since functions on multisets are defined for each copy of an element of their domain, copies of the same element may be mapped differently. For example, in the ring of integers $[2, 2]$ is a subset of $[2, -2, 3]$ up to association, since we can put $f(2) = 2$ and $f(2) = -2$; the two copies of the integer 2 represent distinct elements of the domain of f.

Atomicity will play an important part in the present work. We define it here.

Definition 2.7. An integral domain R is *Atomic* if every non-zero element of R has an irreducible factorization.

Note that the factorization of a unit of R is an empty multiset.

U-UFDs are also central in our treatment of divisibility.

Definition 2.8. An integral domain in which every element that admits a factorization into irreducible factors has a unique such factorization (up to association of multisets) is called an *unrestricted unique factorization domain*, or U-UFD for short.

We are now ready to define a Unique Factorization Domain.

Definition 2.9. An integral domain R is a *unique factorization domain* if

1. R is Atomic,
2. R is a U-UFD.

A *principal ideal* in a ring R is an ideal I generated by a single element a, i.e. $I = \{r \cdot a \mid r \in R\}$.

A *principal ideal domain* (PID) is an integral domain in which every ideal is principal. In a PID, the set of irreducibles coincides with the set of primes. Every element of a PID admits a factorization into irreducibles. It turns out that every PID is a UFD, for example the Integers and the Gaussian Integers. It must be noted that the converse does not hold: not every UFD is a PID. For example, $\mathbb{Z}[x]$ is not a PID (e.g. the set of polynomials in $\mathbb{Z}[x]$ whose constant term is even is a non-principal ideal) but it is a UFD.

As in a PID, every irreducible of a UFD is a prime.

Proposition 2.10. Every UFD is an AP domain.

Proof. Let p be an irreducible of Q and suppose $ph = ab$. We have $h = \prod_{h_i \in B_h} h_i$, $a = \prod_{a_j \in B_a} a_j$ and $b = \prod_{b_k \in B_b} b_k$, such that each factorization is unique.

Then, $p \cdot \prod_{h_i \in B_h} h_i = \prod_{a_j \in B_a} a_j \cdot \prod_{b_k \in B_b} b_k$.

By uniqueness, each irreducible on $[p] \cup B_h$ is an associate of an irreducible in $B_a \cup B_b$, so $[p] \cup B_h$ is a subset of $B_a \cup B_b$, up to association.

In particular, this means p associates with one irreducible in the factorization of ab, which means that either $p \mid a$ or $p \mid b$. This shows every irreducible of Q is prime.

□

We will make use of the following condition, which we name ACCP. We will prove later that the presence of this condition logically implies that every element admits a factorization into irreducibles.

Lemma 2.11. *Let R be an integral domain. The following are equivalent:*

1. Every ascending chain of principal ideals is eventually constant,

2. In R, the divisibility relation is well-founded; that is, there is no infinite descending chain $\langle c_i \rangle_{i \in \omega}$ such that c_{i+1} properly divides c_i.

Proof. We make use of the following facts:

Claim 1 For $a, b \in R$, $a \mid b$ if and only if $\langle a \rangle \subseteq \langle b \rangle$.

This fact is straightforward: if $a \mid b$, then $a \cdot r = b$ for some $r \in R$, which is equivalent to $\langle a \rangle \subseteq \langle b \rangle$.

Claim 2 a properly divides b if and only if $\langle a \rangle \subsetneq \langle b \rangle$.

Now, if $a \cdot r = b$ for non-unit r, then $b = a \cdot r \notin \langle a \rangle$ whereas $a \in \langle b \rangle$ and if $\langle a \rangle = \langle b \rangle$ then $a \cdot r_1 = b$ and $b \cdot r_2 = a$, which makes r_1 and r_2 inverses of each other.

1. $\Rightarrow$ 2.

Let $\langle p_i \rangle_{i \in \omega}$ be an infinite descending chain in divisibility. In light of the claims, this corresponds to an infinite ascending chain of principal ideals, contradicting 1.

2. $\Rightarrow$ 1.

Let $\langle I_i \rangle_{i \in \omega}$ be a non-constant ascending chain of principal ideals. From the claims, this corresponds to an infinite descending chain in divisibility, which proves divisibility is not well-founded, contradicting 2.

□

Proposition 2.12. Let B be a multiset of primes and C a multiset of irreducibles. Then $\prod_{p \in B} p \mid \prod_{q \in C} q$ if and only if B is a subset of C up to association. Furthermore, the division is proper if and only if the subset inclusion is proper.

Proof. Suppose $\prod_{p_i \in B} p_i \mid \prod_{q_j \in C} q_j$. Since every p_i is prime, we have by induction for all p_i that $p_i \mid q_j$ for some $q_j \in C$. Define $f \colon B \to C$ by $f(p_i) = q_j$, where $j = \min\{j \mid p_i \mid q_j \text{ and } q_j \notin f[\{p_1, p_2, \cdots p_{i-1}\}]\}$. Notice that the choice of j ensures injectivity of f. By primeness, $p_i \sim f(p_i)$. We claim this choice is always possible, and we prove this by induction on $|B|$. If $|B| = 1$ with

$p \in B$, then $p \mid \prod_{q_j \in C} q_j$ and an induction on $|C|$ shows using primeness of p that p divides exactly one element of C, which shows our choice for mapping p under f is possible. Suppose $|B| = t+1$, $B = [p_1, p_2 \cdots p_t, p_{t+1}]$ and each p_i with $i \leq t$ is mapped to q_i under f. We have $\prod_{i \leq t+1} p_i = \prod_{q_k \in C} q_k$, and we can use cancellation to obtain $p_{t+1} = \prod_{q_k \in C, k \geq t+1} q_k$, and an induction on $|C \setminus f([p_1, p_2 \cdots p_t])|$ shows using primeness of p_{t+1} that p_{t+1} divides exactly one element of $C \setminus f([p_1, p_2 \cdots p_t])$, hence an injective choice for $f(p_{t+1})$ is possible.

Also, if the division was proper, this means that f was not surjective, which implies B is a proper subset of C up to association. This proves the first direction.

The second direction is easier: if B subset of C up to association, there is injective $f \colon B \to C$ such that $f(p) = q$ if $p \sim q$. This means $\prod_{p_i \in B} p_i \mid \prod_{p_i \in B} f(p_i) \mid \prod_{q_j \in C} q_j$. Again, if B proper subset of C, then f is not surjective, which implies the division is proper.

□

The following is a somewhat technical consequence of a ring being an UFD. We will make use of it in Chapter 4

Proposition 2.13. If Q is a UFD, a is irreducible in Q, $b, c \in Q$ and m the greatest power of a dividing b , n the greatest power of a dividing c, and suppose $m > n$. Then $b \nmid c$.

Proof. Let $b = \prod_{p_i \in B} p_i$ and $c = \prod_{q_j \in C} q_j$ be prime decompositions of b and c in Q.

By Proposition 2.12, $\prod_{p_i \in B} p_i \mid \prod_{q_j \in C} q_j$ if and only if B is a subset of C up to association.

Suppose $b \mid c$, in the light of the claim this means $t \leq v$ and there is an injective map $f \colon \{1, 2 \cdots t\} \to \{1, 2 \cdots v\}$ such that each p_i with $i \leq t$ associates with some $q_{f(j)}$ for $j \leq v$.

Note that a is prime, so if $a^m \mid b$ then without loss of generality $a = u_i p_i$ for units u_i and $i \leq m \leq t$ and similarly since $a^n \mid c$ $a = v_j q_j$ for units v_j and $j \leq n \leq v$.

But then $a = u_i p_i = v_i q_{f(i)}$ for all $i \leq m$, and so $a^m \mid c$. Since $m > n$ and we assumed n is the largest such that $a^n \mid c$, we have a contradiction.

□

Since an isomorphism is a "structure-preserving map", it makes sense for many properties to be preserved under an isomorphism.

Proposition 2.14. If R, Q are rings such that $R \cong Q$ via isomorphism φ, then

1. $\varphi(0_R) = 0_Q$,
2. $\varphi(1_R) = 1_Q$,
3. if $u \in R^\times$ then $\varphi(u) \in Q^\times$,
4. if p is irreducible in R, then $\varphi(p)$ is irreducible in Q,
5. if p is prime in R, then $\varphi(p)$ is prime in Q,
6. if R is an integral domain, then Q is an integral domain,
7. if R is a UFD, then Q is a UFD.

The proof is straightforward, so we omit it.

2.2 Localization

A multiplicative subset of a ring R is a subset of R that contains 1_R and is closed under multiplication, but it does not contain 0_R.

Definition 2.15. If R is a ring and $a_1, a_2 \cdots a_k \in R$, P is a multiplicative subset of R generated by $a_1, a_2 \cdots a_k$ if it is the collection of finite products of elements in $\{a_1, a_2 \cdots a_k\}$.

We use r/a in the ring R to denote the element $r \cdot a^{-1}$, for a unit a.

The localization of a ring R with respect to a multiplicative set S is a generalization of the idea of fraction. Intuitively, it contains precisely those "fractions" of the form r/s where $r \in R$ and $s \in S$. We make this notion precise with the following definition.

Definition 2.16. Let R be an integral domain, and I be a multiplicative subset of R. Define a relation $\sim$ on $R \times I$ by setting $\langle r, a\rangle \sim \langle r', a'\rangle$ if $r \cdot a' = r' \cdot a$ in R. Remark 2.17 shows that $\sim$ is an equivalence relation. The localization of R by I, written $I^{-1}R$, is defined as the collection of $\sim$-equivalence classes.

We define the operations on $I \times R$:

$\langle r, a\rangle +_{I\times R} \langle r', a'\rangle = \langle ra' + r'a, a \cdot a'\rangle$, and $\langle r, a\rangle \cdot_{I\times R} \langle r', a'\rangle = \langle r \cdot r', a \cdot a'\rangle$.

Operations on $I^{-1}R$ are defined by taking the equivalence classes of the operands and the results. Remark 2.18 shows these operations are well-defined. The multiplicative subset of R generated by a is $\{a^k \mid k \in \omega\}$. If I is generated by a single element a, we denote the localization of R by I by R_a.

Remark 2.17. The relation $\sim$ on $R \times I$ of Definition 2.16 is an equivalence relation.

Proof. Reflexivity and symmetry of $\sim$ are immediate. For transitivity, let $\langle r, a\rangle \sim \langle r', a'\rangle$ and $\langle r', a'\rangle \sim \langle r'', a''\rangle$. Then $r\cdot r'\cdot a'' = r\cdot_Q r''\cdot a'$, multiplying by a gives $r\cdot r'\cdot a\cdot a'' = r\cdot a\cdot r''\cdot a'$, which is equivalent to $(r\cdot a'')\cdot(r'\cdot a) = (r'\cdot a)\cdot(r''\cdot a)$ and by cancellation, $r \cdot a'' = r'' \cdot a$.

□

Remark 2.18. The operations on $I^{-1}R$ are well-defined.

Proof. Let $\langle r, a\rangle \sim \langle r', a'\rangle$ and $\langle p, b\rangle \sim \langle p', b'\rangle$.

We need to show that $\langle r'b' + p'a', a'b'\rangle \sim \langle rb + pa, ab\rangle$ and $\langle r'p', a'b'\rangle \sim \langle rp, ab\rangle$.

Note that $ra' = r' \cdot a$ and $pb' = p' \cdot b$.

For addition, we have: $(r'b' + p'a') \cdot ab = r'b'ab + p'a'ab = (rb + pa) \cdot a'b'$, as required.

For multiplication, we have: $r'p' \cdot ab = rp \cdot a'b'$, as required.

□

We show below that a localization is always a ring and its elements can be written in the fraction form.

Remark 2.19. If R is an integral domain and I is a multiplicative subset of R, then the localization of R by I, $I^{-1}R$, is a ring.

Proof. We note that $[\langle 0, 1\rangle]$ and $[\langle 1, 1\rangle]$ are the identities under addition and multiplication.

We note that the additive inverse of $[\langle r, a\rangle]$ is $[\langle -r, a\rangle]$, since $[\langle r, a\rangle] + [\langle -r, a\rangle] = [\langle 0, a\rangle] \sim [\langle 0, 1\rangle]$.

Let $[\langle r, a\rangle]$, $[\langle r', a'\rangle]$ and $[\langle r'', a''\rangle]$ be elements of $I^{-1}R$.

That the operations on $I^{-1}R$ are well-defined was shown on Remark 2.18.

Commutativity of addition carries from R: $[\langle r, a\rangle] + [\langle r', a'\rangle] = [\langle r \cdot a' + r' \cdot a, a \cdot a'\rangle] = [\langle r' \cdot a + r \cdot a', a' \cdot a\rangle] = [\langle r', a'\rangle] + [\langle r, a\rangle]$.

Commutativity of multiplication carries as well: $[\langle r, a\rangle] \cdot [\langle r', a'\rangle] = [\langle r \cdot r', a \cdot a'\rangle] = [\langle r' \cdot r, a' \cdot a\rangle] = [\langle r', a'\rangle] \cdot [\langle r, a\rangle]$.

Associativity of addition: $[\langle r, a\rangle] + ([\langle r', a'\rangle] + [\langle r'', a''\rangle]) = ([\langle r, a\rangle] + [\langle r', a'\rangle]) + [\langle r'', a''\rangle] = [\langle ra'a'' + r'aa'' + r''aa', aa'a''\rangle]$.

Associativity of multiplication: $[\langle r, a\rangle] \cdot ([\langle r', a'\rangle] \cdot [\langle r'', a''\rangle]) = ([\langle r, a\rangle] \cdot [\langle r', a'\rangle]) \cdot [\langle r'', a''\rangle] = [\langle rr'r'', aa'a''\rangle]$.

Distributivity carries from R: $[\langle r, a\rangle]([\langle r', a'\rangle] + [\langle r'', a''\rangle]) = [\langle r, a\rangle] \cdot [\langle r', a'\rangle] + [\langle r, a\rangle] \cdot [\langle r'', a''\rangle] = [\langle rr'a'' + rr''a', aa'a''\rangle]$.

□

Remark 2.20. A ring R is embedded into $I^{-1}R$ by the map φ defined by $r \mapsto [\langle r, 1\rangle]$.

Proof. φ is injective since $r \cdot 1 = p \cdot 1$ implies $r = p$.

We show φ is a homomorphism. Additivity: $\varphi(r+p) = [\langle r+p, 1\rangle]$ while $\varphi(r)+\varphi(p) = [\langle r, 1\rangle]+[\langle p, 1\rangle]$ which is the same as $[\langle r+p, 1\rangle$. Multiplicativity is analogous.

□

At times we will choose to regard R as a subring of $I^{-1}R$ and identify R with its image under this embedding.

Remark 2.21. The equivalence class of $\langle r, a\rangle$ in $I^{-1}R$ is equal to $\varphi(r)/\varphi(a)$, where φ is the canonical embedding $\varphi\colon R \to I^{-1}R$.

Proof. We note that $\varphi(a)$ is a unit of $I^{-1}R$, since $\varphi(a) = [\langle a, 1\rangle]$ and $[\langle a, 1\rangle] \cdot [\langle 1, a\rangle] = [\langle 1, 1\rangle]$.

Also note that $\varphi(r)/\varphi(a) = \varphi(r) \cdot (\varphi(a))^{-1} = [\langle r, 1\rangle] \cdot [\langle 1, a\rangle] = [\langle r, a\rangle]$.

□

Due to Remarks 2.19 and 2.21, we can write r/a for the element $[\langle r, a\rangle]$ of $I^{-1}R$, and note that this notation is well-defined.

If the underlying ring R is an integral domain or a UFD, the localization of R by one of its multiplicative subsets is an integral domain or a UFD.

Lemma 2.22. *Let R be an integral domain and I be a multiplicative subset of R. Then $I^{-1}R$, the localization of R by I, is an integral domain.*

Proof. Suppose $p/a \cdot r/b = 0$, for $p, r \in R$, $a, b \in I$. Note that $p/a = 0$ if and only if $p = 0$ and assume $p/a \neq 0$ and $r/b \neq 0$, so $p \neq 0$, $r \neq 0$. But $p/a \cdot r/b = pr/ab$, so $pr = 0$, so R cannot be an integral domain.

□

Lemma 2.23. *Let R be an integral domain and I a multiplicative subset of R. If $p \in R$ is prime, then in $I^{-1}R$ p is a unit or prime.*

Proof. Let $a \in R$ be prime and not a unit of $I^{-1}R$. Suppose $a \mid r^{-1}b \cdot q^{-1}c$ in $I^{-1}R$. So $d^{-1}e \cdot a = r^{-1}b \cdot q^{-1}c$ for some $d^{-1}e \in I^{-1}R$. Then $a \nmid d$ in R since a is not a unit of $I^{-1}R$. So $eqr \cdot a = dbc$. Since a is prime and $a \nmid d$, then it must be the case that $a \mid b$ or $a \mid c$ in R. But then $a \mid r^{-1}b$ or $a \mid q^{-1}c$ in $I^{-1}R$, as required.

□

Proposition 2.24. Let R be an integral domain. If every element of R has a prime factorization, then R is a UFD.

Proof. We need to prove R is Atomic and U-UFD.

Atomicity follows immediately from the assumption and the fact that every prime is irreducible.

Let $a \in R$. We know a has a prime decomposition B. Suppose C is another irreducible factorization of a. By Proposition 2.12, we know that B is a subset of C up to association. But if $B \neq C$ up to association, then $\prod_{q \in B} q$ properly divides $\prod_{p \in C} p$, which is not the case since they are associates.

□

Lemma 2.25. *Let R be a UFD and let I be a multiplicative subset of R. Then $I^{-1}R$, the localization of R by I, is a UFD.*

Proof. By Lemma 2.22, $I^{-1}R$ is an integral domain.

We note that prime elements in I become units in $I^{-1}R$. This is immediate, since all elements of I are invertible in $I^{-1}R$.

Take an arbitrary non-zero element $r^{-1}a$ of $I^{-1}R$. Let the prime factorization of a in R be B with $a \sim \prod_{p_i \in B} p_i$. We want to show that it is an associate of a product of primes of $I^{-1}R$. But $r^{-1}a$ is an associate of a, units of R are also units of $I^{-1}R$ and if an element is prime in R, by Lemma 2.23 it is either

a unit or a prime in $I^{-1}R$. Let B' be the multiset of elements of B that are units in $I^{-1}R$, then $B \setminus B'$ is the required prime factorization of $r^{-1}a$. By Proposition 2.24, the localization $I^{-1}R$ is a UFD.

□

2.3 Polynomial Rings

Next, we give a formal treatment of the ring of polynomials $R[x_1, x_2 \cdots x_k]$ associated with a ring R. Informally, this comprises of the collections of finite expressions of the form $\sum_\iota r_\iota \bar{x}^\iota$, where ι is a multi-index. Formally, polynomials can be thought of as finite (nested) sequences of elements of R.

Definition 2.26. Let R be a ring. A *polynomial in one variable* f over R is an element of $R^{<\omega}$, i.e. a finite tuple of the form $\langle r_0, r_1, r_2 \cdots r_n \rangle$, where $r_i \in R$ for $0 \leq i \leq n$, $n \in \omega$ and $r_n \neq 0$. We write as shorthand $f(x) = \sum_{i=0}^{n} r_i x^i$ for the polynomial, and $R[x]$ for the class of all such polynomials. The operations on $R[x]$ are defined naturally as:

$(\sum_{i=0}^{n} r_i x^i) +_{R[x]} (\sum_{i=0}^{n} t_i x^i) = \sum_{i=0}^{n} (r_i + t_i) x^i$, and

$(\sum_{i=0}^{n} r_i x^i) \cdot_{R[x]} (\sum_{i=0}^{m} t_i x^i) = \sum_{k=0}^{m+n} (\sum_{i+j=k} r_i \cdot t_j) x^k$.

By the degree of f we mean the largest $i \leq n$ such that $r_i \neq 0$, and write $deg(f) = i$. If $a \in R$, then f evaluates at a as $f(a) = \sum_{i=0}^{n} r_i a^i$.

We extend this to finitely many variables, and let $R[x_1, x_2 \cdots x_{k-1}, x_k] = R[x_1, x_2 \cdots x_{k-1}][x_k]$

To define a shorthand notation, we write $\bar{x} = x_1, x_2 \cdots x_k$ and if $\iota = i_1, i_2 \cdots i_k$, where $i_1, i_2 \cdots i_k \in \omega$, define $\bar{x}^\iota = x_1^{i_1} x_2^{i_2} \cdots x_k^{i_k}$, and write $g(\bar{x}) = \sum_\iota q_\iota \bar{x}^\iota$, where only finitely many q_ι are different from zero.

By the degree of g relative to x_j we mean the largest $i_j \in \iota$ with $q_\iota \neq 0$ and write $deg_{x_j}(g) = i_j$.

If $a_1, a_2 \cdots a_k \in R$, write $\bar{a} = a_1, a_2 \cdots a_k$, and then g evaluates at $\langle a_1, a_2 \cdots a_k \rangle$ as $g(\bar{a}) = \sum_\iota q_\iota \bar{a}^\iota$.

Note that the zero polynomial is coded by the empty string.

We note in the following remark that if $\bar{x'}$ is a permutation of $\bar{x}$, then $R[\bar{x}] = R[\bar{x'}]$.

Remark 2.27. Note that $R[x_{n_1}, x_{n_2} \cdots x_{n_k}]$ for distinct $n_1, n_2 \cdots n_k \in \omega$ refer to the same polynomial ring, namely $R[x_1, x_2 \cdots x_k]$, therefore the indeterminate variables are not to be distinguished by order. We will sometimes write $R[y, x_1, x_2 \cdots x_k]$ and this is the same as $R[x_1, x_2 \cdots x_k, x_{k+1}]$.

We give a proof that the collection of polynomials associated with a ring R forms a ring and further below that if R is an integral domain, then $R[\bar{x}]$ is an integral domain.

Remark 2.28. If R is a ring, then $R[x_1, x_2 \cdots x_k]$ is a ring and R embeds into $R[x_1, x_2 \cdots x_k]$.

As is the case with localization, note that technically R is only embedded into $R[x_1, x_2 \cdots x_k]$, however at times we choose to regard R as a subring of $R[x_1, x_2 \cdots x_k]$ and identify it with its image under the embedding.

