Reverse Mathematics and Countable Algebraic Systems

A thesis presented
by

Takashi SATO

to
The Mathematical Institute
for the degree of
Doctor of Science

Tohoku University
Sendai, Japan

November 2016

Abstract

This thesis is a contribution to the foundation of mathematics, especially to the *Reverse Mathematics* program, whose core question is "What are the appropriate axioms to prove each mathematical theorem?" The main targets of this thesis are countable algebraic systems and its theories in second order arithmetic. This thesis establishes that several theorems and the existence of objects of countable algebraic systems are equivalent to specific set existence axioms—arithmetical comprehension or weak König's lemma. These equivalences are proven within RCA_0, a subsystem of arithmetic mainly consisting of recursive comprehension and Σ^0_1 induction. Weak König's lemma is a non-constructive (however, strictly weaker than arithmetical comprehension) set existence axiom which asserts that every infinite 0-1 tree has a path.

In Chapter 3, we develop countable order theory in second order arithmetic. We prove within RCA_0 that a countable version of the Abian-Brown least fixed point theorem, Davis' converse, Markowsky's converse, and arithmetical comprehension are pairwise equivalent. We also show that a countable version of the Knaster-Tarski fixed point theorem, the Tarski-Kantorovitch fixed point theorem, and the Bourbaki-Witt fixed point theorem are provable within RCA_0.

In Chapter 4, we develop countable semigroup theory in second order arithmetic. We prove within RCA_0 that Isbell's zig-zag theorem for countable monoids is equivalent to weak König's lemma, and that the existence of dominions is equivalent to arithmetical comprehension. We also show that the Rees theorem for countable semigroups is implied via arithmetical comprehension.

In Chapter 5, we develop countable group theory in second order arithmetic. We prove within RCA_0 that the existence of essential closures (as known as neat hulls), normalizers, and abelianizers (as known as derived subgroups or commutator groups) are equivalent to arithmetical comprehension. We also show that characterizations of normalizers and ablianizer are equivalent to weak König's lemma.

In Chapter 6, we develop countable commutative ring theory or ideal theory in second order arithmetic. We show within RCA_0 that the existence of the sum, the product, the quotient, and the radical of two ideals is equivalent to arithmetical comprehension. We also show that the Lasker-Noether primary ideal decomposition theorem for countable commutative rings is implied via arithmetical comprehension.

Acknowledgments

Yamazaki Takeshi *sensei* is who taught me "What is *doing* mathematics?"
I am in debt to all the member of Sendai Logic Group.
I appreciate comments from Prof. S. G. Simpson, Prof. K. Tanaka, and Asst. Prof. K. Yokoyama.
I thank all my family, friends, lovers, and possible gods whom I have met in my life.
Finally, this thesis is dedicated to two H's.

Contents

0 Introduction

Foundation of Mathematics

The naive and personal motivation for this research is to answer "What is mathematics?" How are mathematical activities justified? For example, we collect—and sometimes even infinitely repeat collecting—infinite things to construct a set. But how?

Such questions are not ridiculous but philosophical. For practical reasons, some mathematicians at the beginning of the 20th century were forced to encounter such problems. The discovery of paradoxes such as Russell's paradox caused the foundational crisis of mathematics (cf. the explanation of [22]). A method taken at the time was, interestingly enough, very mathematical; they reconsidered mathematics itself as mathematical objects.

Mathematical language, mathematical statements, mathematical axioms, and logical rules were formalized and investigated mathematically; this idea led to *proof theory*. Simultaneously, *recursion theory*, *model theory*, and *set theory* arose by the need—*metamathematics* emerged.

A *formal system* is a formalization of (a part of) the playground of mathematics in which formalized mathematics is developed. ZFC (Zelmelo-Fraenkel set theory with axiom of choice), for example, is designed to develop the entire mathematics avoiding paradoxes. On the other hand, PA (first order Peano arithmetic) is a small formal system which is designed to develop arithmetic. Within PA, finite group theory etc. can be developed due to the expressive ability equipped by natural numbers (via a *coding* method, cf. [25]). However, if we hope to capture the systematic treatment of *actual infinity* in modern mathematics, the formal system must at the very least equip the language which can express sets of natural numbers as mathematical objects. Z_2 (second order arithmetic) is a minimal formal system in the sense above. Axioms of Z_2 consist of (i) basic axioms for order, addition, and multiplication, (ii) induction axiom, and (iii) comprehension axiom. The comprehension axiom asserts the existence of all sets definable in the language of second order arithmetic. The expressive ability of this minimal formal system is much richer than first order arithmetic. In fact, the bulk of modern mathematics can be developed within Z_2 (cf. [3]). Moreover, a smaller subsystem of Z_2 suffices to formalize and prove each individual theorem such as the mean value theorem, Isbell's zig-zag theorem, and so on. A subsystem of Z_2 is obtained by restricting the scheme of induction or comprehension axiom to a smaller class of formulae.