Proof. Let $f, g, h \in R[x]$ with $f(x) = \sum_{i=0}^{n} p_i x^i$, $g(x) = \sum_{j=0}^{m} q_j x^j$ and $h(x) = \sum_{l=0}^{v} r_l x^l$

Note that $\bar{f}(x) = \sum_{i=0}^{n} (-p_i) x^i$ is an additive inverse of $f(x)$. Commutativity of addition carries from R: $f(x) + g(x) = g(x) + f(x) = \sum_{i=0}^{\max(m,n)} (p_i + q_i) x^i$, where we can assume a padding of the polynomial of lesser degree, that is p_i or q_i are taken as zero if $n < i \leq m$ or $m < i \leq n$. Commutativity of multiplication carries as well: $f(x) \cdot g(x) = g(x) \cdot f(x) = \sum_{k=0}^{m+n} (\sum_{k=i+j} p_i q_j) x^k$. Associativity of addition: $f(x)+(g(x)+h(x)) = (f(x)+g(x))+h(x) = \sum_{i=0}^{\max(n,m,v)} (p_i + q_i + r_i) x^i$, where we can assume a similar padding. Associativity of multiplication: $f(x) \cdot (g(x) \cdot h(x)) = (f(x) \cdot g(x)) \cdot h(x) \sum_{k=0}^{n+m+v} (\sum_{k=i+j+l} p_i q_j r_l) x^k$. Distributivity carries from R: $f(x) \cdot (g(x) + h(x)) = f(x)g(x) + f(x)h(x)$ $\sum_{k=0}^{n+\max(m,v)} (\sum_{k=i+j} p_i (q_j + r_j)) x^k$

0_R and 1_R serve as additive and multiplicative inverses in $R[x]$. By iteration, $R[x_1, x_2 \cdots x_k]$ is a ring. Since R is embedded in $R[x_1, x_2 \cdots x_k]$ by the map $q \mapsto f$ for $f(\bar{x}) = q$, the second part of the remark holds.

□

Lemma 2.29. *Let R be an integral domain. Then $R[x_1, x_2 \cdots x_k]$ is an integral domain.*

Proof. Suppose $\sum_{i=0}^{n}(a_i x^i) \cdot \sum_{j=0}^{m}(b_j x^j) = 0_R$, for $a_i \in R$, $b_j \in R$ for $0 \leq i \leq n$ and $0 \leq j \leq m$. Assume $\sum_{i=0}^{n}(a_i x^i) \neq 0$ and $\sum_{j=0}^{m}(b_j x^j) \neq 0$, and this implies $a_n \neq 0$ and $b_m \neq 0$. But then $\sum_{k=0}^{n+m}(\sum_{k=i+j} a_i \cdot b_j)x^k = 0$. In particular, this means $a_n b_m = 0$, so R cannot be an integral domain. This shows $R[x]$ must be an integral domain. By iteration, $R[x_1, x_2 \cdots x_k]$, must be an integral domain.

□

The units of an integral domain R and the units of the associated ring of polynomials $R[x_1, x_2 \cdots x_k]$ coincide.

Proposition 2.30. If R is an integral domain, then $(R[x_1, x_2 \cdots x_k])^\times = R^\times$.

Proof. By Remark 2.28, $1_R = 1_{R[x]}$.

If $r \in R^\times$ then there is $r^{-1} \in R$ such that $r \cdot r^{-1} = 1_R$. By Remark 2.28, $R < R[x]$, so $r^{-1} \in R[x]$.

Now suppose $f, g \in R[x]$ such that $f \cdot g = 1_R$. Then, $\deg(fg) = \deg(1)$, so $\deg(f) + \deg(g) = 0$ which means both f and g are constant, so $f, g \in R^\times$.

By iteration, $(R[x_1, x_2 \cdots x_k])^\times = R^\times$.

□

Each element in the collection of indeterminates $\{x_1, x_2 \cdots x_k\}$ of $R[x_1, x_2 \cdots x_k]$ is irreducible.

Proposition 2.31. If R is an integral domain, in $R[x_1, x_2 \cdots x_k]$ each x_i with $1 \leq i \leq k$ is irreducible.

Proof. Suppose $g(\bar{x}) \cdot h(\bar{x}) = x_i$. Then $\deg_{x_i}(gh) = \deg_{x_i}(x_i)$, so $\deg_{x_i}(g) + \deg_{x_i}(h) = 1$. Note that $\deg_{x_j}(gh) = 0$ for $j \neq i$ so $\deg_{x_j}(g) = 0$ and $\deg_{x_j}(h) = 0$.

Suppose without loss of generality that $\deg_{x_i}(g) = 0$ and $\deg_{x_i}(h) = 1$. Then $h = ax_i + b$, $g = c$ for $a, b, c \in R$. Then $gh = acx_i + bc$ and so $c \neq 0$ so $b = 0$ and $c \cdot a = 1$ which means $c \in R^\times$ so $g \in R[x_1, x_2 \cdots x_k]^\times$.

□

The next result is known as the Factor Theorem, and it states that in $R[x]$ the element $a \in R$ is a zero of $f(x)$ if and only if $x - a$ divides $f(x)$.

Proposition 2.32 (Factor Theorem)**.** If R is an integral domain, $f \in R[x]$ and $a \in R$ then $f(a) = 0$ if and only if there exists $g \in R[x]$ with $\deg(g) < \deg(f)$ such that $f(x) = (x - a)g(x)$.

Proof. If $f(x) = (x - a)g(x)$ then $f(a) = (a - a)g(a) = 0 \cdot g(a) = 0$.

Conversely, suppose $f(a) = 0$, and suppose $f(x) = \sum_{i=0}^{n} r_i x^i$ with $r_n \neq 0$, so $\deg(f) = n$. Then, $f(x) = f(x) - f(a) = \sum_{i=0}^{n} r_i(x^i - a^i)$, but for any m, $x^m - a^m = (x - a)(x^{m-1} + x^{m-2}a + \cdots + a^{m-1})$. Then $f(x) = (x - a)g(x)$, where $g(x) = \sum_{i=1}^{n} r_i(x^{i-1} + x^{i-2}a + \cdots + a^{i-1})$, so $\deg(g) = n - 1$.

□

We use Proposition 2.32 to show that a polynomial of degree k can have at most k zeros.

Proposition 2.33. If R is an integral domain, then if $f \in R[x]$ with $f \neq 0$ and $\deg(f) = k$, there are at most k elements of R α_i for $i \leq k$ such that $f(\alpha_i) = 0$.

Proof. Proceed by induction on k. If $k = 0$, the polynomial is constant and we can see there are no roots of $f(x)$.

Assume that if $k < n$, all $f \in R[x]$ have at most k roots.

Let $k = n$ for some $f \in R[x]$. Let $a \in R$ such that $f(a) = 0$.

By Proposition 2.32, $f(x) = (x - a)g(x)$ for some $g \in R[x]$ with $\deg(g) < \deg(f) = n$. By induction hypothesis, $g(x)$ has at most $n - 1$ roots.

If $f(x)$ has no other roots, we are done. Otherwise, let $b \in R$, $b \neq a$ such that $f(b) = 0$. So $f(b) = (b - a)g(b) = 0$, and we can see that $g(b) = 0$, i.e. b is a root of $g(x)$. We know there are at most $n - 1$ choices for such a b. Thus, $f(x)$ has at most $n - 1 + 1 = n$ roots.

□

In any ring of polynomials $R[x]$ that contains the field of rationals, for any polynomial $f(x)$, there exists a unit α that is not a zero of f. Intuitively, this is because $\mathbb{Q}$ contains infinitely many units, while $f(x)$ can have only finitely many zeroes.

Proposition 2.34. If R is an integral domain and $\mathbb{Q} < R$, for any $f, g \in R[x]$ there is $\alpha \in R^\times$ such that $f(\alpha) \neq 0$ and $g(\alpha) \neq 0$.

Proof. Let $n = \deg(f)$ and $m = \deg(g)$. By Proposition 2.33, there are at most $m + n$ zeroes of f and g. But $\mathbb{Q}$ is an infinite field and $\mathbb{Q} \subseteq R^\times$. So $R^\times$ is infinite, while the set of roots of f and g is finite.

□

The next lemma is known as Gauss' Theorem. We will use it in a construction of Chapter 4.

Lemma 2.35 (Gauss' Theorem)**.** *Let R be a UFD. Then $R[x]$ is a UFD.*

2.4 Independence and Generation

In this section we are concerned with the algebraic independence and generation of certain subrings of a ring; both notions involve sets of elements of a ring R. Intuitively, a set $I \subset R$ is algebraically independent over some ring $Q < R$ if no finite sequence of ring operations involving elements of Q and elements of I evaluates to 0_R. Similarly, the ring generated by I over Q comprises of the collection of elements we obtain through such sequences of operations. We make these concepts precise in what follows.

Definition 2.36. If $Q < P$ are rings and $a_1, a_2, \cdots, a_k \in P$, the ring $Q[a_1, a_2, \cdots a_k] = \{f(a_1, a_2 \cdots a_k) \mid f \in Q[x_1, x_2, \cdots x_k]\}$ is the subring of P generated by $Q \cup \{a_1, a_2, \cdots, a_k\}$.

The ring $Q[a_1, a_2 \cdots a_k]$ is the smallest subring of P under inclusion which contains $Q \cup \{a_1, a_2, \cdots, a_k\}$. It is important to note that this ring depends on both P and Q.

A generated ring will always be a subring of the ring in which we generate it.

Remark 2.37. If $Q < P$ and $a_1, a_2 \cdots a_k \in P$, then $Q \leq Q[a_1, a_2, \cdots a_k] \leq P$.

We omit the proof of this remark.

The subring of P generated over Q by a multiplicative inverse of an element b of Q can be viewed as a collection of "fractions" over Q with denominators powers of b. Hence, such a collection of fractions is isomorphic to the localization Q_b. This is the gist of the following two propositions.

Proposition 2.38. If $Q < P$ are rings, $c \in Q$ and c is invertible in P, then $Q[c^{-1}] = \{b/c^k \mid b \in Q, k \in \omega\}$.

Proof. By Definition 2.36, $Q[c^{-1}] = \{f(c^{-1}) \mid f \in Q[x]\}$. But if $f(x) = \sum_{i=0}^{n} q_i x^i$, then $f(c^{-1}) = \sum_{i=0}^{n} q_i c^{-i} = c^{-n}(\sum_{i=0}^{n} q_i c^{n-i}) = c^{-n} \cdot b$ where $b \in Q$, therefore $Q[c^{-1}] = \{b/c^k \mid b \in Q, k \in \omega\}$.

□

For rings R, T, S and embeddings $\psi_1 \colon R \to T$ and $\psi_2 \colon R \to S$, we say $T \cong S$ *over* R with isomorphism φ, if φ is an isomorphism between T and S such that $\varphi \circ \psi_1 = \psi_2$. In particular, $R < T$ and $R < S$ is a special case of this definition, given by $\varphi_{\restriction R} = id_R$.

Proposition 2.39. Let P be a ring, and let $b \in P$ be non-zero. Let $Q < P$ be a ring. The following are equivalent:

1. $Q_b \cong P$ over Q,
2. b is a unit of P and $P = Q[b^{-1}]$.

Proof. Recall $Q_b = Q \times I/\sim$ where I is the multiplicative subset of Q generated by b and $\langle q, b^k\rangle \sim \langle q', b^{k'}\rangle$ if $q \cdot b^{k'} = q' \cdot b^k$. The embedding of Q into Q_b is defined by $q \mapsto \langle q, 1\rangle$ and the operations on Q_b are given by: $\langle q, b^k\rangle +_{Q_b} \langle q', b^{k'}\rangle = \langle qb^{k'} + q'b^k, b^k b^{k'}\rangle$ and $\langle q, b^k\rangle \cdot_{Q_b} \langle q', b^{k'}\rangle = \langle qq', b^k b^{k'}\rangle$.

This is an instance in which we identify Q with its image under the canonical embedding into Q_b.

1. $\Rightarrow$ 2.

Let φ be an isomorphism between Q_b and P. Note that $\varphi_{\restriction Q} = id_Q$

Since b is a unit of Q_b, let $c = \langle 1, b\rangle \in Q_b$ such that $bc = 1$ in Q_b. Then, $b\varphi(c) = \varphi(b)\varphi(c) = \varphi(bc) = 1$ in P, so b is a unit of P.

We need to show $Q[b^{-1}] \subseteq P$ and $P \subseteq Q[b^{-1}]$. The first inclusion is by definition.

Let $p \in P$, we have that $\varphi^{-1}(p) \in Q_b$ and so it is of the form $[\langle c, b^k\rangle]$, so $b^k\varphi^{-1}(p) = c \in Q$. Since $\varphi_{\restriction Q} = id_Q$, we obtain $b^k p \in Q$, which means $p \in Q[b^{-1}]$.

2. $\Rightarrow$ 1.

By Proposition 2.38, $Q[b^{-1}] = \{c/b^k \mid c \in Q, k \in \omega\}$.

Define a map $\varphi\colon P \to Q_b$ by $\varphi(p) = [\langle c, b^k\rangle]$ where $p = c/b^k$. Note that if $\langle c', b^{k'}\rangle \in [\langle c, b^k\rangle]$, then $p = c'/b^{k'}$, since $p \cdot b^k = c$ and $c' \cdot b^k = c \cdot b^{k'}$ so we have $c' \cdot b^k = p \cdot b^k \cdot b^{k'}$ which implies $c' = p \cdot b^{k'}$ and so $p = c'/b^{k'}$.

Bijectivity follows by definition of φ, we check additivity and multiplicativity:

$\varphi(c/b^k + c'/b^{k'}) = \varphi((cb^{k'} + c'b^k)/b^k b^{k'}) = [\langle c, b^k\rangle + \langle c', b^{k'}\rangle] = [\langle cb^{k'} + c'b^k, b^k b^{k'}\rangle$, while $\varphi(c/b^k) + \varphi(c'/b^{k'}) = [\langle c, b^k\rangle] + [\langle c', b^{k'}\rangle] = [\langle cb^{k'} + c'b^k, b^k b^{k'}\rangle]$, and $\varphi(c/b^k \cdot c'/b^{k'}) = \varphi(cc'/b^k b^{k'}) = [\langle cc', b^k b^{k'}\rangle]$, while $\varphi(c/b^k) + \varphi(c'/b^{k'}) = [\langle c, b^k\rangle] + [\langle c', b^{k'}\rangle] = [\langle cc', b^k b^{k'}\rangle]$.

This shows φ is an isomorphism. It is an isomorphism over Q since elements of Q are mapped to elements of Q_b by the canonical embedding ψ_1, to elements of P by the inclusion map ψ_2, and $\varphi \circ \psi_2 = \psi_1$, because $\varphi(\psi_2(q)) = \varphi(q) = [\langle q, 1\rangle] = \psi_1(q)$.

□

Proposition 2.40. If $R < Q$ are rings and $I, J \subset Q$, then $R[I][J] = R[I \cup J]$.

Proof. Let $I = \{i_1, i_2 \cdots i_k\}$ and $J = \{j_1, j_2 \cdots j_t\}$.

We need to show $R[I][J] \subseteq R[I \cup J]$ and $R[I \cup J] \subseteq R[I][J]$.

Let $r \in R[I][J]$. Then $r = f(\bar{j})$, with $f(\bar{x}) = \sum_{\zeta} r_\zeta \bar{x}^\zeta$, where each $r_\zeta \in R[I]$, so $r_\zeta = g_\zeta(\bar{i}) = \sum_{\iota} r_{\zeta,\iota} \bar{i}^\iota$, with $r_{\zeta,\iota} \in R$. Then we define $h \in R[I \cup J]$ as $h(\bar{x}, \bar{y}) = \sum_{\zeta} \sum_{\iota} r_{\zeta,\iota} \bar{x}^\zeta \bar{y}^\iota$, and we can see that $h(\bar{j}, \bar{i}) = f(\bar{j})$. Hence, $r \in R[I \cup J]$.

For the other inclusion, suppose without loss of generality that I and J are disjoint and let $r \in R[I \cup J]$ and the previous argument reverses. So $r = h(\bar{i}, \bar{j}) = \sum_{\zeta} \sum_{\iota} r_{\zeta,\iota} \bar{i}^\zeta \bar{j}^\iota$, with $r_{\zeta,\iota} \in R$, we can define the family of polynomials $g_\zeta \in R[I]$ by $g_\zeta(\bar{y}) = \sum_{\iota} r_{\zeta,\iota} \bar{y}^\iota$, and the polynomial $f(\bar{x}) = \sum_{\zeta} g_\zeta(\bar{i}) \bar{x}^\zeta$, and we can see that $f(\bar{j}) \in R[I][J]$ and $f(\bar{j}) = h(\bar{i}, \bar{j}) = r$.

□

We now define algebraic independence.

Definition 2.41. Let $Q < P$ and $a_1, a_2 \cdots a_k \in P$. The set $\{a_1, a_2 \cdots a_k\}$ is *algebraically independent* or *independent* over Q if for all non-zero $f \in Q[x_1, ..., x_k]$,

$f(a_1, ..., a_k) \neq 0$.

If the set $\{a\}$ is algebraically independent over Q we say the element a is *transcendental* over Q.

Note that in $R[x_1, x_2 \cdots x_k]$ the set $\{x_1, x_2 \cdots x_k\}$ is independent over R. The proof of this is immediate.

If $\varphi\colon R \to S$ and $\psi\colon P \to Q$ are maps between rings with $R < P$ and $S < Q$, we say that ψ *extends* φ if $\psi_{\restriction R} = \varphi$.

The following fact will be useful in many of our proofs.

Lemma 2.42. *Suppose we have rings $R < P = R[a_1, a_2 \cdots a_k]$ with $\{a_1, a_2 \cdots a_k\}$ independent over R and $\psi\colon R \to S$ a homomorphism. Let $R' = \psi[R] < S$ and let $\psi^*\colon R[x_1, x_2 \cdots x_k] \to R'[x_1, x_2 \cdots x_k]$ be defined by $\psi^*(f) = \sum_\iota \psi(q_\iota)\bar{x}^\iota$ for $f = \sum_\iota q_\iota \bar{x}^\iota$.*

Let $b_1, b_2 \cdots b_k \in S$. Then the map $f(\bar{a}) \mapsto \psi^*(f)(\bar{b})$ is the unique homomorphism $\bar{\psi}\colon P \to S$ such that $\bar{\psi}(a_i) = b_i$ for $i \leq k$ and $\bar{\psi}$ extends ψ.

Further, if ψ is injective and $\bar{b}$ is independent over R', then $\bar{\psi}$ is injective.

Also, the range of $\bar{\psi}$ is $R'[b_1, b_2 \cdots b_k]$.

Proof. We claim $\bar{\psi}$ is well-defined: suppose $f(\bar{a}) = g(\bar{a})$, then put $h(\bar{a}) = f(\bar{a}) - g(\bar{a})$ and if $f \neq g$ then h contradicts the independence of $\bar{a}$. So $f = g$, which means $g(\bar{a}) \mapsto \psi^*(f)(\bar{b})$ and the claim is proved.

We note that $\bar{\psi}$ is defined on all of P, by definition of P.

Let $f(\bar{x}) = \sum_\iota q_\iota \bar{x}^\iota$ and $g(\bar{x}) = \sum_\iota r_\iota \bar{x}^\iota$, for $q_\iota, r_\iota \in R$.

Check that $\bar{\psi}$ is a homomorphism. Note that $f(\bar{a}) + g(\bar{a}) = (f + g)(\bar{a})$ and $f(\bar{a}) \cdot g(\bar{a}) = (f \cdot g)(\bar{a})$. Check additivity: $\bar{\psi}(f(\bar{a}) + g(\bar{a})) = \bar{\psi}((f + g)(\bar{a})) = \psi^*(f + g)(\bar{b}) = \sum_\iota \psi(q_\iota + r_\iota)\bar{b}^\iota$ and since ψ is a homomorphism, this is $\psi^*(f)(\bar{b}) + \psi^*(g)(\bar{b})$. Multiplicativity is analogous.

Now $\bar{\psi}$ is injective if ψ is injective and $\bar{b}$ is independent over R'. To see this, let $f(\bar{a}) \mapsto \psi^*(f)(\bar{b})$ and $g(\bar{a}) \mapsto \psi^*(g)(\bar{b})$, and suppose $\psi^*(f)(\bar{b}) = \psi^*(g)(\bar{b})$. Since $\bar{b}$ is independent, we get $\psi^*(f) = \psi^*(g)$. By injectivity of ψ, this means $q_\iota = r_\iota$. Hence, $f = g$.

We claim $\bar{\psi}$ is onto $R'[\bar{b}]$. To see this, let $q = \sum_\iota \psi(q_\iota)\bar{b}^\iota$ be a member of $R'[\bar{b}]$ and we can see that $q = \bar{\psi}(\sum_\iota q_\iota \bar{a}^\iota)$.

Finally, we prove uniqueness of $\bar{\psi}$. Let $\phi\colon P \to S$ be a homomorphism such that ϕ extends ψ and $\phi(a_i) = b_i$. Let $c = f(\bar{a})$ be an element of P, written as above. Then $\phi(c) = \sum_\iota \phi(q_\iota \bar{a}^\iota)$, and since ϕ extends ψ this is the same as $\phi(c) = \sum_\iota \psi(q_\iota)\phi(\bar{a}^\iota)$ and since $\phi(a_i) = b_i$, we finally get $\phi(c) = \sum_\iota \psi(q_\iota)\bar{b}^\iota = \bar{\psi}(c)$.

□

If Q is a UFD and subring of R, $\bar{b} \in R$ is independent over Q, then the subring of R generated by Q and $\bar{b}$ is a UFD.

Proposition 2.43. Let Q be a UFD, $Q < R$ and $\{b_1, b_2 \cdots b_k\} \subset R$ be algebraically independent over Q. Then $Q[b_1, b_2 \cdots b_k]$ is a UFD.

Proof. By Lemma 2.35, $Q[x]$ is a UFD, and by iteration $Q[x_1, x_2 \cdots x_k]$ is a UFD. By Lemma 2.42, we have an isomorphism $\varphi\colon Q[b_1, b_2 \cdots b_k] \to Q[x_1, x_2 \cdots x_k]$ with $b_i \mapsto x_i$. By Proposition 2.14, $Q[b_1, b_2 \cdots b_k]$ is a UFD.

□

Proposition 2.44. Suppose we have rings $Q < P$ with $b_1, b_2 \cdots b_k \in P$. The following are equivalent:

1. $P \cong Q[x_1, x_2 \cdots x_k]$ over Q, with $b_i \mapsto x_i$ for $1 \leq i \leq k$;
2. $\{b_1, b_2 \cdots b_k\}$ is independent over Q and $P = Q[b_1, b_2 \cdots b_k]$.

Proof. 1. $\Rightarrow$ 2.

First we argue that $\{b_1, b_2 \cdots b_k\}$ is independent over Q. We note that $0_P \mapsto 0_{Q[x_1, x_2 \cdots x_k]}$. Suppose for a contradiction we have some non-zero $f \in Q[x_1, x_2 \cdots x_k]$ with $f(\bar{b}) =_P 0$. By isomorphism, $f(\bar{x}) =_{Q[\bar{x}]} 0$, contradicting injectivity. So $f(\bar{b}) \neq 0$ for any non-zero f.

Now apply Lemma 2.42 to Q, P, $\bar{x}$ and the embedding ψ of Q into P which is the restriction of the isomorphism from P to $Q[x_1, x_2 \cdots x_k]$, to obtain an isomorphism $\bar{\psi}$ between $Q[b_1, b_2 \cdots b_k]$ and P. Since $Q = \psi[Q]$, the range of $\bar{\psi}$ is $Q[b_1, b_2 \cdots b_k]$, hence $P = Q[b_1, b_2 \cdots b_k]$.

2. $\Rightarrow$ 1.

Apply Lemma 2.42 to Q, P, $Q[b_1, b_2 \cdots b_k]$, $\{b_1, b_2 \cdots b_k\}$ and the embedding $\psi\colon Q \to P$ to obtain a homomorphism $\bar{\psi}\colon P \to Q[x_1, x_2 \cdots x_k]$ with

$b_i \mapsto x_i$. Then, $\bar{\psi}$ is one to one and onto $Q[x_1, x_2 \cdots x_k]$, so it is an isomorphism.

□

The following result states that if a is transcendental over R and $f(a)$ is irreducible, then $f(x)$ must be irreducible in $R[x]$.

Proposition 2.45. If $R < P$ are rings, $f \in R[x]$, $a \in P$ transcendental over R and $f(a)$ is irreducible in $R[a]$, then f is irreducible in $R[x]$.

Proof. By Proposition 2.44, $R[a] \cong R[x]$ with $a \mapsto x$. This means $f(a) \mapsto f(x)$ under this isomorphism. By Proposition 2.14, f is irreducible in $R[x]$.

□

We give an equivalent condition for the union of sets of elements to be independent over some ring.

Lemma 2.46. *If Q and R are rings, with $Q < R$ and $J, K \subset R$ with $J \cap K = \emptyset$, then $J \cup K$ is independent over Q if and only if J is independent over T and K is independent over $Q[J]$.*

Proof. Let $J = \{j_1, j_2 \cdots j_r\}$ and $K = \{k_1, k_2 \cdots k_t\}$.

Note that by Proposition 2.40, $Q[x_1, x_2 \cdots x_r][x_r, x_{r+1} \cdots x_t] = Q[x_1, x_2 \cdots x_{r+t}]$.

Suppose J is independent over Q and K is independent over $Q[J]$. We show $J \cup K$ is independent over Q.

For suppose $f(\bar{j}, \bar{k}) = 0$, with non-zero $f \in Q[x_1, x_2 \cdots x_{t+r}]$.

Write f as $f(\bar{x}, \bar{y}) = \sum_{\iota} f_\iota(\bar{x})\bar{y}^\iota$, where $\bar{x} = x_1, x_2 \cdots x_r$, $\bar{y} = y_1, y_2 \cdots y_t$ and $f_\iota \in Q[x_1, x_2 \cdots x_r]$.

Note that since $f \neq 0$, some $f_\iota(\bar{x})$ must be non-zero.

However, since $f(\bar{j}, \bar{k}) = 0$ and since K is independent over $Q[J]$, it follows that each $f_\iota(\bar{j})$ must be zero, so there is a non-zero polynomial f over $Q[x_1, x_2 \cdots x_r]$ with $f(\bar{j}) = 0$. Since J is independent over Q, this produces a contradiction.

Conversely, suppose $J \cup K$ is independent over Q. That J is independent over Q is almost immediate, since $J \subseteq J \cup K$ and from $f \in Q[x_1, x_2 \cdots x_r]$ we can define $f^* \in Q[x_1, x_2 \cdots x_{r+t}]$ with zero-coefficients for $x_{r+1}, x_{r+2} \cdots x_{r+t}$, so $f^* = f$. So if J is not independent over Q, neither can $J \cup K$ be.

We now show K is independent over $Q[J]$. Let $g \in (Q[J])[\bar{y}]$, write g as $g(\bar{y}) = \sum_{\iota} g_\iota(\bar{j})y^\iota$ where as before $\bar{x} = x_1, x_2 \cdots x_r$, $\bar{y} = y_1, y_2 \cdots y_t$, and each $g_\iota \in Q[x_1, x_2 \cdots x_r]$. But then we can define g^* over Q as $g^*(\bar{x}, \bar{y}) = \sum_{\iota} g_\iota(\bar{x})y^\iota$, and we can see that if $g(\bar{k}) = 0$, then $g^*(\bar{j}, \bar{k}) = 0$, against the independence of $J \cup K$.

□

Lemma 2.47 and Remarks 2.48, 2.49 and 2.50 establish properties of elements in independent generating sets.

If an element is transcendental over a ring, then all its associates are also transcendental.

Lemma 2.47. *If $Q < R$ are rings, $a \in R$ is transcendental over Q and $a \cdot_R u = b$ for some unit u of R, then b is transcendental over Q.*

Proof. Suppose b is not transcendental over Q. So there is $f \in Q[x]$, $f \neq 0$ and $f(x) = \sum_{i=0}^{n} q_i x^i$, such that $f(b) = 0$.

Define $h \in Q[x]$ by $h(x) = \sum_{i=0}^{n} q_i u^{-i} x^i$, We claim $h \neq 0$. Otherwise, if $q_i u^{-i} = 0$ for all $0 \leq i \leq n$, since we know $u \neq 0$ it must be that $q_i = 0$ for all i, but this is impossible since $f \neq 0$.

Then, $h(a) = \sum_{i=0}^{n} q_i u^i a^i = q_0 + q_1 b + q_2 b^2 + \cdots + q_n b^n = f(b) = 0$, therefore a is not transcendental over Q.

□

No transcendental elements of a generating set can be units in the generated ring.

Remark 2.48. If $Q < R$ are rings and $Q[a_1, a_2 \cdots a_k] < R$ where the set $\{a_1, a_2 \cdots a_k\}$ is independent over Q, then no a_i with $1 \leq i \leq k$ is invertible in $Q[a_1, a_2 \cdots a_k]$.

Proof. Suppose $b \cdot a_i = 1_Q$.

Now suppose $b \in Q[a_1, a_2 \cdots a_k]$, so $g(a_1, a_2 \cdots a_k) = b$, for some $g \in Q[x_1, x_2 \cdots x_k]$. Define $f \in Q[x_1, x_2 \cdots x_k]$ as $f(x_1, x_2 \cdots x_k) = x_i \cdot g(x_1, x_2 \cdots x_k) - 1$ and note that $f \neq 0$, and so we have $f(a_1, a_2 \cdots a_k) = a_i b - 1 = 0$. In this case, $\{a_1, a_2 \cdots a_k\}$ would not be independent over Q.

□

No elements of an independent generating set associate or divide any elements of the base ring or other elements in the set.

Remark 2.49. If $Q < R$ are rings and $Q[a_1, a_2 \cdots a_k] < R$ where the set $\{a_1, a_2 \cdots a_k\}$ is independent over Q, then no a_i with $1 \leq i \leq k$ divides or associates with any element of $Q \cup \{a_1, a_2 \cdots a_k\} \setminus \{a_i\}$.

Proof. Suppose $b = a_i \cdot c$, where $c = g(a_1, a_2 \cdots a_k)$ for $g \in Q[x_1, x_2 \cdots x_k]$.

Now suppose $b \in \{a_1, a_2 \cdots a_k\} \setminus \{a_i\}$, so $b = a_j$. Define $f \in Q[x_1, x_2 \cdots x_k]$ as $f(x_1, x_2 \cdots x_k) = x_i g(x_1, x_2 \cdots x_k) - x_j$ and note that $f \neq 0$ since $i \neq j$, and so we have $f(a_1, a_2 \cdots a_k) = a_i c - b = 0$.

If $b \in Q$, define $f \in Q[x_1, x_2 \cdots x_k]$ similarly as $f(x_1, x_2 \cdots x_k) = x_i g(x_1, x_2 \cdots x_k) - b$, which again gives $f(a_1, a_2 \cdots a_k) = a_i c - b = 0$.

In either case, $\{a_1, a_2 \cdots a_k\}$ would not be independent over Q.

□

All elements of an independent generating set are irreducible in the generated ring.

Remark 2.50. If $Q < R$ are rings and $Q[a_1, a_2 \cdots a_k] < R$ where the set $\{a_1, a_2 \cdots a_k\}$ is independent over Q, then every a_i with $1 \leq i \leq k$ is an irreducible of $Q[a_1, a_2 \cdots a_k]$.

Proof. By Proposition 2.44 $Q[a_1, a_2 \cdots a_k] \cong Q[x_1, x_2 \cdots x_k]$ over Q, with $a_i \mapsto x_i$ for $1 \leq i \leq k$. By Proposition 2.31, each such x_i is irreducible in $Q[x_1, x_2 \cdots x_k]$. By Proposition 2.14, each a_i is irreducible in $Q[a_1, a_2 \cdots a_k]$.

□

Given a polynomial f over some ring R containing "fractions", it will later be a useful trick to define a polynomial g over a subring of R that has no denominators. This is a convenient way of restricting the domain of the polynomials we deal with.

Lemma 2.51. *If Q and R are rings such that $Q < R$ and $b \in Q$ is a unit of R, then for all $f \in Q[b^{-1}][x_1, x_2 \cdots x_n]$ there exists $N \in \omega$ such that $b^N f \in Q[x_1, x_2 \cdots x_n]$.*

Proof. Let $f \in Q[b^{-1}][x_1, x_2 \cdots x_k]$, $f(\bar{x}) = \sum_{\iota} (q_\iota \bar{x}^\iota$ where each $q_\iota \in Q[b^{-1}]$.

For each ι, let $I_\iota = \min\{k \in \omega \mid q_\iota = c \cdot b^{-k}, c \in Q\}$. Let $N = \max\{I_\iota\}$. Then $b^N \cdot q_\iota \in Q$ for all ι, so $b^N f \in Q[x_1, x_2 \cdots x_n]$.

□

Lemma 2.52 gives the intersection of rings generated by different elements in terms of the intersection of the generating sets.

Lemma 2.52. *If P, Q, R, S are rings, with $P = R[b, b_1 \cdots b_k]$, $Q = R[b, b^{-1}]$ for $b, b_1 \cdots b_k \in S$ and b a unit of S, $P < S$ and $Q < S$ where $\{b, b_1 \cdots b_k\}$ is independent over R, then $P \cap Q = R[b]$.*

Proof. $R[b] \subseteq P \cap Q$ is immediate since $R[b] \subseteq R[b_1 \cdots b_k][b] = R[b, b_1 \cdots b_k]$ and $R[b] \subseteq R[b^{-1}][b] = R[[b, b^{-1}]]$.

To prove the other containment, suppose $c \in P \cap Q$, so $c \in P$ and $c \in Q$. Write $\bar{b} = b_1, b_2 \cdots b_k$ and $\bar{y} = y_1, y_2 \cdots y_k$. Since $c \in P$, $c = f(b, \bar{b})$, for some $f \in R[x, \bar{y}]$. Since $c \in Q$, using Proposition 2.38, $c = d/b^k$ where $d \in R[b]$ therefore $d = g(b)$, for some $g \in R[x]$.

Put $\bar{f}(x, \bar{y}) = x^k f(x, \bar{y})$ and let $h(x, \bar{y}) = \bar{f}(x, \bar{y}) - g(x)$ and we can see that $h \in R[x, \bar{y}]$ and $h(b, \bar{b}) = d - d = 0$.

If $h(x, \bar{y}) \neq 0$ then $\{b, \bar{b}\}$ is not independent over R. So it must be that $h(x, \bar{y}) = 0$, which means $g(x) = \bar{f}(x, \bar{y})$ so $\bar{f} \in R[x]$ which means $f \in R[x]$ but this implies $c \in R[b]$, as required.

□

This concludes our exposition of the elements of Abstract Algebra we will be using in our proofs. The next Chapter is concerned with Computability and Reverse Mathematics, and also with a few results of Effective Algebra, building on the material presented here.

Chapter 3

Reverse Mathematics and Logic

In this chapter we set out the logic machinery we will be employing in our proofs, while also proving relevant results concerning Effective Algebra.

We now present briefly the fundamental notions of Computability and the framework of Reverse Mathematics.

A set $S \subseteq \omega$ will often be equated with its characteristic function. If $\sigma = \langle s_0, s_1 \cdots s_{k-1} \rangle$, we will write $\sigma(i)$ for the element s_i and $|\sigma|$ for k. If $i \geq k$, we leave the function $\sigma(i)$ undefined. Recall that $S^{<\omega}$ denotes the collection of finite tuples on S.

We will make use of strings of natural numbers to index elements of some particular ring. We will work in Baire space ${}^{\omega}\omega$ of sequences, or strings, of natural numbers. If σ and τ are strings, we use $\sigma^\frown\tau$ to denote appending τ to the end of σ, to form a third string. We denote by $\sigma \upharpoonright n$ the initial segment of σ of length n. A *tree* is a collection T of strings $\sigma \in \omega^{<\omega}$ such that T is closed under initial segments, i.e. if $\sigma \in T$ then any initial segment of σ is in T. The empty string is represented by λ. The relation $\preceq$ on a collection of strings T is defined by $\sigma \preceq \tau$ if σ is an initial segment of τ. We write $\sigma \prec \tau$ if $\sigma \preceq \tau$ and $\sigma \neq \tau$. The relations $\succeq$ and $\succ$ are the inverses of relations $\preceq$ and $\prec$. If $\sigma \preceq \tau$ or $\sigma \succeq \tau$, the strings are said to be *comparable*. Otherwise we call them *incomparable*, written $\sigma \mid \tau$. For two strings σ and τ, we denote by $\sigma \cap \tau$ their longest common initial segment. An *infinite path* on a tree $T \subseteq \omega^{<\omega}$ is a function $f : \omega \to \omega$ such that for all n, $f \upharpoonright n$ is in T. We say τ is a *child* of σ in T if both strings are in T and $\tau = \sigma^\frown s$ for some $s \in \omega$. Write $\sigma = \tau^-$. Intuitively, a string τ will later be called *terminal* in T

if it is not the initial segment of an infinite path. This nomenclature is not standard, as a string is usually called terminal in the literature if it has no descendants. We will make this notion precise in Chapter 4, in such a way as to be definable within a certain axiomatic framework. A tree T is *finitely branching* if any string in T has finitely many children. T is *binary branching* if elements of T have at most two children.

3.1 Notions from Computability Theory

For the primitive notions of Computability we follow Soare in [27].

Computability Theory is the study of the effective content of Mathematics, developing the informal concept of an algorithm, or computation, into a more formal framework consisting of computable functions and the structures they act upon. These functions are rigorously defined on the set of natural numbers $\omega = \{0, 1, 2, 3 \cdots\}$. More complicated structures can be embedded into ω using the technique of Gödel Numbering.

A partial function $\varphi \colon \omega^k \to \omega$ is a function $\varphi \colon D \to \omega$, where $D \subseteq \omega^k$. We denote the domain of φ by dom_φ.

A *Turing Machine* is an abstract model of computation that formalizes the notion of algorithm. Turing Machines compute partial computable functions.

A set $A \subseteq \omega$ is c.e. if it is the empty set or the range of a total computable function. Hence, a set is c.e. if it can be listed (or enumerated) effectively. A set is *computable* if it and its complement are c.e.

Assuming these details, Turing Machines can be constructed to compute most of the common functions of ordinary Mathematics. We equate the informal concept of effective/computable with the formally defined notion of Turing Computable. This idea is a version of the well-known Church's Thesis.

There exists a *Universal Turing Machine*. This provides us with an enumeration of the partial computable functions $\varphi_0, \varphi_1, \varphi_2 \cdots$ and an enumeration of the c.e. sets $W_0, W_1, W_2 \cdots$, where $W_i = dom_{\varphi_i}$.

The most natural c.e. set is $\emptyset' = \{e \mid \varphi_e(e) \downarrow\}$, known as the Halting Problem. This set is not computable. We denote by $\emptyset'_s$ the result of enumerating $\emptyset'$ for s steps of some enumeration.

In general, theorems could claim the existence of (non-computable) objects given other (non-computable) objects. Such a theorem claiming the existence of a particular object (output) given the existence of some other object (input) will be said to hold *uniformly* if there exists an effective way to pass from indices for the inputs to indices for the outputs. If such a proposition claims that for every computable function g and number b there is a computable function h and number d such that some property holds, then to say that the proposition is uniform is to say that there is a computable function f such that for all a and b, if φ_a is total then $f(a,b) = \langle c, d\rangle$, φ_c is total and the pair $\langle \varphi_c, d\rangle$ satisfies the conclusion of the proposition given the input $\langle \varphi_a, b\rangle$.

We will often say that A computes B if given access to a finite fragment of the characteristic sequence of A, we can decide membership for B.

We code sequences by elements of ω in a way which makes the basic relations and operations on strings (such as $\sigma \preceq \tau$ and $\langle \sigma, \tau\rangle \mapsto \sigma \cap \tau$) computable.

For two sets $A, B \subseteq \omega$, their join is defined as:

$$A \oplus B = \{2a \mid a \in A\} \cup \{2b+1 \mid b \in B\}.$$

The join $A \oplus B$ is the least upper bound of the Turing degrees of A and B.

3.2 Reverse Mathematics

Reverse Mathematics is carried out using the language, $\mathcal{L}_2$, of Second Order Arithmetic, $\mathcal{Z}_2$. It is the study of theories weaker than $\mathcal{Z}_2$. $\mathcal{L}_2$ is a two sorted first order language, which has two types of variables: number variables, which are denoted by lower-case letters, and set variables, which are denoted by upper-case letters. $\mathcal{L}_2$ also has two types of quantifiers, $\exists x$, $\forall x$ and $\exists X$, $\forall X$.

The axioms for $\mathcal{Z}_2$ come in three categories: axioms specifying the properties of $+, \cdot, 0, 1, <, \in$, to which we add the induction axiom for sets:

$$((0 \in X \wedge \forall n(n \in X \to n+1 \in X)) \to \forall n(n \in X))$$

and a simplified version of the comprehension scheme for forming sets:

$$\exists X \forall n (n \in X \leftrightarrow \phi(n)).$$

The Arithmetical Hierarchy is ubiquitous in Mathematical Logic and we define it here, for formulas of $\mathcal{L}_2$.

Definition 3.1 (Arithmetical Hierarchy)**.** A formula ψ is Σ_0^0 and Π_0^0 if it is logically equivalent to a first order formula with only bounded quantifiers.

A formula is classified as Σ_{n+1}^0 (or Σ_{n+1}) if it is logically equivalent to a formula of the form:

$$\exists n_1 \exists n_2 \cdots \exists n_k \psi,$$

where ψ is a Π_n^0 formula.

A formula is classified as Π_{n+1}^0 (or Π_{n+1}) if it is logically equivalent to a formula of the form:

$$\forall n_1 \forall n_2 \cdots \forall n_k \psi,$$

where ψ is a Σ_n^0 formula.

Note that a formula of $\mathcal{L}_2$ is said to be *arithmetical* if it contains no set quantifiers.

The base system will use a weak form of induction, restricted to Σ_1^0 formulas:

Definition 3.2 (Σ_1^0-Induction)**.** The Σ_1^0-Induction scheme is given by the following formula:

$$(\phi(0) \wedge \forall n(\phi(n) \rightarrow \phi(n+1)) \rightarrow \forall n \phi(n)),$$

where $\phi(n)$ is a Σ_1^0 formula that can contain set variables.

Various versions of the axiom for comprehension will also be used.

Definition 3.3 (Axiom Schema of Arithmetic Comprehension)**.** The axiom schema of arithmetic comprehension is as follows:

$$\forall w_1, ..., w_n \exists B \forall x \, (x \in B \Leftrightarrow \phi(x, w_1, \ldots, w_n)),$$

where the formula ϕ is in the Arithmetical Hierarchy. This essentially means:

"there exists a set B whose members are precisely those objects that satisfy the predicate ϕ."

Note that ϕ cannot contain set quantifiers, however set parameters are allowed.

Definition 3.4 (Recursive Comprehension)**.** Recursive comprehension is defined as follows:

$$\forall x(\phi(x) \leftrightarrow \psi(x)) \rightarrow \exists X \forall x(x \in X \leftrightarrow \phi(x)),$$

where ϕ is Σ_1^0 and ψ is Π_1^0 and X is not free on either ψ or ϕ.

A model for $\mathcal{L}_2$ is a first order structure

$$\mathcal{U} = (A, S_A, +_A, \cdot_A, 0_A, 1_A, <_A, \in_{S_A}),$$

where the number variables range over A and the set variables range over $S_A \subseteq \mathcal{P}(A)$ and the function, relation and constant symbols are interpreted as indicated in the context.

$\mathcal{Z}_2$ consists of basic arithmetic axioms, the comprehension axiom for every formula φ, and a second-order induction axiom. This theory is sometimes called "full second order arithmetic" to distinguish it from its subsystems, defined below.

The intended model for $\mathcal{Z}_2$ is $(\omega, \mathcal{P}(\omega), +, \cdot, 0, 1, <, \in)$, but we can also have non-standard models, if the number variables would range over a non-standard set or the set variables would range over a set smaller than the full powerset of A.

An ω-model M is an $\mathcal{L}_2$-model for which the first order part is standard, i.e. $A = \omega$. So M can be viewed as a collection of sets of natural numbers, representing the range of the set variables in $\mathcal{L}_2$.

3.3 Subsystems of $\mathcal{Z}_2$

The five subsystems of $\mathcal{Z}_2$ most frequently used in Reverse Mathematics are RCA_0, WKL_0, ACA_0, ATR_0 and $\Pi_1^1 CA_0$. The subscript 0 refers to the usage of restricted induction.

The first and weakest subsystem of $\mathcal{Z}_2$, RCA_0, is named because of the recursive comprehension axiom and it includes the arithmetic axioms, the recursive comprehension scheme and restricted induction. RCA_0 includes the semi-ring axioms while addition and multiplication satisfy their recursive definition. Σ^0_1 induction is allowed, while a classic result of [6] shows that Π^0_1 induction is also admissible. The unique smallest ω-model for RCA_0 is the collection REC of computable/recursive sets. The ω-models of RCA_0 are the collections of subsets of ω which are closed under join and relative computability.

This system corresponds roughly to constructive mathematics. If a statement is provable in RCA_0, its effective or computable version will always be true.

The second subsystem of $\mathcal{Z}_2$ is WKL_0 and is named after the Weak König's Lemma. This is the statement "every infinite binary branching tree has an infinite path". As the name suggests, WKL_0 is made up by adding Weak König's Lemma to the axioms of RCA_0. WKL_0 is strictly stronger than RCA_0 - we can see this because the effective version of the Weak König's Lemma is not true. One consequence of equivalences to WKL_0 is that the effective versions of the results fail to hold.

The third subsystem is dubbed ACA_0, for Arithmetic Comprehension Axiom, which comprises of RCA_0 plus the Σ^0_1 comprehension. This system can prove the Full König's Lemma and can define the Turing Jump of any set. ACA_0 allows us to form the set of natural numbers satisfying an arbitrary arithmetical formula, no matter how complex. In this framework, it is easy to prove the existence of the integers, the rationals, the reals (as Cauchy sequences of rationals), the complex numbers (as pairs of reals) and also show some of their properties.

It is then provable that RCA_0 and the restriction of the comprehension scheme to arithmetical formulas, which yield the arithmetical induction scheme, is equivalent to ACA_0. The unique smallest ω-model for ACA_0 is then the collection $ARITH$ of arithmetical sets. Among the ω-models of RCA_0, the ω-models for ACA_0 are characterized by the property of closure under Turing Jump.

The system ATR_0, short for arithmetic transfinite recursion, comprises of ACA_0, plus axioms which allow for the arithmetic comprehension to be

iterated transfinitely, along any well-order.

Given that a well-ordering is *an irreflexive linear ordering of a subset of the natural numbers having no infinite descending sequences*, the ATR_0 main axiom asserts that "if '$<$' is a well-ordering, then for any arithmetical formula $\phi(j, Y)$ there exists a set X such that for all j and n, $(j, n) \in X$ if and only if $\phi(j, \{(i, m)|m < n \wedge (i, m) \in X\})$".