Reverse Mathematics

It was Harvey Friedman who gave insight to *Reverse Mathematics*;

> When the theorem is proved from the right axioms, the axioms can be proved from the theorem ([15]).

He provided a classification of mathematical theorems according to their logical strength. Five subsytems RCA, WKL, ACA, ATR, and Π^1_1-CA (put in weak order, so-called "big five") with each characteristic axiom were presented. It is noteworthy that (i) it is only five that remarkably many theorems are classified into, (ii) theorems are collected from a wide range of mathematics, and (iii) each subsystem can be viewed as a formalization of a standpoint of mathematics. RCA is a system of recursive comprehension and corresponds to "computable mathematics". WKL is characterized by a non-constructive axiom *weak König's lemma* which asserts that "We may take a path of any infinite 0-1 tree." It may be seen as a formalization of Hilbert's formalism; in fact weak König's lemma is known to be equivalent to Gödel's completeness theorem, which asserts that every consistent theory has a model, see [22, page 124]. ACA is an acronym of arithmetical comprehension axiom and corresponds to Weyl's predicativism (cf. [73]). We could say that WKL and ATR have become to draw attention after discovering of Reverse Mathematics phenomenon.

Under the leadership of S. G. Simpson, Kazuyuki Tanaka, et al., *Reverse Mathematics program* have been proceeding since the 1980s (cf. [61] and [69]). This thesis is along this line of research. The main results of this thesis is that theorems of countable algebra or the existence of countable algebraic objects are equivalent to weak König's lemma or arithmetical comprehension over RCA_0. (The subscript 0 means the restriction of induction.)

The main targets of this thesis are *countable* algebraic systems and their theories within second order arithmetic. Uncountable algebraic systems are not expressive within second order arithmetic in a straightforward way. It does not necessarily deny the possibility of development of uncountable mathematics within second order arithmetic. In fact, theories of real numbers or complete separable metric spaces are developed in a nice way since we can reduce their essential properties to those of countable objects. However, exploring distinction between countable and uncountable algebraic systems is by itself a big theme of study, so this thesis simply focuses on countable ones. It is nice to study closely how proofs can be simplified when we focus on countable ones. Reverse Mathematics has a proof theoretical side where we examine how an axiom eventually works in a proof, or seek a new or hidden proof. Like Ockham's razor, we omit unnecessary axioms to save costs. Reverse Mathematics of countable algebraic systems enjoys the spirit of Reverse Mathematics.

Reverse Mathematics today

The number of examples of Reverse Mathematics have been increasing today. However, the research of Reverse Mathematics should be not only quantitative but qualitative. What makes "big five" so important? Are "big five" really robust? Recently, variants on Ramsey theorem for pairs and some combinatorial principles turn out not to be classified into "big five" (cf. [29]). Discoveries of other similar examples in various area of mathematics may bring a big change in Reverse Mathematics program. Chapter 3 was originally motivated to seek an atypical example of Reverse Mathematics. Contrary to expectations, the research revealed that many fixed point theorems for countable posets are proven or equivalent to arithmetical comprehension within RCA_0. This result supports the predominance of "big five".

"Orthodox" Reverse Mathematics adopts a weak subsystem RCA_0, in which induction axiom is restricted to Σ^0_1 formulae, as a base theory. Recently, Reverse Mathematics program counts many branches beside "orthodox" one; (i) Simpson and Smith [63] proposed to weaken a base theory to $\mathsf{RCA}_0{}^*$, in which induction axiom is restricted to Σ^0_0 induction, and redo Reverse Mathematics even for Σ^0_1 induction, (ii) Kohlenbach's group [42] runs Higer Order Reverse Mathematics, (iii) Ishihara's group [37] runs Constructive Reverse Mathematics, (iv) Cook and Nguyen's group [10] runs Bounded Reverse Mathematics.

Reverse Mathematics has been providing new viewpoints on recursion theory and set theory. Especially, it is closely related to recursive mathematics. A typical proof that the existence of some algebraic system implies arithmetical comprehension over RCA_0 is to recursively construct an appropriate algebraic system which encodes the image of an arbitrarily given function. According to this method, one can construct a computable algebraic system with a Σ^0_1 complete accompanying system. Thus, one can obtain the corresponding result of recursive algebra from a result of this thesis.

Calibrating the level of abstraction

All theories and theorems investigated in this thesis were presented in the first half of the 20th century and now we refer them to standards. The following describes the current of algebra in the time.

> "The recent expansion of algebra far beyond its former bounds is mainly due to the "abstract", "formal", or "axiomatic" school. This school has created a number of novel concepts, revealed hitherto unknown interrelations, and led to far-reaching results especially in the theory of *fields* and *ideals*, of *groups*, and *hypercomplex numbers*. The chief purpose of this book is to introduce the reader this whole world of concepts. Within the scope of these modern ideas classical results and methods will find their due place." (van der Warden "Modern Algebra" [72] 1930).

We think that rings of integers of algebraic number fields are more "abstract" objects than the ring of rational integers, that Noetherian rings are more "abstract" objects than rings of integers of algebraic number fields, and so on. The fundamental theorem of arithmetic (which asserts that every integer grater than 1 is a product of prime numbers) for the ring of rational integers is extended to the prime ideal decomposition theorem for rings of integers of algebraic number fields. The prime ideal decomposition theorem is furthermore extended to primary ideal decomposition theorem for Noetherian rings. Does a theorem become more "abstract" when generalized to more abstract objects? Reverse Mathematics presents a mathematical measure to calibrate how "abstract" a theorem is. It is expected that ideal decomposition theorems are equivalent to a more strong axiom than the fundamental theorem of arithmetic. (This research is ongoing, see Section 6.5.) Reverse Mathematics can capture the small history of mathematics.

Background of this thesis

The earliest literature on Reverse Mathematics of algebra is Friedman, Simpson, and Smith [16] (1983), in which they gave several equivalences between "big five" and theorems of field theory, ring theory, and group theory. (This paper has an addendum [17].) Simpson and Smith [63] (1986) and Hatzikiriakou [26] (1989) presented some Reverse Mathematics of algebra for RCA_0 over ${\mathsf{RCA}_0}^*$. Simpson [60] showed that Hilbert basis theorem is equivalent over RCA_0 to the assertion that the ordinal number ω^ω is well ordered. This is a remarkable example of Reverse Mathematics which is not classified into any of "big five". Solomon [65, 66] (1998, 1999) presented Reverse Mathematics of ordered group theory. Hatzikiriakou [27] (2005) showed that the existence of integral closure of a countable ring is equivalent to arithmetical comprehension over RCA_0. In the same paper he developed some theory of prime ideals within WKL_0. Downey et al. [14] (2007) showed that the existence of nontrivial proper ideal of countable commutative ring which is not a field is equivalent to weak König's lemma over RCA_0. This is a generalization of the theorem in [16] that the existence of nontrivial proper *prime* ideal of a countable commutative ring is equivalent to weak König's lemma over RCA_0. They showed a similar result on countable vector spaces in [13]. Conidis [8, 9] (2010, 2012) developed theory of Artinian rings within WKL_0 and gave equivalences between some statements and WKL_0. Frittaion and Marcone [18] (2013) presented some Reverse Mathematics of ordered theory.

Plan of this thesis

This thesis presents Reverse Mathematics of countable order theory, semigroup theory, group theory, and commutative ring theory.

In Chapter 1, after providing several axiom schemes, we give rigorous definitions of the system RCA_0, WKL_0, ACA_0, and stronger systems. The reader who is already familiar with these popular subsystems of second order arithmetic may skip directly to any other chapters.

Chapter 2 discusses general properties of countable sets, relations, and functions from the standpoint of Reverse Mathematics. Results in this chapter will find application throughout the rest of the thesis. A part of the work in this chapter appears in [21].