It is a result of Friedman that ATR_0 is equivalent to the statement that any two well-orderings are comparable. In particular, it is also equivalent to the assertion that the Turing Jump can be iterated along any countable well ordering starting with any set.

The final and strongest system that is usually considered in Reverse Mathematics is $\Pi^1_1 CA_0$, which is strong enough to develop the basic structure theory of countable abelian groups. It consists of the system ATR_0 plus the axiom of Π^1_1 comprehension, which states that $\{x \in \omega|\phi(x)\}$ exists for any Π^1_1 formula $\phi(x)$. This system can prove the existence of Kleene's $\mathcal{O}$, which cannot be shown in ATR_0.

This concludes our exposition of the subsystems of $\mathcal{Z}_2$. For completeness, we have introduced all of the big five subsystems, however we will only refer to RCA_0 and ACA_0 in our proofs, using the first as a base system and proving an equivalence with the latter.

3.4 Computability and Algebra

Computability Theory operates with computable structures, so we define the computable counterpart of a ring.

Definition 3.5. A *computable ring* is a computable subset $R \subseteq \omega$, equipped with two computable binary operations $+$ and $\cdot$ on R, together with two elements $0, 1 \in R$, such that $(R, 0, 1, +, \cdot)$ is a ring.

The embedding of a ring into its associated ring of polynomials is computable with computable image. Furthermore, if the ring is computable, we can effectively compute an index for this embedding.

We state this in the following proposition concerning computability, noting that further details regarding numberings can be found in [26].

Proposition 3.6. If R is a computable ring, then $R[x_1, x_2 \cdots x_k]$ is computable and the embedding $\varphi : R \hookrightarrow R[x_1, x_2 \cdots x_k]$ is computable with computable image.

This is an occasion in which we need to make a distinction between R and its image under its embedding into $R[\bar{x}]$ and note that the map is not an identity.

Proof. $R[x]$ is defined as tuples over R; this can be the empty tuple or tuples in which the last element is non-zero; using a Gödel numbering these tuples can be coded by natural numbers. The operations on the resulting structure are computable, since the ring $R[x]$ is specified by effective rules for addition and multiplication, based on the operations of R. By iteration, $R[x_1, x_2 \cdots x_k]$ is also computable.

The embedding $\varphi\colon R \hookrightarrow R[x]$ is then defined as $q_0 \mapsto \langle q_0 \rangle$. Since the tuple $\langle q_0 \rangle$ is effectively recognizable by the condition $i < 1$, the map φ is computable with computable image.

By iteration, the embedding of R into $R[x_1, x_2 \cdots x_k]$ is computable with computable image.

□

We argue that Proposition 3.6 holds uniformly.

Remark 3.7. Proposition 3.6 is effective.

Proof. From indices for the computable ring R we can pass to indices for the ring $R[x_1, x_2 \cdots x_k]$. This is because $R[x_1, x_2 \cdots x_k]$ is effectively defined using elements of R, while its operations are based on the operations of R.

Also, from indices for the rings R and $R[x_1, x_2 \cdots x_k]$, we can pass to a computable index for φ, and an index for $\varphi[R]$.

□

The following remark notes that the operation of evaluating a polynomial of $R[x_1, x_2 \cdots x_k]$ within a computable ring R is a computable operation.

Remark 3.8. If $R < Q$ are computable rings, then the function $\langle f, \bar{a} \rangle \mapsto f(\bar{a})$ from $R[\bar{x}] \times Q^n \to Q$ is computable.

Proof. $f(\bar{a})$ is obtained effectively by uniformly replacing $\bar{a}$ for $\bar{x}$ in $f(\bar{x})$ and then carrying the multiplications and additions in Q. Since Q is computable, the process of obtaining $f(\bar{a})$ must be effective.

□

Remark 3.9. Let R be a computable integral domain and I a multiplicative c.e. subset of R. Let φ be the embedding of R into $I^{-1}R$. Then, there is a computable ring S, a computable embedding $\psi\colon R \to S$, and an isomorphism $\theta\colon I^{-1}R \to S$, such that $\psi = \theta \circ \varphi$.

Proof. Recall the relation $\sim$ on $R \times I$ is defined by $\langle r, b\rangle \sim \langle r', b'\rangle$ if $r \cdot b' = r' \cdot b$.

Let $b_1, b_2 \cdots$ be an enumeration of I where $b_k = b^k$.

Define a relation E on $R \times \omega$ by $\langle a, k\rangle E \langle a', k'\rangle$ if $\langle a, b_k\rangle \sim \langle a, b_{k'}\rangle$. Then E is a computable relation: to see if a pair $\langle a, k\rangle$ is in the relation we see the enumeration of I up to step k and checking whether two pairs are $\sim$-equivalent can be done effectively, since R is computable.

Consider the collection $(R \times \omega)/E$ and the map $\eta\colon R \times \omega \to R \times \omega$ that chooses a representative for each E-equivalence class and sends each element to its representative. From an enumeration $\langle a_1, k_1\rangle, \langle a_2, k_2\rangle \cdots$ of $R \times \omega$ we can effectively do this by letting $\eta(a_s, k_s) = \langle a_v, k_v\rangle$ where $v = \min\{t \leq s \mid \langle a_s, b_{k_s}\rangle \sim \langle a_t, b_{k_t}\rangle\}$. In virtue of this definition, η is computable with a computable image.

We let $S = \eta[R \times \omega]$.

Define $\theta\colon I^{-1}R \to S$ by $\theta([\langle r, b_k\rangle]) = \eta(r, k)$. Bijectivity of θ follows from the definition of η.

Define the operations on S by: $a +_S b = \theta(\theta^{-1}(a) +_{I^{-1}R} \theta^{-1}(b))$ and $a \cdot_S b = \theta(\theta^{-1}(a) \cdot_{I^{-1}R} \theta^{-1}(b))$ It follows that S is a ring since $I^{-1}R$ is a ring, and θ is an isomorphism.

We claim S is computable. For let $a, c \in S$, we can effectively find $r, s \in R$ and $k, l \in \omega$ such that $a = \langle r, k\rangle$ and $c = \langle s, l\rangle$. Using a search, we can effectively find $m \in \omega$ such that $b_m = b_k \cdot_R b_l$. Then $a \cdot_S c = \eta(r \cdot_R s, m)$ and $a +_S c = \eta(r \cdot_R b_l +_R s \cdot_R b_k, m)$.

It is straightforward that $\psi = \theta \circ \varphi$, since $\psi(r) = \eta(r, k)$ such that $b_k = 1_R$ and $\theta(\varphi(r)) = \theta([\langle r, 1_R\rangle]) = \eta(r, k)$. The fact that ψ is an embedding follows from the fact that both φ and θ are embeddings.

□

Remark 3.10. Proposition 3.9 is effective.

Proof. From an index for R as a computable ring, and a c.e. index for the set I, we can effectively compute an index for S as a computable ring, a computable index for ψ and a computable index for the set $\psi[R]$.

□

Recall that R_b is the localization of R by the multiplicative subset $I = \{b^k \mid k \in \omega, b \in R, b \neq 0_R\}$.

Remark 3.11. Let R be a computable integral domain, let $a \in R$ be nonzero, and suppose that the relation $\{\langle r, k\rangle \in R \times \omega \mid b^k \mid r\}$ is computable. Then there is a computable integral domain S and a computable embedding $\psi\colon R \to S$ with computable image, and an isomorphism $\theta\colon R_b \to S$ such that $\psi = \theta \circ \varphi$, where φ is the canonical embedding of R into R_b.

Proof. The construction of S is exactly as in the proof of Remark 3.9.

Under the assumption that the divisibility relation is computable, we have that the image of ψ is computable, since $\langle r, k\rangle \in S$ is in the range of ψ if and only if $b^k \mid_R r$.

□

Remark 3.12. Remark 3.11 is uniform.

Proof. Just as in the proof of Remark 3.10, with the added assumption that we have a computable index for the relation $\{\langle r, k\rangle \in R \times \omega \mid b^k \mid r\}$. With this added index we obtain a computable index for the set $\psi[R]$.

□

The following proposition will allow us to prove Corollary 3.21. Again, we need it to hold uniformly.

Proposition 3.13. If Q and P are computable rings with $P = Q[a]$ for $a \in P$ transcendental over Q, there is a computable embedding $\varphi\colon P \hookrightarrow Q[y, z]$, such that:

1. $\varphi(a) = y \cdot z$,
2. $\varphi[P]$ is computable,
3. $\varphi \restriction Q = id_Q$.

Proof. This is an instance in which we can assume $Q < Q[y,z]$ and the embedding of Q into $Q[y,z]$ is id_Q. Note that id_Q is a homomorphism.

Since $Q < P = Q[a]$ and a is transcendental over Q, we can apply Lemma 2.42 to Q, P and id_Q to obtain the unique homomorphism $\varphi\colon P \to Q[y,z]$ such that $f(a) \mapsto (f)(yz)$, that extends id_Q with $\varphi(a) = yz$. We claim yz is transcendental over Q, otherwise we have non-zero $f \in Q[x]$ with $f(yz) = 0$ from which we can construct non-zero $g \in Q[y,z]$ with $g(y,z) = f(yz) = 0$, but this is impossible.

We claim φ is the required embedding. By definition, $\varphi(a) = y \cdot z$.

We claim φ is computable. $Q[x]$ is computable. Fix an element $p \in P$. From an enumeration $f_1, f_2 \cdots$ of $Q[x]$, check if $f_i(a) = p$, and if so, map p to $f_i(y \cdot z)$.

Note that the image of φ is computable, since a polynomial $f \in Q[y,z]$ is in the image of Q if and only if $f(y,z) = \sum_{i,j=0}^{i=n,j=m} q_{i,j} y^i z^j$ with $q_{i,j} = 0$ when $i \neq j$. Also, $f \in \varphi[Q]$ if and only if $q_{i,j} = 0$ if $i > 0$ or $j > 0$. These conditions are recognizable, given the description of the polynomial f.

□

Remark 3.14. Proposition 3.13 is effective.

Proof. From computable indices for Q and P and the element a we can effectively compute indices for φ and for the set $\varphi[P]$.

□

If a computable ring Q is embedded into a computable ring S and S is infinitely bigger than Q and given superset R of Q that is infinitely bigger than Q, we can uniformly define a computable structure on R and a computable isomorphism between R and S.

Proposition 3.15. Given computable ring Q, a computable embedding $\psi\colon Q \hookrightarrow S$ with $\psi[Q]$ computable, where S is a computable ring and $|S \setminus \psi[Q]| = \omega$ and given computable set $R \supset Q$ with $|R \setminus Q| = \omega$, then there are functions $+_R\colon R^2 \to R$ and $\cdot_R\colon R^2 \to R$ such that $(R, +_R, \cdot_R, 0_Q, 1_Q)$ forms a computable ring with $Q < R$, and a computable isomorphism $\eta\colon S \to R$ such that $\eta \circ \psi = id_Q$.

Proof. We want to define η as a computable bijection $\eta\colon S \to R$, such that $\eta \circ \psi = id_Q$.

To see that such a function exists, let $s_0, s_1, s_2 \cdots \in S$ be an effective enumeration of S and $r_0, r_1, r_2 \cdots$ be an effective enumeration of $R \setminus Q$. Define η as follows

$$\eta(s_i) = \begin{cases} \psi^{-1}(s_i), & \text{if } s_i \in \psi[Q] \\ r_j \text{ such that } j = \min\{j \mid r_j \notin \eta[\{s_0, s_1 \cdots s_{i-1}\}]\}, & \text{otherwise} \end{cases}$$

Then $\eta_{\restriction \psi[Q]}$ is bijective due to the fact that ψ is an embedding, and $\eta_{\restriction S \setminus \psi[Q]}$ is surjective because we are mapping s_i to a minimum r_j and injective because r_j was not mapped before. In virtue of our definition, η is also computable and $\eta \circ \psi = id_Q$.

Define the computable ring structure on R by $s_1 +_R s_2 = \eta(\eta^{-1}(s_1) +_S \eta^{-1}(s_2))$ and $s_1 \cdot_R s_2 = \eta(\eta^{-1}(s_1) \cdot_S \eta^{-1}(s_2))$.

Because they are compositions of computable operations, these functions are computable and η becomes the required isomorphism.

□

Remark 3.16. Proposition 3.15 is effective.

Proof. Form computable indices for the rings Q and S, and computable indices for the sets R and $\psi[Q]$ we can effectively obtain the enumerations $s_0, s_1 \cdots$ and $r_0, r_1 \cdots$ and pass to a computable index for the ring R and a computable index for the map η.

□

If Q is a computable ring and there is a computable superset S of Q infinitely bigger than Q and an element a of S that is not in Q, we can uniformly put a computable structure on S such that the ring S is generated by Q and the element a.

Corollary 3.17. *If Q is a computable ring, S is a computable superset of Q with $|S \setminus Q|$ infinite, then there are functions $+_S\colon S^2 \to S$ and $\cdot_S\colon S^2 \to S$ such that $(S, +_S, \cdot_S, 0_Q, 1_Q)$ is a computable ring, Q is a subring of S, and there is some $a \in S$ such that $S = Q[a]$ and a is transcendental over Q.*

Proof. From Proposition 3.6 we know $Q[x]$ is computable, and we have a computable embedding with computable image $\varphi\colon Q \hookrightarrow Q[x]$.

Now, we get by Proposition 3.15 a computable structure $(S, +_S, \cdot_S, 0_Q, 1_Q)$ and an isomorphism $\eta\colon Q[x] \to S$. Let $a = \eta(x)$, we know $a \mapsto x$, i.e. a is transcendental over Q. By Proposition 2.44 a is transcendental over Q and $S = Q[a]$.

□

Remark 3.18. Corollary 3.17 is effective.

Proof. Follows from Remark 3.7, Remark 3.16 and Proposition 3.6.

□

The next Corollary is analogous to Corollary 3.17, and it uniformly defines a computable structure on S such that S is isomorphic to $Q[c^{-1}]$, for a non-unit non-zero $c \in Q$.

Corollary 3.19. *If Q is a computable integral domain and S is a computable set such that $Q \subset S$ and $|S \setminus Q|$ is infinite, and given some non-zero non-unit $c \in Q$ such that the relation $\{\langle r, k\rangle \in Q \times \omega \mid c^k \mid r\}$ is computable, then there are functions $+_S\colon S^2 \to S$ and $\cdot_S\colon S^2 \to S$ such that $(S, +_S, \cdot_S, 0_Q, 1_Q)$ forms a computable integral domain, with Q a subring of S, c a unit of S, and $S = Q[c^{-1}]$.*

Proof. Note that $Q_c = I^{-1}Q$, where $I = \{c^k \mid k \in \omega\}$, a c.e. set.

From Remark 3.9, we know there is a computable ring P, a computable embedding $\psi\colon Q \to P$ with computable image and an isomorphism $\theta\colon Q_c \to P$ which extends ψ. Note that we are considering Q as a subring of Q_c.

From Proposition 3.15, we obtain a computable structure on S and an isomorphism $\eta\colon P \to S$ such that $\eta \circ \psi = id_Q$.

We need to show that c is a unit of S and $S = Q[c^{-1}]$. This follows by Proposition 2.39 because $\eta \circ \theta$ is an isomorphism between Q_c and S, over Q.

□

Remark 3.20. Corollary 3.19 is effective.

Proof. Follows from Remark 3.16, Remark 3.10, Remark 3.18 and Proposition 3.6.

□

In Chapter 4 we will need a ring homomorphism that maps a particular element of its domain to the product of two elements of its range. We will start with a given ring Q and use this result for defining a ring R containing Q in which a particular element of Q is the product of two elements of R. The following Corollary will allow that.

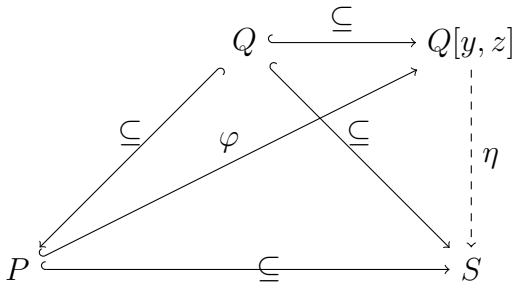
Corollary 3.21. *If Q and P are computable rings such that $Q < P$ and $P = Q[a]$ with a transcendental over Q, and S is a computable set such that $P \subset S$ and $S \setminus P$ is infinite, then there are functions $+_S, \cdot_S \colon S^2 \to S$ such that $(S, +_S, \cdot_S, 0_Q, 1_Q)$ is a computable ring, P is a subring of S and elements $b, c \in S$ transcendental over Q, such that:*

1. *$Q[b, c] = S$, and*
2. *$b \cdot_S c = a$.*

Proof. From Proposition 3.13 we obtain a computable embedding $\varphi \colon P \to Q[y, z]$ such that $\varphi(a) = y \cdot z$.

Apply Proposition 3.15 to P, S and $Q[y, z]$ to put a computable structure on S and obtain an isomorphism $\eta \colon Q[y, z] \to S$ such that $\eta \circ \varphi = id_P$.

Put $b = \eta(y)$ and $c = \eta(z)$ to obtain $b \cdot_S c = \eta(y) \cdot_S \eta(z) = \eta(y \cdot_{Q[y,z]} z))$ $= \eta(\varphi(a)) = id_P(a) = a$, and the following diagram:



From Definition 2.41, $\{y, z\}$ is independent in $Q[y, z]$ over Q, so $\{b, c\}$ is independent in S over Q. For if there is $f \in Q[y, z]$ such that $f(b, c) = 0$, by isomorphism $f(y, z) = 0$. This shows $S = Q[b, c]$ with $\{b, c\}$ independent over Q.

□

Remark 3.22. Corollary 3.21 is effective.

Proof. Follows from Remark 3.16, Remark 3.14 and Remark 3.7, and the fact that b and c can be found effectively, since the function η from Proposition 3.15 can be found effectively.

□

The following Proposition concerns computability of a generated ring, under the assumptions that the generating set is finite and the base ring is computable.

Proposition 3.23. If $Q < R$ are computable rings with $R = Q[J]$ for some finite $J \subseteq R$ independent over Q, and given $I \subset J$, then the ring $Q[I]$ is computable.

Proof. Let $I = \{a_1, a_2 \cdots a_k\}$ and $J = \{a_1, a_2 \cdots a_r\}$ with $r > k$. Then $Q[I] = \{f(a_1, a_2 \cdots a_k) \mid f \in Q[x_1, x_2 \cdots x_k]\}$ and $R = Q[J] = \{g(a_1, a_2 \cdots a_r) \mid g \in Q[x_1, x_2 \cdots x_r]\}$.

Let $\bar{x} = x_1, x_2 \cdots x_k$ and $\bar{y} = a_k, a_{k+1} \cdots a_r$. Note that $Q[\bar{x}]$ is a computable subset of $Q[\bar{x}, \bar{y}]$.

By Proposition 2.44, fix a computable bijection $\psi \colon R \to Q[\bar{x}, \bar{y}]$. Then $a \in Q[I]$ if and only if $\psi(a) \in Q[\bar{x}]$, so $Q[I]$ is computable.

□

Remark 3.24. Proposition 3.23 is uniform.

Proof. From computable indices for the rings Q and J and for the sets I and J, we can pass to computable indices for the ring $Q[I]$.

□

Finally, Lemma 3.25 gives a sufficient condition for the computability of a ring generated by two specific elements.

Lemma 3.25. *If P, Q, R are computable rings, $Q < R < P$ and b invertible in P, with $R = Q[b, b_1, b_2 \cdots b_k]$ where the presented variables are independent over Q, and $P = R[b^{-1}]$, then the ring $Q[b, b^{-1}]$ is computable.*

Proof. By Proposition 3.23 applied to R, $\{b, b_1, b_2 \cdots b_k\}$ and $\{b\}$, $Q[b]$ is computable.

Proposition 2.38 shows $P = \{c/b^k \mid c \in R, k \in \omega\}$.

Due to Remark 2.40, $Q[b, b^{-1}] = (Q[b])[b^{-1}]$. Since $Q[b] \subset P$, Proposition 2.38 also shows that $Q[b, b^{-1}] = \{c/b^k \mid c \in Q[b], k \in \omega\}$.

Given $d \in P$, we claim we can effectively find $c \in R$ and $k \in \omega$ such that $d = c/b^k$. Starting from enumerations $c_1, c_2 \cdots \in R$ and $1, b, b^2, b^3 \cdots$, we

can consider all pairs c, b^k. We must eventually find such a pair and halt, because $d \in P$.

Now, if $d = c_1/b^{k_1} = c_2/b^{k_2}$ with $c_1 \in Q[b]$ and $c_2 \in R$, then $c_2 = c_1 b^{k_2}/b^{k_1} \in Q[b, b^{-1}]$, so by Lemma 2.52 $c_2 \in Q[b]$.

Finally, we note that the condition $c \in Q[b]$ is decidable. This shows $Q[b, b^{-1}]$ is computable, for we can perform a search for $d = c/b^k \in P$ and decide whether $c \in Q[b]$.

□

Remark 3.26. Lemma 3.25 is uniform.

Proof. From computable indices for the rings P, Q, R and the element b we can pass to computable indices for the ring $Q[b, b^{-1}]$.

□

In the next Chapter we will define a particular sequence of rings. The first ring in the sequence will be isomorphic to the field of rationals $\mathbb{Q}$, hence we need a proposition that establishes an isomorphism between the rationals and an arbitrary countably infinite set.

Proposition 3.27. If Q is a computable set with $|Q| = \omega$, there are computable functions $+_Q \colon Q^2 \to Q$ and $\cdot_Q \colon Q^2 \to Q$ and elements $0_Q, 1_Q \in Q$ such that $(Q, +_Q, \cdot_Q, 0_Q, 1_Q)$ forms a ring and $Q \cong \mathbb{Q}$.

Proof. Let R be a computable copy of the integers, such that the set Q contains R and $|Q \setminus R| = \omega$. This can be achieved, for example, by coding the integers into the even numbers and letting $Q = \omega$.

Now let $I = R \setminus \{0_R\}$. Note that I is a c.e. subset of R. By Remark 3.9, there is a computable ring S, a computable embedding $\psi \colon R \to S$ with computable image, and an isomorphism $\eta \colon I^{-1}R \to S$ that extends ψ.

Note that $I^{-1}R \cong \mathbb{Q}$, so $S \cong \mathbb{Q}$.

By Proposition 3.15, there is a computable structure on Q such that $R < Q$ and there exists isomorphism $\theta \colon S \to Q$ with $\theta \circ \psi = id_R$.

This proves there exists an isomorphism between Q and $\mathbb{Q}$.

□

This is the end of Chapter 3. The final Chapter is an exposition of our main results.

Chapter 4

Equivalent characterizations of UFDs

In this chapter we present our results, which deal with the proof-theoretic strength of Theorems 1.2 and 1.3. We will work in the base system RCA_0.

4.1 The theorems

We will make use of the following two lemmas in the proof of Theorem 1.3.

Recall that $C \sim C'$ means that there is a bijection $f\colon C \to C'$ such that $p \sim f(p)$ for all $p \in C$. Let $\prod C = \prod_{c \in C} c$.

Lemma 4.1 (RCA_0)**.** *Let R be an integral domain. Let C and C' be multisets of primes of R. If $C \sim C'$ then $\prod C \sim \prod C'$.*

Proof. Let $C = [p_1, p_2 \cdots p_m]$, so $C' = [q_1, q_2 \cdots q_m]$ and there is injective $f\colon \{1, 2 \cdots m\} \to \{1, 2 \cdots m\}$ such that $p_k \sim q_{f(k)}$ for all $k \in \{1, 2 \cdots m\}$.

For $k \leq m$ let $C_k = [p_1, p_2 \cdots p_k]$ and $C'_k = [q_{f(1)}, q_{f(2)} \cdots q_{f(k)}]$.

We prove the Σ_1 statement $\prod C_k \sim \prod C'_k$ using induction on k. Take the base case as $k = 0$ and we observe that $C_k = C'_k = \emptyset$, so $\prod C_k = 1_R = \prod C'_k$. Assume the statement holds for $k < m$, so there is $u \in R^\times$ such that $u \prod C_k = \prod C'_k$. By assumption, there is $v \in R^\times$ such that $vp_{k+1} = q_{f(k+1)}$. Then,

$$(uv) \prod C_{k+1} = u \prod C_k \cdot vp_{k+1} = \prod C'_k q_{f(k+1)} = \prod C'_{k+1},$$

as required.

□

Lemma 4.2 (RCA_0)**.** *Let R be an integral domain. Let C be a multiset of elements of R, and let $p \in R$ be prime. If $p \mid \prod C$, then there is some $a \in C$ such that $p \mid a$.*

Proof. Let $C = [a_1, a_2 \cdots a_m]$.

We use induction on $k \leq m$ to show that there is some $j \leq k$ such that $p \mid a_j$, or $p \mid \prod[a_{k+1}, a_{k+2} \cdots a_m]$. For the base step $k = 0$, this is the assumption $p \mid \prod C$. For the induction step, assume the statement holds for k. If there is some $j \leq k$ such that $p \mid a_j$, then certainly the statement holds for $k+1$. If not, since p is prime and by induction

$$p \mid \prod[a_{k+1}, a_{k+2} \cdots a_m] = a_{k+1} \prod[a_{k+2} \cdots a_m],$$

either $p \mid a_{k+1}$ or $p \mid [a_{k+2} \cdots a_m]$, so the statement holds for $k+1$. So the statement holds for m, which means $p \mid a_j$ for some $j \leq m$ or $p \mid \prod \emptyset = 1_R$, which is impossible since p is a non-unit.

□

The first theorem we will be concerned with states that if every irreducible is prime in an integral domain, then every element has at most one factorization into irreducibles. This result is provable in RCA_0.

Theorem 1.3 (RCA_0)**.** *If an integral domain is AP, then it is an U-UFD.*

The proof is essentially a repeat of the proof of Proposition 2.12. We repeat it due to the fact that we are confined to the base system RCA_0.

Proof. Let R be an AP domain. Let B and B' be multisets of irreducibles of R, and suppose $\prod B \sim \prod B'$. Write $B = [p_1, p_2 \cdots p_m]$ and $B' = [q_1, q_2 \cdots q_n]$.

By Σ_1 induction on $k \leq n$ we prove the formula $\varphi(k)$: "there is injective $f \colon \{1, 2 \cdots k\} \to \{1, 2 \cdots m\}$ such that for all $i \leq k$, $p_i \sim q_{f(i)}$. For the base case $k = 0$, the empty function witnesses the formula holds. For the inductive case, suppose f does the job on $\{1, 2 \cdots k\}$. Let $C = [p_1, p_2 \cdots p_k]$, $C' = [q_{f(1)}, q_{f(2)} \cdots q_{f(k)}]$, and let $b = \prod B$, $b' = \prod B'$, $c = \prod C$ and $c' = \prod C'$. Let $d = \prod(B \setminus B')$ and $d' = \prod(C \setminus C')$.

By Lemma 4.1, $c \sim c'$. From the assumption $b \sim b'$ we conclude $d \sim d'$. In particular, $p_{k+1} \mid d'$. By Lemma 4.2, there is $q \in C \setminus C'$ such

that $p \mid q$. By irreducibility of q, $p \sim q$. Let $i \leq m$ such that $q = q_i$, define $g\colon \{1, 2 \cdots k+1\} \to \{1, 2 \cdots m\}$ by letting $g(j) = f(j)$ for $j \leq k$ and $g(k+1) = i$.

□

The second theorem concerns the logical connection between well-foundedness of divisibility and atomicity. The main contribution of our present work is to prove the equivalence of this result to ACA_0.

Theorem 1.2 (ACA_0)**.** *If an integral domain satisfies the ACCP, then it is Atomic.*

Proof. Let R be a computable non-Atomic integral domain. There are two cases to consider.

Case 1: there is some $a \in R$ with no irreducible factor. Recursively define a sequence $\langle a_i \rangle_{i \in \omega}$ with $a_0 = a$ and a_{n+1} some proper factor of a_n. By induction, a_n has no irreducible factor, so is reducible itself. $\emptyset'$ can identify such a_{n+1}, so the sequence $\langle a_i \rangle_{i \in \omega}$ is computable from $\emptyset'$. Since this is an infinite descending chain in divisibility, it is a counter-example to ACCP.

Case 2: every $b \in R$ has an irreducible factor, but some $a \in R$ is not the product of irreducible elements. Recursively define a sequence $\langle a_i \rangle_{i \in \omega}$ with $a_0 = a$ and a_{n+1} a proper factor of a_n such that there is some irreducible $p_n \in R$ with $a_n = a_{n+1} \cdot_R p_n$. By induction, a_n is not the product of irreducible elements, and since p_n is irreducible, this implies a_{n+1} does not have an irreducible factorization. $\emptyset''$ can identify an irreducible factor of a_n and so the sequence $\langle a_i \rangle_{i \in \omega}$ is computable from $\emptyset''$. This sequence is a counter-example to ACCP.

□

These theorems represent the first direction of the following equivalence, which is provable in ACA_0. The equivalence holds for an integral domain R if and only if R is a UFD.

Theorem 1.1 (ACA_0)**.** *Let R be an integral domain. The following are equivalent:*

1. *R is an AP domain which satisfies the ACCP;*
2. *R is an Atomic U-UFD.*

Proof. 1. $\Rightarrow$ 2.

Theorems 1.3 and 1.2 prove this direction in ACA_0.

2. $\Rightarrow$ 1.

Suppose every element has exactly one factorization into irreducibles in R. We need to prove R satisfies the ACCP and it is an AP-domain.

Let $\langle c_i \rangle_{i \in \omega}$ be a descending chain in divisibility of R, that is c_{i+1} divides c_i. Let $c_i = \prod_{p_{i,j} \in B_i} p_{i,j}$ be a factorization into irreducibles of c_i, where B_i is a multiset of irreducibles. Note the use of $\emptyset''$ to construct this sequence of multisets, hence the proof uses ACA_0.

We claim $|B_{i+1}| \leq |B_i|$; for if $p_1 p_2 \cdots p_k \cdot \prod_{p_{i+1,j} \in B_{i+1}} p_{i+1,j} = \prod_{p_{i,j} \in B_i} p_{i,j}$, where each p_i is an irreducible, by uniqueness of factorizations $|B_i| = k + |B_{i+1}|$. In turn, this means the sequence $|B_i|_{i \in \omega}$ is a non-increasing sequence of integers, so by Proposition 4.39, it stabilizes, which means there exists some k such that $|B_r| = |B_{r+1}|$ for all $r \geq k$. By uniqueness of irreducible factorizations, this means p_{r+1} does not divide p_r properly.

The second part, that UFD implies AP, is given by Proposition 2.10.

□

For a complete discussion of factorization in integral domains, we refer the reader to [18].

Grams (1974, [10]) has given an example of an Atomic ring that does not satisfy the ACCP, hence providing a counter example to the converse of Theorem 1.2.

It was shown by Coykendall and Zafrullah (2004, [2]) that the converse of Theorem 1.3 does not hold. They have shown that there exist U-UFDs that are not APs.

We proceed now to showing that Theorem 1.2 implies ACA_0.

We start by constructing, in the next section, a tree T, encoding $\emptyset'$ by its non-terminal elements.

We then proceed, in the following section, to defining an increasing sequence $\langle Q_i \rangle_{i \in \omega}$ of rings that encode precisely the elements of the tree, in such a way as to determine the divisibility relation in those rings by the descendant relation in T.

We prove the union of the rings in the sequence forms a computable integral domain Q_ω, whose infinite descending chains in divisibility computes $\emptyset'$.

The conjuction of this result with Theorem 1.2 proves the existence of $\emptyset'$ in a model of both, hence implying ACA_0.

The proofs that follow will be carried in RCA_0.

4.2 A tree encoding $\emptyset'$

We define in stages trees $T_n \subset \omega^{<\omega}$ with $n \in \omega$. At each stage k, we have a corresponding string σ_k, which either gets extended to obtain σ_{k+1} if it agrees with the configuration of $\emptyset'_k$, or else σ_{k+1} is assigned to the parent of σ_k, in a back-tracking step. In the first case, σ_{k+1} is added to T_k to obtain T_{k+1}, while in the second we simply assign T_k to T_{k+1}.

This will provide an indexing for the elements of a ring we will construct later, which will help us determine the proof-theoretic strength of Theorem 1.2.

The collection of strings is formally defined as follows:

Construction 4.3. *Let $\sigma_1 = \lambda$ and $T_1 = \{\sigma_1\}$.*
Step k, for $k \geq 1$: *If there exists $n \in \omega$ with $n < |\sigma_k|$ such that $\sigma_k(n) = 0$ and $n \in \emptyset'_{k+1}$, then $\sigma_{k+1} = \sigma_k^-$ and $T_{k+1} = T_k$. Otherwise put $n = |\sigma_k|$ and let*

$$\sigma_{k+1} = \begin{cases} \sigma_k^\frown 0, & \text{if } n \notin \emptyset'_{k+1} \\ \sigma_k^\frown s, & \text{where } n \in \emptyset'_{k+1} \text{ and } n \in \emptyset'_s \setminus \emptyset'_{s-1} \end{cases}$$

with $T_{k+1} = T_k \cup \{\sigma_{k+1}\}$.

Finally, let $T = \bigcup_{n\in\omega} T_n$.

Note that T is a computable tree in $\omega^{<\omega}$. Formally, we will not make use of this fact, as we will only need the sequence of strings $\langle\sigma_i\rangle_{i\in\omega}$. It is provable in ACA_0 that T has a unique infinite path which computes $\emptyset'$. Since we are working in RCA_0, we cannot use this fact, however it sheds some light on the reasons behind our definition of T: we want an unbounded sequence in T to compute the Halting Problem. Later, we will encode T in a computable integral domain, and make use of an unbounded sequence in T to show that some sequence of the ring computes the Halting Problem.

Lemma 4.8 and Proposition 4.13 define what it means for a string σ to be correct/non-terminal in T. As noted in Chapter 3, this terminology is non-standard.

For brevity, we say that a string σ *appears correct at stage* s, if for all $n < |\sigma|$, $n \in \emptyset'_s$ if and only if $\sigma(n) > 0$. The next lemmas relate the notion of "appears correct" to Construction 4.3.

Lemma 4.4. *Let $k \in \omega$, let $\sigma \in T_k$, and let $n < |\sigma|$. If $\sigma(n) > 0$ then $n \in \emptyset'_k$.*

Proof. By induction on k. Suppose the statement is correct up to $k-1$. Let $\sigma \in T_k$. If $\sigma \in T_{k-1}$ then we are done since $\emptyset'_{k-1} \subset \emptyset'_{k-1}$. So suppose that $\sigma \in T_k \setminus T_{k-1}$, which implies that $\sigma = \sigma_k$, and σ_k extends σ_{k-1}. Let $n < |\sigma_k|$. If $n < |\sigma_{k-1}|$ and $\sigma_k(n) > 0$ then $\sigma_{k-1}(n) > 0$ (as $\sigma_{k-1} \prec \sigma_k$) and so by induction $n \in \emptyset'_{k-1} \subset \emptyset'_k$. Otherwise $n = |\sigma_{k-1}|$ and by definition of σ_k, $\sigma_k(n) > 0$ if and only if $n \in \emptyset'_k$.

□

Lemma 4.5. *Let $k \in \omega$. If σ_k appears correct at stage $k+1$ then σ_{k+1} is an extension of σ_k. Otherwise, $\sigma_{k+1} = \sigma_k^-$.*

Proof. If σ_k appears correct at stage $k+1$ then certainly the condition of the construction for letting σ_{k+1} extend σ_k holds. Suppose otherwise. Let $n < |\sigma_k|$ such that $\sigma_k(n) \neq 0$ if and only if $n \notin \emptyset'_{k+1}$. By Lemma 4.4, $\sigma_k(n) > 0$ is impossible, so $\sigma_k(n) = 0$ and $n \in \emptyset'_{k+1}$. Thus the condition in the construction for letting $\sigma_{k+1} = \sigma_k^-$ holds.

□

Lemma 4.6. *Suppose σ_k is an extension of σ_{k-1}. Then σ_k appears correct at stage k.*

Proof. Let $n < |\sigma_k|$, we show that $n \in \emptyset'_k$ if and only if $\sigma_k(n) > 0$. There are two cases. First suppose that $n < |\sigma_{k-1}|$. By Lemma 4.5, σ_{k-1} appears correct at stage k, or else σ_k would not be an extension of σ_{k-1}. So $\sigma_k(n) = \sigma_{k-1}(n) > 0$ if and only if $n \in \emptyset'_k$ as required. Next take $n = |\sigma_k|$. Then $\sigma_k(n) > 0$ if and only if $n \in \emptyset'_k$ by the definition of σ_k.

□

Lemma 4.7. *Let $\sigma \in T$ and let k be the least such that $\sigma = \sigma_k$, so that $\sigma \in T_k \setminus T_{k-1}$. The collection of stages $s \geq k$ at which σ appears correct forms an interval.*

Proof. It suffices to show that if σ does not appear correct at some stage s, then it does not appear correct at stage $s+1$.

So suppose σ does not appear correct at $s \geq k$. The assumption says that there is some $n < |\sigma|$ such that $\sigma(n) = 0$ but $n \in \emptyset'_s$. So either $\sigma(n) = 0$ and $n \in \emptyset'_s$, or $\sigma(n) \neq 0$ and $n \notin \emptyset'_s$. However, the second is impossible by Lemma 4.4. So $\sigma(n) = 0$ and $n \in \emptyset'_s$, so $n \in \emptyset'_{s+1}$ as well, and so witnesses that σ does not appear correct at stage $s+1$.

□

Lemma 4.8. *Let $\sigma \in T$ and let k be the least such that $\sigma = \sigma_k$. For all $s \geq k$, if σ appears correct at stage s, then $\sigma \preceq \sigma_s$.*

Proof. We prove the lemma by induction on k. By Lemma 4.7, we can start with base case $k = s$, which is immediate since $\sigma_k = \sigma_s$.

Now assume $\sigma_k \preceq \sigma_s$ and σ_k appears correct at step $s+1$, and show $\sigma_k \preceq \sigma_{s+1}$.

If $\sigma_{s+1} = \sigma_s^\frown s$, then $\sigma_k \preceq \sigma_s \prec \sigma_{s+1}$.

If $\sigma_{s+1} = \sigma_s^-$, there are two cases to consider: $\sigma_s = \sigma_k$ or $\sigma_s \succ \sigma_k$.

If $\sigma_s = \sigma_k$, since $\sigma_{s+1} = \sigma_s^-$, there is $j < |\sigma_s|$ such that $\sigma_s(j) = 0$ and $j \in \emptyset'_{s+1}$. This contradicts our assumption.

If $\sigma_s \succ \sigma_k$, then $\sigma_s = \sigma_k^\frown s_1^\frown s_2 \cdots s_t$ where $t > 0$, so $\sigma_{s+1} = \sigma_s^- = \sigma_k^\frown s_1^\frown s_2 \cdots s_{t-1}$, which shows $\sigma_{s+1} \succeq \sigma_k$.

□

Lemma 4.9. *If σ_k is extending σ_{k-1}, then $\sigma_k \notin T_{k-1}$.*

Proof. let $k \in \omega$ and suppose, for a contradiction, that σ_k is an extension of σ_{k-1} but $\sigma_k \in T_{k-1}$. Let m be the least stage such that $\sigma_m = \sigma_k$, so $m < k$ by the assumption for contradiction. By Lemma 4.6, σ_k appears correct at both stages m and k, so by Lemma 4.7, σ_k appears correct at stage $k-1$. By Lemma 4.8, $\sigma_k \preceq \sigma_{k-1}$, contrary to the hypothesis.

□

We define a string $\sigma = \sigma_k$ to be *correct* if for all $n < |\sigma_k|$, $n \in \emptyset'$ if and only if $\sigma_k(n) \neq 0$. Note that this is the same as σ appearing correct at every stage $s \geq k$. We also use the notion of a string being *non-terminal*, which is equivalent to being correct.

Proposition 4.10. If σ is incorrect and $\tau \succeq \sigma$, then τ is incorrect.

Proof. Let σ be incorrect in T and let $\tau \succeq \sigma$. There exists $n < |\sigma|$ with $n \in \emptyset'$ and $\sigma(n) = 0$. The possibility $\sigma(n) > 0$ and $n \notin \emptyset'$ is excluded. Since $\tau \succeq \sigma$, the same property applies to τ, which makes τ incorrect. □

Lemma 4.11. *For every $\tau \in T$, there is a string of greatest length $\sigma \preceq \tau$ which is correct.*

Proof. We note that λ is correct; this is immediate from definition.

Fix a string $\tau \in T$. If τ is correct, we are done. Otherwise, let $A = \{n \leq |\tau| \mid \tau_{\restriction n} \text{ is not correct}\}$. The set A is Σ_1 and non-empty, by Π_1 induction it has a least element.

Since λ is correct, $n > 0$. By Proposition 4.10, $\tau_{\restriction n-1}$ is the longest correct initial segment of τ.

□

Lemma 4.12. *Let $\rho \in T$ be incorrect, but suppose that $\tau = \rho^-$ is correct. Then $\rho = \tau^\frown 0$, and there is some $s > 0$ such that $\tau^\frown s \in T$ is correct.*

Proof. Let $n = |\tau|$. By definition, we know that if $\rho(n) > 0$ then $n \in \emptyset'$; but in that case, ρ would be correct. Hence $\rho = \tau^\frown 0$, and $n \in \emptyset'$. Now, let s be the greatest stage at which $\tau^\frown 0$ appears correct, so $n \in \emptyset'_{s+1} \setminus \emptyset'_s$. By Lemma 4.7, $\rho = \tau^\frown 0$ does not appear correct at any stage $t > s$. So if $t \geq s$ and $\rho \preceq \sigma_t$, then σ_t does not appear correct at stage t and $\sigma_{t+1} = \sigma_t^-$. By induction we see that $\sigma_{s+1} = \sigma_s^-$, $\sigma_{s+2} = \sigma_{s+1}^- \cdots$ until $\sigma_t = \rho$, for $t = s + |\sigma_s| - |\rho|$, and $\sigma_{t+1} = \tau$. Since τ is correct, it appears correct at stage $t+2$ and so $\sigma_{t+2} = \tau^\frown s$ and that string is also correct.

□

Proposition 4.13. Let $\sigma \in T$ and let k be the least such that $\sigma = \sigma_k$. Then:

1. if σ is correct, then for all $s \geq k$, $\sigma \preceq \sigma_s$,
2. if σ is incorrect, then $\sigma \preceq \sigma_s$ for only finitely many s.

If 1 holds we say σ is non-terminal in T, and if 2 holds we say it is terminal.

Proof. Proof of 1. Follows from Proposition 4.8 and the fact that σ appears correct at every stage $s \geq k$.

Proof of 2. Suppose that σ is not correct. By Lemma 4.11, let τ be its longest initial segment that is correct and let $\rho = \sigma_{|\tau|+1}$, so ρ is not correct and $\tau = \rho^-$. By Lemma 4.12, $\rho = \tau^\frown 0$ and there is some $s > 0$ such that $\tau^\frown s \in T$ is correct. By part 1, for all but finitely many stages t we have that $\tau^\frown s \preceq \sigma_t$. Since $\sigma \succ \tau \frown 0$ is incomparable with $\tau^\frown s$, for every such stage t, $\sigma \not\preceq \sigma_t$.

□

Proposition 4.13 provides us with the definition of "non-terminal", formulated in RCA_0, and shows this notion is equivalent to "correct".

Proposition 4.14. Any two non-terminal strings are comparable.

Proof. Let σ, τ be two non-terminal strings. Let k be the least such that $\sigma \in T_k$ and t be the least such that $\tau \in T_t$.

By Proposition 4.13, if $t \geq k$, then $\sigma \preceq \tau$, otherwise $\sigma \succ \tau$.

□

Proposition 4.15. Every correct string has a correct proper extension in T.

Proof. Let $\sigma \in T$ be correct, and let k be the least such that $\sigma = \sigma_k$. If σ_{k+1} is correct then we are done. Otherwise, Lemma 4.12 shows that $\sigma_{k+1} = \sigma^\frown 0$ and that there is some $s > 0$ such that $\sigma^\frown s \in T$ and is correct.

□

For a sequence along a path in T, it must be that the elements of the sequence have a bigger size than their index in T.

Proposition 4.16. In an infinite sequence $(\tau_i)_{i\in\omega}$ consisting of elements of T such that $\tau_k \prec \tau_{k+1}$, we have that $|\tau_k| \geq k$, for all $k \in \omega$.

Note that we are working in RCA_0 and we assume the sequence $(\tau_i)_{i\in\omega}$ exists, i.e. is an element of the second order part of the model. Hence the induction we will be performing in the proof is valid in RCA_0.

Proof. We know $|\tau_0| \geq 0$ since lengths are non-negative. Assume $|\tau_k| \geq k$, for some $k \in \omega$.

Since $\tau_k \prec \tau_{k+1}$, $\tau_{k+1} = \tau_k \widehat{} s_1 \widehat{} s_2 \cdots \widehat{} s_v$, for $v \geq 1$. But then, $|\tau_{k+1}| = |\tau_k| + v \geq |\tau_k| + 1 \geq k + 1$, so $|\tau_{k+1}| \geq k + 1$.

□

We use Propositions 4.16 and 4.13 to show that an infinite sequence of descendants in T computes $\emptyset'$. Intuitively, this means an infinite path of T computes the Halting Problem.

Lemma 4.17. *Any infinite sequence $(\tau_i)_{i\in\omega}$ consisting of elements of T such that $\tau_k \prec \tau_{k+1}$ computes $\emptyset'$.*

Proof. By Proposition 4.16, for all k, $|\tau_k| \geq k$.

We need to show that each τ_k is correct. This follows from Proposition 4.13 (2) and the fact that τ_k has infinitely many extensions on T, namely τ_m for $m > k$.

□

4.3 Equivalence with ACA_0

We will show there exist a computable non-Atomic integral domain in which every witness of the failure of ACCP computes $\emptyset'$. Since ACA_0 is the weakest system that can prove the existence of the Turing Jump, this will give us our result.

The following proposition gives the sequence of underlying sets for the rings we define in Construction 4.19.

Proposition 4.18. There exists a uniformly computable sequence of sets $\langle Q_n \rangle_{n\in\omega}$ such that

1. $|Q_0| = \omega$,
2. $Q_m \subset Q_{m+1}$ and $|Q_{m+1} \setminus Q_m| = \omega$,
3. $\bigcup_{n\in\omega} Q_n = \omega$.

Proof. We will be implicitly using pairing functions, which means pairs (m, x) are coded as elements of ω.

Define the sequence $(Q_n)_{n\in\omega}$ by $Q_n = \{(m,x) \mid x \in \omega, m \leq n\}$. The sequence is uniformly computable due to the fact that it can be effectively coded into ω using computable pairing functions.

Property 1 follows since $|Q_0| = |\{0\} \times \omega| = \omega$.

Since $Q_m \subset Q_{m+1}$ and $|\{m+1\} \times \omega| = \omega$, property 2 follows.

Property 3 follows because $\bigcup_{n\in\omega} Q_n = \omega \cdot \omega$.

□

Let $Q_0, Q_1, Q_2 \cdots$ be the sequence obtained from Proposition 4.18. We are going to put computable ring structures on each of them in the following construction, which looks at the way Construction 4.3 is carried. Each Q_{k+1} is a superset of Q_k and it is generated as a ring over Q_k. We index its generators a_σ, b_σ, with elements of T. Each Q_k will be a computable subring of Q_{k+1}.

To define Q_{k+1} we look at how T_{k+1} is obtained from T_k. If we back-track and make $\sigma_{k+1} = \sigma_k^-$, then we want b_{σ_k} to be a unit in Q_{k+1}, otherwise we want $a_{\sigma_k} = a_{\sigma_{k+1}} b_{\sigma_{k+1}}$, in order to generate an infinite descending chain in divisibility in the rings.

More formally:

Construction 4.19. *At step* 0, *apply Proposition 3.27 to the set* Q_0 *to obtain* $Q_0 \cong \mathbb{Q}$, *and let* $R_0 = Q_0$.

At step 1, *apply Corollary 3.17 to* Q_0 *and* Q_1 *to obtain a computable structure on* Q_1 *and an element* $a \in Q_1$ *transcendental over* Q_0, *such that* $Q_1 = Q_0[a]$. *Let* $a_\lambda = a$, *and we have* $Q_1 = Q_0[a_\lambda] = R_0[a_\lambda]$, *such that* a_λ *is transcendental over* R_0. *Let* $R_1 = R_0$.

Let $a = a_{\sigma_k}$, $b = b_{\sigma_k}$ *and* $\bar{b} = b_{\sigma_k \restriction n}$ *for* $n = 1, 2 \cdots |\sigma_k|$.

At step k, *we have computable ring* $Q_k = R_k[a, \bar{b}]$, *where* R_k *is a computable subring of* Q_k *and the elements presented are algebraically independent over* R_k.

At step $k+1$, *if* $T_{k+1} = T_k$ *we want to make* b *a unit. Since* $Q_k \subset Q_{k+1}$, $|Q_{k+1} \setminus Q_k|$ *is infinite, choose the element* $b \in Q_k$ *which is non-zero and non-*

unit by Remark 2.48, and since Q_k is an integral domain by Corollary 4.22, apply Corollary 3.19 to put a computable structure on Q_{k+1} that makes it a computable ring with $Q_k < Q_{k+1}$, b a unit of Q_{k+1} and $Q_{k+1} = Q_k[b^{-1}]$. Put $R_{k+1} = R_k[b, b^{-1}]$. Note that the conditions for applying Corollary 3.19 hold, in particular the relation $\{\langle q, m\rangle \in Q_k \times \omega \mid b^m \mid q\}$ is computable. To see this, note that $Q_k \cong R_k[y, x_1, x_2 \cdots x_{|\sigma_k|}]$ over R_k and this isomorphism is computable by Remark 3.8. Let $b = b_{\sigma_k}$, $q \in Q_k$ and $m \in \omega$, to tell whether $b^m \mid q$ find a polynomial $f \in R_k[y, \bar{x}]$ such that $f(a, \bar{b}) = q$ and check whether $x_{|\sigma_k|}^m$ divides f in $R_k[y, \bar{x}]$; this is done by examining the coefficients of f to see if the power of $x_{|\sigma_k|}$ is at least m on any monomial with nonzero coefficient.

If $T_{k+1} = T_k \cup \{\sigma_{k+1}\}$, we have $Q_k = (R_k[\bar{b}])[a]$ by Remark 2.40. Note that by Proposition 3.23, $R_k[\bar{b}]$ is computable. and since $Q_{k+1} \supset Q_k$ we can apply Corollary 3.21 to $R_k[\bar{b}]$, $(R_k[\bar{b}])[a]$ and Q_{k+1} to obtain the set $\{c, d\} \subset Q_{k+1}$ independent over $R_k[\bar{b}]$ and a computable structure on Q_{k+1}, such that $Q_{k+1} = (R_k[a, \bar{b}])[c, d]$, i.e. $Q_{k+1} = Q_k[c, d]$ with $c \cdot_{Q_{k+1}} d = a$. We let $b_{\sigma_{k+1}} = c$ and $a_{\sigma_{k+1}} = d$. Put $R_{k+1} = R_k$.

Remark 4.20 shows the inductive definition preserves the inductive hypothesis.

Finally, let the union of each element of the sequence be a ring, $Q_\omega = \bigcup_{k\in\omega} Q_k$.

It is an essential ingredient of Construction 4.19 that the properties inferred in the inductive definition are preserved by induction. We prove this here.

Remark 4.20. In the inductive definition of Construction 4.19, $Q_{k+1} = R_{k+1}[a_{\sigma_{k+1}}, b_{\sigma_{k+1}\restriction n}]_{n=1,2\cdots|\sigma_{k+1}|}$, with the elements presented being algebraically independent over R_{k+1}, and furthermore R_{k+1} is a computable subring of Q_{k+1}.

Proof. We need to verify the induction hypothesis is preserved at step $k+1$. We need to show we have computable ring $Q_{k+1} = R_{k+1}[a_{\sigma_{k+1}}, b_n]_{n=1,2\cdots|\sigma_{k+1}|}$, where R_{k+1} is a computable subring of Q_{k+1} and the elements presented are algebraically independent over R_{k+1}.

If $T_{k+1} = T_k$ and we make b_{σ_k} a unit, note that $\sigma_{k+1} = \sigma_k^-$ from Construction 4.3. Let $a = a_{\sigma_k}$, $b = b_{\sigma_k}$ and $\bar{b} = b_1, b_2 \cdots b_{|\sigma_k|-1}$.

We have $Q_{k+1} = Q_k[b^{-1}]$, so by inductive hypothesis $Q_{k+1} = (R_k[a, b, \bar{b}][b^{-1}]$, by Remark 2.40 $Q_{k+1} = (R_k[b, b^{-1}])[a, \bar{b}] = R_{k+1}[a, \bar{b}]$. By definition, we have that $R_{k+1} < Q_{k+1}$. Since $\sigma_{k+1} = \sigma_k^-$, $a = a_{\sigma_{k+1}} \cdot b^{-1}$ and $b^{-1} \in R_{k+1}$, we have $Q_{k+1} = R_{k+1}[a_{\sigma_{k+1}}, b_{\sigma_{k+1}\restriction n}]_{n=1,2\cdots|\sigma_{k+1}|}$.

We need to show that $\{a_{\sigma_{k+1}}, \bar{b}\}$ is independent over R_{k+1}.

By Induction Hypothesis we know $\{a, b, \bar{b}\}$ is independent over R_k.

We claim it suffices to show $\{a, \bar{b}\}$ is independent over R_{k+1}. For if this is the case, then by Lemma 2.46 $\{a\}$ is independent over $R_{k+1}[\bar{b}]$ where $\bar{b}$ is independent over R_{k+1}, by Lemma 2.47 $\{ab\}$ is independent over $R_{k+1}[\bar{b}]$, and using Lemma 2.46 again and the fact that $ab = a_{\sigma_{k+1}}$, we obtain $\{a_{\sigma_{k+1}}, \bar{b}\}$ independent over R_{k+1}.

Now let $f \in R_{k+1}[x, y_1, y_2 \cdots y_{|\sigma_k|-1}]$ such that $f \neq 0$. By Remark 2.40, $f \in ((R_k[b])[b^{-1}])[x, y_1, y_2 \cdots y_{|\sigma_k|-1}]$. By Lemma 2.51, there is $N \in \omega$ such that $b^N f = g \in R_k[b][x, \bar{y}]$. By Lemma 2.46, $\{a, \bar{b}\}$ independent over $R_k[b]$ if and only if $\{a, b, \bar{b}\}$ independent over R_k. This last condition holds by Inductive Hypothesis, so $\{a, \bar{b}\}$ independent over $R_k[b]$, which means $g(a, \bar{b}) \neq 0$ which, since $b \neq 0$, means that $f(a, \bar{b}) \neq 0$, so the set $\{a, \bar{b}\}$ is independent over R_{k+1}.

Since $R_{k+1} = R_k[b, b^{-1}]$, R_k is computable and b is transcendental over R_k, by Lemma 3.25 R_{k+1} is computable.

If $T_{k+1} = T_k \cup \{\sigma_{k+1}\}$, and we let $Q_{k+1} = Q_k[a_{\sigma_{k+1}}, b_{\sigma_{k+1}}]$ and $R_{k+1} = R_k$, then we have $Q_{k+1} = (R_k[a_{\sigma_k}, b_{\sigma_k\restriction n}]_{n=1,2\cdots|\sigma_k|}])[a_{\sigma_{k+1}}, b_{\sigma_{k+1}}]$ $= R_k[a_{\sigma_{k+1}}, a_{\sigma_k}, b_{\sigma_{k+1}\restriction n}]_{n=1,2\cdots|\sigma_{k+1}|}$, and since $a_{\sigma_k} = a_{\sigma_{k+1}} b_{\sigma_{k+1}}$ we have $a_{\sigma_k} \in R_k[a_{\sigma_{k+1}}, b_{\sigma_{k+1}\restriction n}]_{n=1,2\cdots|\sigma_{k+1}|}$ so $R_k[a_{\sigma_{k+1}}, a_{\sigma_k}, b_{\sigma_{k+1}\restriction n}]_{n=1,2\cdots|\sigma_{k+1}|} = R_k[a_{\sigma_{k+1}}, b_{\sigma_{k+1}\restriction n}]_{n=1,2\cdots|\sigma_{k+1}|}$, therefore $Q_{k+1} = R_k[a_{\sigma_{k+1}}, b_{\sigma_{k+1}\restriction n}]_{n=1,2\cdots|\sigma_{k+1}|} = R_{k+1}[a_{\sigma_{k+1}}, b_{\sigma_{k+1}\restriction n}]_{n=1,2\cdots|\sigma_{k+1}|}$.

The set $\{b_{\sigma_{k+1}\restriction n} \mid n = 1, 2 \cdots |\sigma_k|\}$ is independent over $R_{k+1} = R_k$, since it is a subset of variables at step k. The set $\{a_{\sigma_{k+1}}, b_{\sigma_{k+1}}\}$ is independent over $R_{k+1}[b_{\sigma_{k+1}} \restriction n]$ in virtue of Corollary 3.21. By Lemma 2.46, $\{a_{\sigma_{k+1}}, b_{\sigma_{k+1}\restriction n}, \mid n = 1, 2 \cdots |\sigma_{k+1}|\}$ is independent over R_{k+1}.

□

The rings defined in Construction 4.19 are UFDs. We will make use of

this property extensively in later stages of our proof.

Proposition 4.21. Each ring in the sequence $\langle Q_i \rangle_{i \in \omega}$ is a UFD.

Proof. First we show that the rings in the sequence $\langle R_i \rangle_{i \in \omega}$ are UFDs. We use induction on i. $R_0 \cong \mathbb{Q}$, R_0 is a UFD since it is isomorphic to a field, and a field is vacuously a UFD.

Assume R_k is a UFD. We look at step $k+1$. If $R_{k+1} = R_k$ we are done. If $R_{k+1} = R_k[b_\sigma, b_\sigma^{-1}] = (R_k[b_\sigma])[b_\sigma^{-1}]$, we use Proposition 2.43, since b_σ is independent over R_k, to obtain that $R_k[b_\sigma]$ is a UFD. Then, by Lemma 2.25, the localization of $R_k[b_\sigma]$ on b_σ, $R_k[b_\sigma]_{b_\sigma}$ must be a UFD. By Proposition 2.39, $R_k[b_\sigma]_{b_\sigma} \cong (R_k[b_\sigma])[b_\sigma^{-1}]$, so the latter must be a UFD.

So R_{k+1} is a UFD.

Since at step k we have computable ring $Q_k = R_k[a_{\sigma_k}, b_{\sigma_k \restriction n}]_{n=1,2 \cdots |\sigma_k|}$, where R_k is a UFD and the elements presented are algebraically independent over R_k, by Proposition 2.43 we deduce that Q_k is a UFD.

This shows that each ring in the sequence must be a UFD. □

As a corollary, each Q_i must be an integral domain.

Corollary 4.22. *Each ring in the sequence $\langle Q_i \rangle_{i \in \omega}$ is an integral domain.*

Proof. By Proposition 4.21. □

The obvious consequence is that Q_ω must be an integral domain.

Proposition 4.23. The ring Q_ω is an integral domain.

Proof. Suppose $a \cdot_{Q_\omega} b = 0_{Q_\omega}$ with $a \neq 0_{Q_\omega}$ and $b \neq 0_{Q_\omega}$. Then $a \cdot_{Q_n} b = 0_{Q_\omega}$ and neither elements are zero in Q_n, where Q_n can be chosen as the smallest ring in the sequence containing all three elements. Such a ring must exist because all elements are added at finite stages, and they all contain the element 0_{Q_ω}.

So an element in the sequence $(Q_i)_{i \in \omega}$ is not an integral domain, which contradicts Corollary 4.22.

□

Since we are working in RCA_0, the structures we define need to be computable. This is the motivation behind the following proposition.

Proposition 4.24. The sequence of rings $(Q_i)_{i \in \omega}$ is uniformly computable.

Proof. By Proposition 4.18 and Construction 4.19, the set $U = \{(q, n) \mid q \in Q_n\}$ is computable.

We need to show that the sets $P = \{(p, q, r, k) \mid p = q +_{Q_k} r\}$ and $T = \{(p, q, r, k) \mid p = q \cdot_{Q_k} r\}$ are computable. So let $q, r \in \bigcup_{i\in\omega} Q_i$. Since U is computable, we can find the least $k_1, k_2 \in \omega$ such that $q \in Q_{k_1}$ and $r \in Q_{k_2}$. Let $k = \max(k_1, k_2)$ and since $Q_i < Q_{i+1}$ for all i, we can see that $q +_{Q_k} r = q +_{Q_t} r$ and $q \cdot_{Q_k} r = q \cdot_{Q_t} r$, for any $t \geq k$. Therefore, $(p, q, r, t) \in P$ and $(v, q, r, t) \in T$ if and only if $t \geq k$, $q +_{Q_k} r = p$ and $q \cdot_{Q_k} r = v$. Note that if $p \notin Q_k$ or $v \notin Q_k$, the corresponding pairs are not in P or T respectively.

We argue that Construction 4.19 is computable. Construction 4.19 appeals to Corollaries 3.19 and 3.21. By Remarks 3.20 and 3.22 these results are effective, which means there is an effective procedure for passing from effective descriptions of the inputs to effective descriptions of the outputs.

We need to argue that the function taking k to:

(i) $a_{\sigma_k}, b_{\sigma_k}$,

(ii) a computable index for Q_k,

(iii) a computable index for R_k,

(iv) a computable index for the isomorphism between $R_k[y, \bar{x}]$ and Q_k,

is computable. This is done by induction on k.

In particular, at Step 0 we take a computable set Q_0 and put a ring structure on it such that $Q_0 \cong \mathbb{Q}$. Step 1 describes a process that takes the computable ring Q_0 and its computable superset Q_1 and outputs a computable ring structure on Q_1 and an element $a \in Q_1$ transcendental over Q_0 such that $Q_1 = Q_0[a]$. These steps are executed once, so uniformity is not an issue.

Assume this has been done up to k. We can effectively tell from Construction 4.19 what σ_{k+1} is, and so which of the two cases holds. In each case we explain how to effectively get (i), (ii), (iii) and (iv).

Step $k+1$, in the first case $T_{k+1} = T_k$, $\sigma_{k+1} = \sigma_k^-$; we first find the greatest $m < k$ such that $\sigma_{k+1} = \sigma_m$.

(i): $a_{\sigma_{k+1}} = a_{\sigma_m}$ and $b_{\sigma_{k+1}} = b_{\sigma_m}$, which by induction we already have.

(ii): first note that by induction we have an index for a computable isomorphism between Q_k and $R_k[y, \bar{x}]$ over R_k. The argument given in the construction shows how to effectively obtain a computable index for the set $\{\langle c, m\rangle \in Q_k \times \omega \mid b^m_{\sigma_k} \mid c\}$. We have a computable index for the set Q_{k+1} since $\langle Q_n\rangle$ is uniformly computable by Proposition 4.18, a computable index for

R_k by induction, and we have b_{σ_k} also by induction. Then we have all the inputs needed for Corollary 3.19 and we effectively get an index for Q_{k+1} from Remark 3.20.

(iii): we have indices for R_k, Q_k by induction, and Q_{k+1} obtained previously, we have b_{σ_k} and indeed the sequence $a, \bar{b}$ also by induction. By Remark 3.26, we get effectively a computable index for R_{k+1}.

(iv): an index for an isomorphism from $R_{k+1}[y, \bar{x}]$ to Q_{k+1} is found effectively given indices for R_{k+1}, Q_{k+1} and given $a_{\sigma_{k+1}}$, $b_{\sigma_{k+1}\restriction 1,2\cdots|\sigma_{k+1}|}$ which we already have. This is done by observing that Remark 3.8 is uniform: given indices for R and Q, and given $\bar{a}$, we get an index for the map $\langle f, \bar{a}\rangle \mapsto f(\bar{a})$.

Finally, step $k+1$, in the second case $T_{k+1} = T_k \cup \{\sigma_{k+1}\}$, and σ_{k+1} is new.

(i) and (ii): by induction we have indices for R_k and Q_k, and we have $a, \bar{b}$. This gives us a computable index for $R_k[\bar{b}]$ by Remark 3.24. We have an index for the set Q_{k+1}. So by Remark 3.22, we effectively get an index for Q_{k+1}, and also we get the elements $a_{\sigma_{k+1}}$ and $b_{\sigma_{k+1}}$.

(iii): $R_{k+1} = R_k$ and by induction we have an index for R_k.

(iv): exactly as above.

□

Computability of Q_ω follows from Proposition 4.24.

Proposition 4.25. The ring Q_ω is computable.

Proof. Given $q, r \in Q_\omega$, by Proposition 4.24, the sets $\{(q, n) \mid q \in Q_n\}$, $\{(p, q, r, k) \mid p = q +_{Q_k} r\}$ and $\{(p, q, r, k) \mid p = q \cdot_{Q_k} r\}$ are computable.

So one can find $k_1, k_2 \in \omega$, such that $q \in Q_{k_1}$ and $r \in Q_{k_2}$. If $k = \max(k_1, k_2)$, then because $Q_k < Q_\omega$, $q +_{Q_\omega} r = q +_{Q_k} r$ and $q \cdot_{Q_\omega} r = q \cdot_{Q_k} r$.

□

We will observe that b_σ is invertible in Q_ω if σ is terminal in T. Further, an element will be invertible in Q_ω if it was explicitly made invertible in a ring Q_n in the sequence.

Remark 4.26. p is invertible in Q_ω if and only if it is invertible in Q_n, for some $n \in \omega$. Furthermore, if p is invertible in Q_n, then it is invertible in all Q_m with $m \geq n$.

Proof. Suppose $p \cdot_{Q_\omega} p^{-1} = 1$. Then $p \cdot_{Q_n} p^{-1} = 1$ in some Q_n.

Since $Q_n < Q_m$ for all $m > n$, $p, p^{-1} \in Q_m$ and furthermore $p \cdot_{Q_m} p^{-1} = 1$.

□

As we noted above, if σ is terminal there will be a stage k of Construction 4.19 at which we make b_σ a unit of Q_{k+1}.

Lemma 4.27. *Suppose σ is terminal in T. Then there is some stage s such that b_σ is a unit of Q_{s+1}.*

Proof. Proposition 4.13 together with the fact that σ is terminal imply there exist stages s with $s \geq k$ such that σ_{s+1} does not extend σ.

Choose $s \geq k$ to be the least such stage.

By the choice of s, we have in Construction 4.3: $\sigma_s = \sigma_k$ and $\sigma_{s+1} = \sigma_k^-$.

This means b_{σ_k} is made a unit of Q_{s+1}.

□

The units b_σ of Q_ω are precisely the b elements indexed by terminal elements of T.

Lemma 4.28. *b_σ is a unit of Q_ω if and only if σ is terminal in T.*

Proof. Suppose σ is terminal. By Proposition 4.27, there is stage k for some $k \in \omega$ such that b_σ is a unit of Q_k. Since $Q_k < Q_\omega$, b_σ is a unit of Q_ω.

Conversely, suppose σ is non-terminal in T. Let k be the step at which σ is added to the union, so $\sigma_k = \sigma$, so we have the ring $Q_k = R_k[a_{\sigma_k}, b_{\sigma_k \restriction n}]_{n=1,2\cdots|\sigma_k|}$ where the presented variables form an independent set over R_k.

Since σ is non-terminal, by Remark 4.13, for all $n > k$, $\sigma_n \succeq \sigma_k = \sigma$ and thus σ is an initial segment of σ_n, and so, in Q_n, b_σ is transcendental over R_n, since all initial segments σ of σ_n index elements b_σ in the independent set that generates R_n.

Therefore, by Remark 2.48, b_σ is not invertible in Q_n. By Remark 4.26, b_σ is not invertible in Q_ω.

□

The structure of the ascending chain of rings $\langle Q_i \rangle_{i \in \omega}$ makes it possible to factorize an element a_σ using elements a_τ and b_τ where τ are strings descending from σ. This will produce an infinite descending chain in divis-

ibility, along the infinite path of T. We refer to these factorizations in the following propositions.

Proposition 4.29. If $\tau \prec \sigma_n$ and $\tau_0, \tau_1 \cdots \tau_t \in T$ is the sequence such that $\tau_0 = \tau$, $\tau_t = \sigma_n$ and $\tau_i = \tau_{i+1}^-$ for $0 \leq i < t$, then $a_\tau = a_{\sigma_n} \prod_{i=1}^{t} b_{\tau_i}$ in $Q_n = R_n[a_{\sigma_n}, b_{\sigma_n \restriction m}]_{m=1,2\cdots|\sigma_n|}$.

Proof. For each $i \in \{1, 2 \cdots t\}$, let $n(i)$ be the least such that $\tau_i = \sigma_{n(i)}$. Then by Construction 4.19, in $Q_{n(i)}$, $a_{\tau_{i-1}} = a_{\tau_i} b_{\tau_i}$. Note that $n(i) \leq n$ for each i, so $a_{\tau_{i-1}} = a_{\tau_i} b_{\tau_i}$ in Q_n as well. By induction on $k \leq t$ we see that in Q_n, $a_\tau = a_{\tau_k} \prod_{i=1}^{k} b_{\tau_i}$.

□

Proposition 4.30. If $\tau \prec \sigma$ and $\tau_0, \tau_1 \cdots \tau_t \in T$ is the sequence such that $\tau_0 = \tau$, $\tau_t = \sigma$ and $\tau_i = \tau_{i+1}^-$ for $0 \leq i < t$, then $a_\tau = a_\sigma \prod_{i=1}^{t} b_{\tau_i}$ in Q_ω.

Proof. Let $\sigma = \sigma_n$ for some $n \in \omega$. By Proposition 4.29, $a_\tau = a_\sigma \prod_{i=1}^{t} b_{\tau_i}$.

□

Intuitively, for all elements σ terminal in T, we make b_σ a unit. This will make a_σ and its terminal ancestors associates, while also providing an associate a_τ for a_σ, where τ belongs to the infinite path. We use this trick to ensure the non-wellfoundedness of divisibility in Q_ω.

Lemma 4.31. *If $\sigma, \sigma^\frown k \in T$ are non-terminal and $\tau \succcurlyeq \sigma^\frown 0$, $k > 0$, then $a_\tau \sim a_\sigma$ in Q_ω.*

Proof. Let $\tau_0, \tau_1 \cdots \tau_k \in T$ be the finite sequence such that $\tau_0 = \tau$, $\tau_k = \sigma$ and $\tau_{i+1} = \tau_i^-$ for $0 \leq i \leq k-1$.

From Proposition 4.30, $a_\sigma = a_\tau \prod_{i=0}^{k-1} b_{\tau_i}$.

Since $\tau_i \succeq \sigma^\frown 0$, by Proposition 4.10, τ_i is terminal for all $0 \leq i < k$. By Lemma 4.28, b_{τ_i} are all invertible in Q_ω.

The fact that the product of finitely many units is a unit is proved by Σ_1 induction.

□

No a_σ in Q_ω is a unit or irreducible. Hence a_λ does not have an irreducible factorization.

Proposition 4.32. For any $\sigma \in T$, a_σ is not a unit of Q_ω.

Proof. Suppose some a_σ is a unit of Q_ω, with $\sigma = \sigma_m$. Then by Remark 4.26, it is a unit of some element of the sequence $\langle Q_i \rangle_{i \in \omega}$, $Q_k = R_k[a_{\sigma_k}, b_{\sigma_k \restriction n}]_{n=1,2 \cdots |\sigma_k|}$. We can choose k such that $k > m$.

By Lemma 4.31, if σ is terminal, then $a_\sigma \sim a_\tau$ such that τ is non-terminal; here, τ is the longest non-terminal initial-segment of σ. τ exists by Lemma 4.11.

So we may assume that σ is non-terminal.

By Remark 4.13, $\sigma_k \succeq \sigma$, and so by Proposition 4.30 $a_{\sigma_k} \mid a_\sigma$. But then a_{σ_k} is a unit, but this is impossible due to Remark 2.48.

□

Lemma 4.33. *For all $\sigma \in T$, no a_σ is irreducible in Q_ω.*

Proof. In the first case, if σ is non-terminal, by Proposition 4.15 there is some τ non-terminal such that $\sigma \prec \tau$. But then by Remark 4.30, $a_\tau \mid a_\sigma$. But we know a_τ cannot be a unit by Proposition 4.32, and we know b_τ is also not a unit by Lemma 4.28, and so the division $a_\tau \mid a_\sigma$ must be proper.

If σ is terminal, then we can find the longest initial segment τ of σ that is not. By Lemma 4.31, there is invertible $b \in Q_\omega$ such that $a_\tau b = a_\sigma$. This reduces the proof to the first case.

□

Since every ring Q_i in our sequence is a UFD, we will use unique factorization to our advantage in inferring that *all* factorizations must be along a path in T. We give the consequence of unique factorization here.

Proposition 4.34. Let $\sigma \in T$. If σ is non-terminal and $a_\sigma \in Q_k$, then the only irreducible factorization of a_σ in Q_k is $[a_{\sigma_k}, b_{\sigma_k \restriction n} \mid n = |\sigma| + 1, |\sigma| + 2 \cdots |\sigma_k|]$, where $Q_k = R_k[a_{\sigma_k}, b_{\sigma_k \restriction n}]_{n=1,2 \cdots |\sigma_k|}$.

Proof. In this proof, irreducible will mean irreducible in Q_k.

Note that by Remark 4.13, $\sigma \preceq \sigma_k$.

By Remark 2.50, the elements a_{σ_k} and $b_{\sigma_k \restriction n}$ are irreducible.

By Proposition 4.30, $a_\sigma = a_{\sigma_k} \prod_{n=|\sigma|+1}^{|\sigma_k|} b_{\sigma_k \restriction n}$.

By Proposition 4.21, Q_k is a UFD, so any factorization of a_σ into irreducibles must be equal up to association to $[a_{\sigma_k}, b_{\sigma_k \restriction n} \mid n = |\sigma|+1, |\sigma|+2 \cdots |\sigma_k|]$.

□

As note above, a_λ has no irreducible factorization. This implies that Q_ω is non-Atomic.

Corollary 4.35. *Q_ω is non-Atomic.*

Proof. We claim a_λ has no irreducible factorization in Q_ω. Suppose the contrary, and let $[p_i \mid i \leq n]$ be such a factorization. Find the minimum k such that Q_k contains all p_i with $i \leq n$. We know $Q_k = R_k[a_{\sigma_k}, b_{\sigma_k \restriction n}]_{n=1,2\cdots|\sigma_k|}$.

Note the mentioned elements are irreducible in Q_ω, we argue by contrapositive they are irreducible in Q_k. Note that a_{σ_k} divides a_λ in Q_k. Because a_{σ_k} is a prime element of Q_k, there is some i such that a_{σ_k} divides p_i in Q_k, and so divides it in Q_ω as well; but a_{σ_k} is reducible in Q_ω, and so p_i too is reducible in Q_ω.

□

We need the following Lemma for proving a few of the upcoming results. It essentially states that along the chain of rings $\langle Q_i \rangle_{i \in \omega}$, the irreducibles remain irreducible or become units.

Lemma 4.36. *If $p \in Q_n$ is irreducible and $a_{\sigma_n} \nmid_{Q_n} p$, then either:*

1. *$p \in Q_{n+1}^\times$ or*
2. *p is irreducible in Q_{n+1} and $a_{\sigma_{n+1}} \nmid_{Q_{n+1}} p$.*

Proof. We have $Q_n = R_n[a_{\sigma_n}, b_{\sigma_n \restriction m}]_{m=1,2\cdots|\sigma_n|}$.

According to Construction 4.19 there are two cases to consider: $Q_{n+1} = Q_n[b_{\sigma_n}^{-1}]$ and $Q_{n+1} = Q_n[a_{\sigma_{n+1}}, b_{\sigma_{n+1}}]$ with $a_{\sigma_{n+1}} \cdot b_{\sigma_{n+1}} = a_{\sigma_n}$.

Suppose $Q_{n+1} = Q_n[b_{\sigma_n}^{-1}] = R_n[b_{\sigma_n}, b_{\sigma_n}^{-1}][a_{\sigma_n^-}, b_{\sigma_n \restriction m}]_{m=1,2\cdots|\sigma_n|-1}$.

By Proposition 2.39, Q_{n+1} is isomorphic to the localization of Q_n by $\{b_{\sigma_n}^t \mid t \in \omega\}$, and by Lemma 2.23 and the fact that Q_n is a UFD we have that p is either prime or unit in Q_{n+1}.

Now suppose $Q_{n+1} = Q_n[a_{\sigma_{n+1}}, b_{\sigma_{n+1}}]$ where $a_{\sigma_{n+1}} \cdot b_{\sigma_{n+1}} = a_{\sigma_n}$.

Write $a_1 = a_{\sigma_{n+1}}, b_1 = b_{\sigma_{n+1}}, a_2 = a_{\sigma_n}$, $\bar{b} = b_{\sigma_n \restriction m}$ for $m = 1, 2 \cdots |\sigma_n|$, $R = R_n[\bar{b}]$ and $\bar{y} = y_1, y_2 \cdots y_{|\sigma_n|}$.

We have $Q_n = R[a_2]$ with a_2 transcendental over R and $Q_{n+1} = R[a_1, b_1]$ with $\{a_1, b_1\}$ independent over R and $a_1 \cdot b_1 = a_2$.

By Proposition 2.44, let $\varphi\colon R[y, z] \to Q_{n+1}$ be an isomorphism over R, with $\varphi(y) = a_1$ and $\varphi(z) = b_1$. Similarly, let $\psi\colon R[x] \to Q_n$ be an isomorphism over R with $\psi(x) = a_2$.

Let $h \in R[x]$ with $h = \psi^{-1}(p)$, so $h(a_2) = p$. Since p is irreducible in Q_n, h is irreducible in $R[x]$. Since a_2 does not divide p in Q_n, $x = \psi^{-1}(a_2)$ does not divide h in $R[x]$. This means that the constant coefficient of h is nonzero. Let $\hat{h} = h(yz) \in R[y, z]$. Since $a_2 = a_1 b_1$ and $h(a_2) = p$, we see that $\hat{h}(a_1, b_1) = p$. Hence $\hat{h} = \varphi^{-1}(p)$.

We show that p is irreducible in Q_{n+1}. To do that, let $s, t \in Q_{n+1}$ and suppose that $p = s \cdot t$; we need to show that either s or t is a unit of Q_{n+1}. Let $f = \varphi^{-1}(s)$ and $g = \varphi^{-1}(t)$; equivalently, we need to show that either f or g is a unit of $R[y, z]$. Since $p = st$, applying the isomorphism φ^{-1} we have $\hat{h} = fg$.

There are several cases to consider:

(i) $\deg(h) = 0$,

(ii) $\deg_y(f), \deg_y(g) > 0$ (this case is analogous to $\deg_z(f), \deg_z(g) > 0$, which we therefore omit),

(iii) $\deg_y(f) = deg_z(f) = 0$, i.e. $f \in R$ (analogous to $g \in R$), and

(iv) $\deg_y(f), \deg_z(g) > 0, \deg_z(f) = \deg_y(g) = 0$ (analogous to the case with y and z exchanged).

Case (i): in this case $h = \hat{h} \in R$, and therefore $f, g \in R$ also. Since h is irreducible in $R[x]$, it is irreducible in R, and so $fg = \hat{h} = h$ implies that either f or g is a unit of R and certainly this implies that f or g is a unit of $R[y, z]$.

Case (ii): write $f = \sum_{i=0}^{e} f_i(z) y^i$ and $g = \sum_{i=0}^{d} g_i(z) y^i$, for $d, e \in \omega$ and $g_i, f_i \in R[z]$ and $f_e, g_d \neq 0$.

By Proposition 2.34, there is some $\alpha \in R^\times$ such that $f_e(\alpha) \neq 0$ and

$g_d(\alpha) \neq 0$. Let $\bar{f}(x) = f(x\alpha^{-1}, \alpha) = \sum_{i=0}^{e} \alpha^{-i} f_i(\alpha) x^i$ and similarly let $\bar{g}(x) = g(x\alpha^{-1}, \alpha) = \sum_{i=0}^{d} \alpha^{-i} g_i(\alpha) x^i$. Since $f_e(\alpha) \neq 0$ and $g_d(\alpha) \neq 0$, we have that $\deg_x(\bar{f}) = e > 0$ and $\deg_x(\bar{g}) = d > 0$. Since the units of $R[x]$ are the same as the units of R by Proposition 2.30, neither $\bar{f}$ nor $\bar{g}$ are units of $R[x]$.

We have $h = h(x\alpha^{-1} \cdot \alpha) = \hat{h}(x\alpha^{-1}, \alpha) = \bar{f}\bar{g}$ in $R[x]$. So in $R[x]$ h is the product of two non-units, which contradicts the assumption that it is an irreducible. Thus, case (ii) cannot happen.

Case (iii): if $f \in R$, then the monomials which appear in g are the same as the monomials which appear in $\hat{h} = fg$. Write $h = \sum_{i=0}^{v} h_i x^i$ with $h_i \in R$ and $h_v \neq 0$; then $\hat{h} = \sum_{i=0}^{v} h_i y^i z^i$, and so $g = \sum_{i=0}^{v} \gamma_i y^i z^i$, with $h_i = f \cdot \gamma_i$ for all i.

Let $\bar{g} = \sum_{i=0}^{v} \gamma_i x^i \in R[x]$; so $h = f\bar{g} \in R[x]$. We assume that case (i) does not hold, and so $v > 0$, and so $\bar{g}$ is not a unit of $R[x]$. Since h is irreducible in $R[x]$, it follows that f is a unit of $R[x]$, hence a unit of R, and so is also a unit of $R[y, z]$.

Case (iv): this is the interesting case, in which we use the assumption that x does not divide h. In this case $f \in R[y]$ and $g \in R[z]$ are nonconstant. The constant coefficient of $\hat{h}$ is the same as the constant coefficient h_0 of h, which by assumption is nonzero. Since $fg = \hat{h}$, this implies that both the constant coefficient f_0 of f and the constant coefficient g_0 of g are nonzero, as $h_0 = f_0 g_0$. Let $d = \deg_y(g)$, and let f_d be the leading coefficient of f. Then $g_0 f_d z^d$ is a monomial of $fg = \hat{h}$, which is impossible, since the monomials of $\hat{h}$ are all of the form $h_i y^i z^i$, for $h_i \in R$. Thus case (iv) cannot happen either.

We still need to show that $a_{\sigma_{n+1}} \nmid p$.

Again, we consider the cases $Q_{n+1} = Q_n[b_{\sigma_n}^{-1}]$ and $Q_{n+1} = Q_n[a_{\sigma_{n+1}}, b_{\sigma_{n+1}}]$.

If $Q_{n+1} = Q_n[b_{\sigma_n}^{-1}]$, then $\sigma_{n+1} = \sigma_n^-$, write $a_1 = a_{\sigma_{n+1}}, b_1 = b_{\sigma_{n+1}}, a_2 = a_{\sigma_n}, b_2 = b_{\sigma_n}$.

Note that $a_2 b_2 = a_1$ so $a_2 b_2 \nmid p$ in Q_n. Suppose $a_1 \mid p$ in Q_{n+1}, so there is $\gamma \in Q_{n+1}$ such that $a_1 \cdot \gamma = p$, so $a_2 b_2 \cdot \gamma = p$. By Proposition 2.38, $\gamma = c/b_2^k$ for some $c \in Q_n$, $k \in \omega$. Then, $a_2 b_2 c = b_2^k p$, so $a_2 \mid b_2^k p$ in Q_n. By Proposition 2.50,

a_2 is irreducible in Q_n, by Proposition 4.21 Q_n is a UFD, so by Proposition 2.10 a_2 is prime in Q_n. Which means $a_2 \mid b_2^k$ or $a_2 \mid p$ in Q_n. The second is impossible by assumption, so $a_2 \mid b_2^k$ in Q_n, so $a_2 \mid b_2$. By Proposition 2.50, b_2 is irreducible in Q_n, so either a_2 is a unit of Q_n or $a_2 = b_2$. The first case is impossible by Proposition 2.48, and the second is impossible because a_2 is transcendental over R, by Construction 4.19.

Now suppose $Q_{n+1} = Q_n[a_{\sigma_{n+1}}, b_{\sigma_{n+1}}]$, where $\{a_{\sigma_{n+1}}, b_{\sigma_{n+1}}\}$ is independent over Q_n and $a_{\sigma_{n+1}} \cdot b_{\sigma_{n+1}} = a_{\sigma_n}$. If $a_{\sigma_{n+1}} \mid p$ in Q_{n+1}, then $a_{\sigma_{n+1}}\gamma = p$ for some $\gamma \in Q_{n+1}^\times$. From Construction 4.19, $Q_{n+1}^\times = Q_n^\times$, so $p\gamma^{-1} \in Q_n$, which means $a_{\sigma_{n+1}} \in Q_n$, a contradiction.

□

If an element is irreducible or prime in a ring in the sequence $\langle Q_i \rangle_{i\in\omega}$, then it is either a unit or an irreducible/prime in Q_ω.

Lemma 4.37. *If p is prime in some Q_n and $p \notin Q_\omega^\times$, with $a_{\sigma_n} \nmid_{Q_n} p$, then p is prime in Q_ω and no $a_\sigma \mid_{Q_\omega} p$, for any $\sigma \in T$.*

Proof. By induction on $m \geq n$ we see that p is prime in Q_m and a_{σ_m} does not divide p in Q_m. For if this holds for Q_m, then by Lemma 4.36 it holds for Q_{m+1}, unless p is a unit of Q_{m+1}. But in that case, p is a unit of Q_ω, which we assumed is not the case.

Now let $c, d \in Q_\omega$ and suppose that $p \mid cd$ in Q_ω. Let $m \geq n$ be sufficiently large so that $c, d \in Q_m$ and $p \mid cd$ in Q_m. Then $p \mid c$ or $p \mid d$ in Q_m, and so $p \mid c$ or $p \mid d$ in Q_ω. Hence p is prime in Q_ω.

Let $\sigma \in T$, and suppose that $a_\sigma \mid p$ in Q_ω. Since $a_\sigma \sim a_\tau$ for some nonterminal string τ by Lemma 4.31, we may assume that σ is non-terminal. Let $m \geq n$ be sufficiently large so that $\sigma \in T_m$ and a_σ divides p in Q_m. By Proposition 4.29 4.25, a_{σ_m} divides a_σ in Q_m, and so a_{σ_m} divides p in Q_m, contrary to what we just showed.

□

Any elements of Q_ω that are not divisible by an a_σ admit a prime factorization in Q_ω.

Proposition 4.38. If $p \in Q_\omega$ such that $a_\sigma \nmid_{Q_\omega} p$ for all $\sigma \in T$, then p has a prime decomposition in Q_ω.

Proof. If $p \in Q_n$ then $a_{\sigma_n} \nmid_{Q_n} p$. Since Q_n is a UFD, by Proposition 2.10 p has a prime decomposition in Q_n, $B = [p_i \mid i \leq t]$.

By Lemma 4.37 and since $a_{\sigma_n} \nmid p$ so $a_{\sigma_n} \nmid p_i$, each p_i is a prime or a unit of Q_ω.

□

In a ring, a sequence $(n_i)_{i\in\omega}$ *stabilizes* if there exists $k^* \in \omega$ such that for all $k \geq k^*$, $n_{k+1} = n_k$. If rather $n_{k+1} = un_k$ for some unit u, we say the sequence stabilizes *up to association*. If the ring is ω, we say the sequence is *increasing* if $n_{k+1} > n_k$ for all $k \in \omega$. We say the sequence is *non-increasing* if $n_{k+1} \leq n_k$ for all $k \in \omega$.

Proposition 4.39. Let $(n_i)_{i\in\omega}$ be a non-increasing sequence in ω. Then, this sequence stabilizes.

Proof. Suppose the sequence does not stabilize, so it has a subsequence $(m_j)_{j\in\omega}$ such that $m_k \neq m_t$ for $k \neq t$. Then, for $k > 1$, $m_k < n_0, m_{k+1} < n_0 - 1 \cdots m_{k+n_0} < 0$, a contradiction.

□

If an element a_σ is in Q_n and σ is a descendant of σ_n in T, then a_σ and the generator a_{σ_n} of Q_n are associates in Q_n.

Lemma 4.40. *If $a_\sigma \in Q_n$ and $\sigma_n \prec \sigma$ in T, then $a_{\sigma_n} \sim a_\sigma$ in Q_n.*

Proof. Let $\sigma \in T$. If $\sigma \in T_{m+1} \setminus T_m$ for some $m \geq n$, then $a_\sigma \in Q_{m+1} \setminus Q_m$. Hence, if $a_\sigma \in Q_n$ then $\sigma \in T_n$.

Suppose that $\sigma_n \prec \sigma$. Let k be the least such that $\sigma = \sigma_k$; since $\sigma \in T_n$ we have $k \leq n$, and since $\sigma \neq \sigma_n$ we have $k \neq n$, so $k < n$.

Let s be the least such that σ_s does not extend σ; then $s \leq n$. Then $\sigma_{s-1} = \sigma$ and $\sigma_s = \sigma^-$, and b_σ is a unit of Q_s. Hence b_σ is a unit of Q_n.

Now let $\sigma \in T_n$ properly extending σ_n, and write $\sigma_n = \tau_0, \tau_1, \cdots \tau_t = \sigma$, with $\tau_i = \tau_{i+1}^-$. By Proposition 4.29, $a_{\sigma_n} = a_\sigma \prod_{i=1}^{t} b_{\tau_i}$ in Q_k, where $\sigma \in T_k \setminus T_{k-1}$. Since $k < n$, this equation holds in Q_n as well, and by the argument just given, each b_{τ_i} for $i \geq 1$ is a unit of Q_n, and so $a_\sigma \sim a_{\sigma_n}$ in Q_n.

□

The generator a_{σ_n} of Q_n divides in Q_n any element a_σ that belongs to Q_n.

Proposition 4.41. If $a_\sigma \in Q_n$, then $a_{\sigma_n} \mid_{Q_n} a_\sigma$.

Proof. There are three cases to consider:

(i) $\sigma \preceq \sigma_n$,

(ii) $\sigma_n \prec \sigma$ and

(iii) $\sigma \mid \sigma_n$.

If (i) $\sigma \preceq \sigma_n$, by Proposition 4.29, the result follows.

If (ii) $\sigma_n \prec \sigma$, by Lemma 4.40, the result follows.

If (iii) $\sigma \mid \sigma_n$, by Proposition 4.13 σ is terminal. Take the longest non-terminal τ such that $\tau \prec \sigma$ and $\tau \preceq \sigma_n$. Since $\sigma \in T_n$, τ is the longest non-terminal initial segment of σ.

By Lemma 4.40, if $\tau = \sigma_m$ with $\sigma \in T_m$, a_τ and a_σ are associates in Q_m with $Q_m < Q_n$, hence they associate in Q_n.

By Proposition 4.29, $a_{\sigma_n} \mid a_\tau$. The result follows by transitivity.

□

If $d \in Q_n$ and the generator a_{σ_n} of Q_n does not divide d, it follows that no other a element divides d in Q_ω.

Proposition 4.42. Let Q_n be a ring in the sequence $(Q_i)_{i\in\omega}$. If for some $d \in Q_n$, $a_{\sigma_n} \nmid_{Q_n} d$, then for all $\delta \in T$ $a_\delta \nmid_{Q_\omega} d$.

Proof. Suppose $a_\delta \mid_{Q_\omega} d$. Then $a_\delta \mid_{Q_m} d$ for some $m \in \omega$ such that $m > n$. Since $a_\delta \in Q_m$, by Proposition 4.41 $a_{\sigma_m} \mid_{Q_m} a_\delta$, so $a_{\sigma_m} \mid_{Q_m} d$.

Let $d = up_1p_2 \cdots p_t$ be an irreducible factorization of d in Q_n. Since $a_{\sigma_n} \nmid_{Q_n} d$, we have $a_{\sigma_n} \nmid_{Q_n} p_i$ for $1 \leq i \leq t$, and by iterating Lemma 4.36 each p_i is either a unit of Q_m or irreducible in Q_m with $a_{\sigma_m} \nmid_{Q_m} p_i$. Since a_{σ_m} is irreducible in Q_m, $a_{\sigma_m} \nmid_{Q_m} d$, a contradiction.

□

Next, we give a general form for the elements of Q_ω. This will be useful when dealing with infinite descending chains in divisibility.

Lemma 4.43. *Every element of Q_ω is of the form da_σ^n for some $\sigma \in T$, $n \in \omega$ and $d \in Q_\omega$ not divisible by any a_τ.*

Proof. Let $q \in Q_\omega$; let $m \in \omega$ such that $q \in Q_m$. Let k be the greatest power of a_{σ_m} which divides q in Q_m; so $d = q/a^k_{\sigma_m} \in Q_m$ and a_{σ_m} does not divide $q/a^k_{\sigma_m}$ in Q_m. By Proposition 4.42, no a_τ divides d in Q_ω, and we have $q = d \cdot a^k_{\sigma_m}$ in Q_ω.

□

By an *infinite descending chain in divisibility* in a ring we mean a sequence $(c_i)_{i\in\omega}$ such that for all i, c_{i+1} *properly divides* c_i.

Any infinite divisibility descending sequence of Q_ω whose terms do not have an a_σ factor must stabilize.

Lemma 4.44. *Suppose $(c_i)_{i\in\omega}$ is a sequence of elements of Q_ω such that $c_{k+1} \mid c_k$, for all $k \in \omega$. Then, if for all $\sigma \in T$, $a_\sigma \nmid c_0$, there is some $k^* \in \omega$ such that for all $k \geq k^*$ $c_k \sim c_{k+1}$.*

Proof. Since for all $\sigma \in T$ $a_\sigma \nmid c_0$ and every c_k divides c_0, it follows that $a_\sigma \nmid c_k$ for all $k \in \omega$.

By Proposition 4.38, for all $k \in \omega$, $c_k \sim \prod B_k$ where $B_k = [p_{k,i} \mid i \leq n_k]$, for $n_k \in \omega$, where each $p_{k,i}$ is non-unit and prime.

By Proposition 2.12 we have $B_{k+1} \subseteq B_k$ up to association, and since each B_k is finite, the sequence $|B_k|$ must stabilize; hence the sequence $(c_i)_{i\in\omega}$ stabilizes up to association.

□

An essential ingredient to our proof: an infinite descending chain in divisibility of Q_ω must compute the Halting Problem.

Proposition 4.45. Any infinite descending chain in divisibility of Q_ω computes $\emptyset'$.

Proof. Let $(c_i)_{i\in\omega}$ be such a chain. We claim we can write non-effectively each c_k as $c_k = d_k \prod_{b\in B_k} b \cdot a^{m_k}_{\epsilon_k}$, where B_k is a multiset of elements b_σ, for σ non-terminal, and d_k is not divisible in Q_ω by any a_σ and by any b_σ with σ non-terminal.

By Lemma 4.43 there is some d'_k and some $\epsilon_k \in T$ and $m_k \in \omega$ such that no a_σ divides d'_k in Q_ω and such that $c_k = d'_k a^{m_k}_{\epsilon_k}$.

By Proposition 4.38, d'_k has a prime decomposition D'_k in Q_ω. Let B_k be the multiset of primes $p \in D'_k$ such that $p \sim b_\sigma$ for some non-terminal $\sigma \in T$.

Then let $d_k = \prod(D'_k \setminus B_k) = d'_k / \prod B_k$.

We claim $d_{k+1} \mid d_k$. Take m sufficiently large so Q_m contains $d_k, d_{k+1}, a_{\epsilon_k}, a_{\epsilon_{k+1}}$ and each element of B_k and B_{k+1} such that $c_{k+1} \mid_{Q_m} c_k$ and σ_m is a correct string with $\sigma_m \notin T_{m-1}$. Then for all σ with $b_\sigma \in Q_m$, σ is correct if and only if $\sigma \preceq \sigma_m$ if and only if b_σ is prime in Q_m; if $b_\sigma \in Q_m$ and $\sigma \not\preceq \sigma_m$ then b_σ is a unit of Q_m.

In Q_m, let D_k and D_{k+1} be prime decompositions of d_k and d_{k+1} respectively, and let A_k and A_{k+1} be prime decompositions of $a_{\epsilon_k}^{m_k}$ and $a_{\epsilon_{k+1}}^{m_{k+1}}$ respectively. So $A_k \cup B_k \cup D_k$ is a a prime decomposition of c_k in Q_m, and similarly for $k+1$. So $c_{k+1} \mid_{Q_m} c_k$ means that $A_{k+1} \cup B_{k+1} \cup D_{k+1}$ is a subset of $A_k \cup B_k \cup D_k$ up to association. Now all the primes which appear in $A_k \cup B_k$ (and in $A_{k+1} \cup B_{k+1}$) are associates of either a_{σ_m} or b_σ for some $\sigma \preceq \sigma_m$, and no such primes can occur in D_k or in D_{k+1}. Hence we can conclude that $D_{k+1} \subseteq D_k$ up to association, and so $d_{k+1} \mid d_k$ in Q_m, and so $d_{k+1} \mid d_k$ in Q_ω. We also see that a_{σ_m} does not appear in $B_k \cup D_k$ (or $B_{k+1} \cup D_{k+1}$) but appears (up to association) with multiplicity m_k in A_k, and m_{k+1} in A_{k+1}. Then the fact that $A_{k+1} \cup B_{k+1}$ is a subset of $A_k \cup B_k$ (up to association) implies that $m_{k+1} \leq m_k$.

Write $c'_k = c_{k+K}/d_K$ and note that $\langle c_k \rangle$ computes the sequence $\langle c'_k \rangle$. To avoid excess notation, write c_k instead of c'_k, and it remains to show that the new $\langle c_k \rangle$ computes $\emptyset'$.

For the multiset B of elements of T, if $S = [\sigma \mid b_\sigma \in B]$, we write $B(S) = B$.

Claim (i). Let S be a finite multiset of strings from T and let $\rho \in T$. We claim there exist S' and and ρ' such that:

(a) all of the strings in $S' \cup [\rho']$ are comparable, and

(b) $a_{\rho'}$ and a_ρ are associates in Q_ω, and

(c) $\prod_{b \in B(S)} b$ associates with $\prod_{b \in B(S')} b$ in Q_ω.

Proof: let R be the collection of initial segments of strings in $S \cup [\rho]$, so R is a finite subtree of T. Let τ be the rightmost leaf of R. Then, every $\sigma \in R$

which is not extended by τ is terminal, hence by Lemma 4.28, b_σ is a unit of Q_ω. We let $S' = [\sigma \cap \tau \mid \sigma \in S]$ and let $\rho' = \rho \cap \tau$.

Let S and S' be multisets of strings of T and let $\rho, \rho' \in T$.

Claim (ii). There is a multiset $\bar{S}$ of strings of T and a string $\bar{\rho} \in T$ such that:

(a) $a_{\rho'}^{m_k} \cdot \prod B(S') \sim a_{\bar{\rho}}^{m_k} \prod B(\bar{S})$,

(b) for all $\sigma \in \bar{S}$, $\sigma \preceq \bar{\rho}$ and

(c) either $\rho' \preceq \bar{\rho}$ or ρ' lies lexicographically to the left of $\bar{\rho}$, i.e. if $\sigma = \rho' \cap \bar{\rho}$ then $\sigma^\frown 0 \preceq \rho'$ and $\sigma^\frown s \preceq \bar{\rho}$ for some $s > 0$.

Proof: let R be the collection of initial segments of $S \cup S' \cup [\rho, \rho']$. Let τ be the rightmost leaf of R. Let $\bar{\rho} = \tau$ and let $\bar{S} = [\sigma \cap \tau \mid \sigma \in S'] \cup m_K \cdot [\sigma \mid (\rho' \cap \tau) \prec \sigma \preceq \tau]$.

Using this claim we can find, computably from $\langle c_k \rangle$, by recursion a sequence $\langle S_k, \rho_k \rangle$ such that for all k:

(a') $s_k \sigma_{\rho_k}^{m_k} \prod B(S_k)$,

(b') for all $\sigma \in S_k$, $\sigma \preceq \rho_k$, and

(c') either $\rho_k \preceq \rho_{k+1}$ or ρ_k lies lexicographically to the left of ρ_{k+1}.

Let $\eta_k = \rho_k \cap \rho_{k+1}$, and let $\bar{\rho}_k$ be longest correct initial segment of ρ_k. Note that the sequence $\langle \eta_k \rangle$ is computable from $\langle c_k \rangle$.

Property (c') above implies that $\bar{\rho}_k \preceq \eta_k$: this certainly holds if $\rho_k \preceq \rho_{k+1}$, otherwise, because ρ_{k+1} witnesses that $\eta_k^\frown 0 \preceq \rho_k$ is terminal. Hence $\bar{\rho}_k \preceq \bar{\rho}_{k+1}$, as $\bar{\rho}_k$ is a correct initial segment of ρ_{k+1}.

Further, we note that property (b') above implies that $\rho \in S_k$ is correct if and only if $\rho \preceq \bar{\rho}_k$. Let $\bar{S}_k = [\sigma \in S_k \mid \sigma \preceq \bar{\rho}_k]$, then $c_k \sim a_{\bar{\rho}_k}^{m_K} \prod B(\bar{S}_k)$.

Note that in the model of RCA_0 in which we work, the sequence $\langle \bar{S}_k \rangle$ may not exist, but it is definable.

Claim (iii). For all $\sigma \preceq \bar{\rho}_k$, $m_\sigma(S_{k+1}) \leq m_\sigma(S_k)$.

Proof: let n be large, so that $c_{k+1} \mid c_k$ in Q_n and all the elements mentioned are in Q_n. Since $\bar{\rho}_{k+1}$ is correct, it is an initial segment of σ_n. Let A_k be an irreducible factorization of $a_{\bar{\rho}_k}^{m_K}$ in Q_n, so $A_k \cup B(\bar{S}_k)$ is an irreducible factorization of c_k in Q_n. We also have that $B(\bar{S}_{k+1})$ is a set of

primes of Q_n and $\prod B(\bar{S}_{k+1}) \mid c_k$ in Q_n, as $\prod B(\bar{S}_{k+1}) \mid c_{k+1}$ in Q_n, and so $B(\bar{S}_{k+1}) \subseteq A_k \cup B(\bar{S}_k$ up to association. However, for $\sigma \preceq \bar{\rho}_k$, $b_\sigma \notin A_k$, as $b_\tau \in A_k$ implies $\bar{\rho}_k \prec \tau$. Hence $m_\sigma(\bar{S}_{k+1}) \leq m_\sigma(\bar{S}_k)$. Since $\sigma \preceq \bar{\rho}_k, \bar{\rho}_{k+1}$, $m_\sigma(S_k) = m_\sigma(\bar{S}_k)$ and similarly for $k+1$.

Claim (iv). If η_k is not correct, then there is some correct $\sigma \preceq \eta_k$ such that $m_\sigma(S_k) < m_\sigma(S_{k+1})$.

Proof: the assumption implies that $\bar{\rho}_k = \bar{\rho}_{k+1}$ is a proper initial segment of η_k, and so

$$a_{\bar{\rho}_k}^{m_K} \cdot \prod B(\bar{S}_k) \sim c_k \mid c_{k+1} \sim a_{\bar{\rho}_{k+1}}^{m_K} \cdot \prod B(\bar{S}_{k+1})$$

implies that

$$\prod B(\bar{S}_k) \mid \prod B(\bar{S}_{k+1}),$$

and the division is proper. However, if for all $\sigma \preceq \bar{\rho}_k$ we have $m_\sigma(S_k) \leq m_\sigma(S_{k+1})$, then by Claim (iii) we would have $\bar{S}_k = \bar{S}_{k+1}$, so the division would not be proper.

Now define a string ζ_k as:

$\zeta_k = \eta_k$ if for all $\sigma \preceq \eta_k$, $m_\sigma(S_{k+1}) = m_\sigma(S_k)$. Otherwise, let ζ_k be the shortest initial segment σ of η_k such that $m_\sigma(S_{k+1}) < m_\sigma(S_k)$. Claim (iv) implies each ζ_k is correct. It follows that the strings ζ_k are pairwise comparable.

Now define the string μ_k as the longest string in $\{\zeta_j \mid j \leq k\}$. So each μ_k is correct and $\mu_k \preceq \mu_{k+1}$.

Claim (v). Suppose that $\zeta_k = \eta_k$ and $m_{\eta_k}(S_k) = m_{\eta_k}(S_{k+1})$. In other words for all $\sigma \preceq \eta_k$ we have $m_\sigma(S_k) = m_\sigma(S_{k+1})$. Then $\bar{\rho}_{k+1} \succ \eta_k$.

Proof: suppose for a contradiction that $\bar{\rho}_{k+1} = \eta_k = \bar{\rho}_k$. The assumption on k implies that $\bar{S}_k = \bar{S}_{k+1}$. And then:

$$c_k \sim a_{\bar{\rho}_k}^{m_K} \prod B(\bar{S}_k) = a_{\bar{\rho}_{k+1}}^{m_K} \prod B(\bar{S}_{k+1}) \sim c_{k+1},$$

contrary to our assumption that the division $c_{k+1} \mid c_k$ is proper.

Claim (vi). For all $k \in \omega$, for all $m \geq k$, $\bar{\rho}_k \preceq \rho_m$.

Proof: by induction on $m \geq k$. Note that the sequence $\langle \rho_m \rangle_{m \geq k}$ exists, and so the statement is both Σ_1 and Π_1 as $\bar{\rho}_k$ is fixed.

For the base case, $m = k$ and note that $\bar{\rho}_k \preceq \bar{\rho}_m$. Let $m \geq k$ and suppose $\bar{\rho}_k \preceq \rho_m$. Since $\bar{\rho}_k$ is correct, we have $\bar{\rho}_k \preceq \bar{\rho}_m$. We know that $\bar{\rho}_m \preceq \bar{\rho}_{m+1} \preceq \rho_{m+1}$ so $\bar{\rho}_k \preceq \rho_{m+1}$.

It follows that for all k, for all $m \geq k$, $\zeta_k \preceq \rho_m$, so $\zeta_k \preceq \bar{\rho}_m$. It then follows that for all k, $\mu_k \preceq \rho_k$, since $\mu_k = \zeta_j$ for some $j \leq k$. Since μ_k is correct, $\mu_k \preceq \bar{\rho}_k$.

Claim (vii). For all $\sigma \preceq \mu_k$, $m_\sigma(S_k) \geq m_\sigma(S_{k+1})$.

Proof: immediate from Claim (iii), since $\mu_k \preceq \bar{\rho}_k$.

Claim (viii). Now let $k \in \omega$ and $n = |S_k| + 3$. We claim $|\mu_{k+n}| > |\mu_k|$.

Proof: we see that $n > |S_k| + 2$ together with Claim (vii) implies that there are at least two $i, j \in \{k, k+1, \cdots, k+n-1\}$ such that for all $\sigma \preceq \mu_k$, $m_\sigma(S_i) = m_\sigma(S_{i+1})$ and similar for j. If $\eta_i \succ \mu_k$ then $\zeta_i \succ \mu_k$ and we are done. Otherwise, $\eta_i = \mu_i$ and by Claim (vi) $\bar{\rho}_{i+1} \prec \mu_i$. By Claim (vi), $\bar{\rho}_{i+1} \preceq \bar{\rho}_j$, and we know that $\bar{\rho}_j \preceq \eta_j$, so $\eta_j \succ \mu_k$, and so $\zeta_j \succ \mu_k$, and we are done.

Now we know that for all i there is some $j > i$ such that $\mu_i \prec \mu_j$. By recursion we define a sequence $\langle \mu'_k \rangle$; given $\mu'_k = \mu_i$ for some i, we let $\mu'_{k+1} = \mu_j$ for some $j > i$ such that $\mu_i \prec \mu_j$. Then $\mu'_k \prec \mu'_{k+1}$, and so by Lemma 4.17, $\langle \mu'_k \rangle$ computes $\emptyset'$. This completes our proof.

□

We now put all of our previous work together to show that there exists a ring that satisfies the conditions of the contrapositive of Theorem 1.3 and some sequence in the ring computes the Halting Problem.

Proposition 4.46 (RCA_0)**.** There exists a computable integral domain Q, not Atomic, such that any sequence $\langle c_i \rangle_{i \in \omega}$ from Q, with c_{k+1} properly dividing c_k for all k, computes $\emptyset'$.

Proof. Let $Q = Q_\omega$. By Proposition 4.35, it is non-Atomic. By Proposition 4.45, any chain $\langle c_i \rangle_{i \in \omega}$ of Q with c_{k+1} properly dividing c_k computes $\emptyset'$. □

Finally, we obtain our desired result.

Theorem 4.47 (RCA_0)**.** *Theorem 1.3 is equivalent to* ACA_0.

Proof. The proof of Theorem 1.3, carried in ACA_0 provides the first direction of the equivalence.

Let M be a model of RCA_0+ Theorem 1.3. Let $X \in M$, we show X' exists. Note that M is closed under Turing reducibility. In M, from Proposition 4.46 and X, obtain an X-computable ring Q which is non-Atomic and if $\langle c_i \rangle_{i \in \omega}$ from Q with $\forall k \; c_{k+1} \mid c_k$ and they do not associate then $X \oplus \langle c_i \rangle \geq_T X'$.

By Theorem 1.3, there is such a sequence in M. So $X' \in M$. This shows Theorem 1.3 implies ACA_0. □

This concludes our proof. We have shown that Theorem 1.3 is equivalent to ACA_0, over the base system RCA_0.

4.4 Conclusion

We have investigated the proof-theoretic strengths of Theorems 1.2 and 1.3. We have found that Theorem 1.2 is provable within RCA_0 and that Theorem 1.3 is equivalent to ACA_0 over the base system RCA_0.

The proof of Theorem 1.2 in RCA_0 is straight-forward and relies on a Σ_1-induction argument. A good open question here would be establishing an equivalence between RCA_0 and Theorem 1.2 over a weaker base system.

The proof of the equivalence with ACA_0 was accomplished by proving Theorem 4.46, which gives a non-Atomic integral domain in which any descending chain in divisibility computes $\emptyset'$. The conjunction of this result and Theorem 1.3 proves the existence of $\emptyset'$ in any ω-model of RCA_0+ Theorem 1.3.

One thing to notice here is that the direct proof in ACA_0 of Theorem 1.3 uses $\emptyset''$ as an oracle, so it is natural to ask whether a version of Theorem 4.46 that implies the existence of $\emptyset''$ holds. Hence, we state this as a question.

Question 4.48. *Does there exist a computable integral domain Q, non-Atomic, such that any sequence $\langle c_i \rangle_{i \in \omega}$ from Q, with c_{k+1} properly dividing c_k for all k, computes $\emptyset''$?*

Bibliography

[1] D. Bridges and F. Richman, *Varieties of Constructive Mathematics*. Lon. Math. Soc. Lec. Ser., 97, Cambridge University Press, Cambridge, 1987.

[2] J. Coykendall and M. Zafrullah, *AP-domains and unique factorization*. J. of Pure and App. Algebra, 189, (2004), 27-35.

[3] C. J. Conidis, *Chain Conditions in Computable Rings*. Trans. Amer. Math. Soc., 362, (2010), 6523-6550.

[4] R. G. Downey, S. Lempp and J. R. Mileti, *Ideals in Computable Rings*. J. Algebra, 314, (2007), 872-887.

[5] R. G. Downey and D. R. Hirschfeldt, *Algorithmic Randomness and Complexity*. Springer-Verlag 2010.

[6] H. M. Friedman, S. G. Simpson and R. L. Smith, *Countable Algebra and Set Existence Axioms*. Ann. of Pure and App. Logic, 25, (1983), 141-181.

[7] A. Fröhlich and J.C. Sheperdson, *On the factorization of polynomials in finite number of steps*. Math. Z., 62, (1955), 331-334.

[8] A. Fröhlich and J.C. Sheperdson, *Effective procedures in field theory*. Philos. Trans. Royal Soc. London Ser. A, 248, (1956), 407-432.

[9] J. A. Gallian, *Contemporary Abstract Algebra*. Houghton Mifflin Company, Boston, 2nd edition, 2006.

[10] A. Grams, *Atomic Rings and the Ascending Chain Condition for Principal Ideals*. Proceedings of the Cambridge Philosophical Society, 75, (1974), 321-329.

[11] K. Hatzikiriakou, *Commutative algebra in subsystems of second order arithmetic*. PhD Thesis, Penn. State University, 1989.

[12] M. Kneser, *Bemerkung über die Primpolynomzerlegung in epdlich vielen Schritten*. Math. Z., 57, (1953), 238-240.

[13] S. Lang, *Undergraduate Algebra*. Undergraduate texts in mathematics, Springer, 2004.

[14] A. I. Mal'cev, *Constructive algebra I*. Russ. Math. Surv., 16, (1961), 77-129.

[15] G. Metakides and A. Nerode, *Effective content of field theory*. Ann. Math. Logic, 17, (1979), 289-320.

[16] R. Mines, F. Richman and W. Ruitenburg, *A course in constructive algebra*. Springer, New York, 1988.

[17] A. Montalbán, *Open Questions in Reverse Mathematics*. manuscript, 2010.

[18] J. Mott, *The Theory of Divisibility*. in *Factorization in Integral Domains*, Marcel Dekker Inc., New York, 1997.

[19] A. Nerode and N. Greenberg *The theory of the donut. Elliptic curves for undergraduates*. manuscript, 2012.

[20] M. O. Rabin, *Computable algebra, general theory and theory of computable fields*. Trans. Amer. Math. Soc., 95, (1960), 341-360.

[21] M. O. Rabin, *Computable algebraic systems*, in *Summer Institute for Symbolic Logic, Cornell University*. Institute for Defence Analyses, 1957.

[22] J. Rao and S.G. Simpson, *Factorization in subsytems of second order arithmetic*, quoted in *Handbook of Recursive Mathematics*. Elsevier, 1998.

[23] S. G. Simpson, *Subsystems of Second Order Arithmetic*. Cambridge University Press, 2nd edition, 2010.

[24] S. G. Simpson and J. Rao, *Reverse Algebra*, in *Handbook of Recursive Mathematics*. Elsevier, 1998.

[25] S. G. Simpson and R. L. Smith, *Factorization of polynomials and Σ_1^0 Induction*. Ann. Pure Appl. Logic, 31, (1986), 289-306.

[26] V. Stoltenberg-Hansen and J. V. Tucker, *Computable rings and fields*, in *Handbook of Computability Theory*. Elsevier, 1999.

[27] R. I. Soare, *Recursively Enumerable Sets and Degrees*. Springer-Verlag, New York, 1987.

[28] D. R. Solomon, *Reverse Mathematics and Ordered Groups*. PhD Thesis, Cornell University, 1998.

[29] B.L. van der Waerden, *Eine Bemerkung über die Unzerlegbarkeit von Polynomen*. Math. Ann., 102, (1930), 738-739.