In Chapter 3 we do Reverse Mathematics of order theoretic fixed point theorems. We show that RCA_0 proves a countable version of the Knaster-Tarski fixed point theorem, the Tarski-Kantorovitch fixed point theorem, and the Bourbaki-Witt fixed point theorem. We also show within RCA_0 that a countable version of the Abian-Brown least fixed point theorem, Davis' converse, Markowsky's converse, and arithmetical comprehension are pairwise equivalent. These converses state that some fixed point properties characterize the completeness of underlying spaces. Our results show that it is arithmetical comprehension that makes the notion of completeness work as an intended way to develop the countable fixed point theory.

In Chapter 4 we do Reverse Mathematics of countable semigroup theory. We show that Isbell's zig-zag theorem for countable monoids is equivalent to WKL_0 over RCA_0. We note that Isbell's zig-zag theorem for countable monoids is of the form

$$(\forall x \in M)(\varphi(M, x) \leftrightarrow \psi(M, x)) \tag{$\natural$}$$

where M is any countable monoid, φ is Π^0_1 and ψ is Σ^1_1. We present several analogous results in Chapter 5 and 6. We also show that the existence of dominions is equivalent to ACA_0 over RCA_0 and that the Rees theorem is provable within ACA_0. A part of the work in this chapter appears in [54].

In Chapter 5 we do Reverse Mathematics of countable group theory. The work of Section 5.1 is strongly influenced by [13, 14]. We show the analog of their results; over RCA_0, WKL_0 is equivalent to the assertion that every countable group which is not a cyclic group of prime order has a nontrivial proper subgroup. We also show that the existence of essential closures , normalizer, and abelianizer is respectively equivalent to ACA_0 over RCA_0. Moreover, we show that characterizations for normalizers and abelianizers is respectively equivalent to WKL_0 over RCA_0. Note that these characterizations are of the form $\natural$.

In Chapter 6 we do Reverse Mathematics of countable commutative ring theory or ideal theory. We show that the existence of the sum, the product, the quotient, the radical of given two ideals is equivalent to ACA_0 over RCA_0. We also see that a characterization of nilradicals, which is again of the form $\natural$, is equivalent to WKL_0 over RCA_0. Finally, the theory of commutative rings with ascending chain conditions is developed within ACA_0.

1 Subsystems of Second Order Arithmetic

In this chapter we briefly summarize the characters and properties of subsystems of second order arithmetic. We provide some axiom schemes and give rigorous definitions of systems which are used in this thesis. For more information for subsystems of second order arithmetic, see Simpson [61].

The formal system of second order arithmetic Z_2 is a two-sorted first-order predicate logic. The language of second order arithmetic L_2 consists of countably infinite number variables $i, j, k, l, m, n, x, y, z, \ldots$ and set variables $X, Y, Z, \ldots$, two distinct constant symbols 0 and 1, two 2-ary function symbols $+$ and $\cdot$, and three 2-ary relation symbols $=$, $<$, and $\in$. *Numerical terms* are number variables, the constant symbols 0 and 1, and $t + s$ and $t \cdot s$ whenever t and s are numerical terms. An atomic formula of L_2 is of the form $t = s$, $t < s$, $t \in X$ where t and s are numeral terms and X is any set variable. We distinguish quantifiers of a formula of L_2 between *number quantifiers* and *set quantifiers* according as it is applied to a number variable or a set variable. A number quantifier is said to be *bounded* if it is either of the form $(\exists i)(i < t \wedge \varphi)$ or $(\forall i)(i < t \to \varphi)$ where t is a numeral term not containing i. A formula φ of L_2 is said to be Σ^0_0 or Π^0_0 if φ does not contain any set quantifiers and every number quantifier is bounded. For $k \in \omega$ (ω denotes the set of all natural numbers), a formula φ of L_2 is said to be Σ^0_{k+1} (respectively Π^0_{k+1}) if φ is of the form $\exists i_0 \exists i_1 \ldots \exists i_n \psi$ (respectively $\forall i_0 \forall i_1 \ldots \forall i_n \psi$) where ψ is Π^0_k (respectively Σ^0_k). A formula φ of L_2 is said to be Σ^1_0, Π^1_0, or *arithmetical* if φ does not contain any set quantifiers. For $k \in \omega$, a formula φ of L_2 is said to be Σ^1_{k+1} (respectively Π^1_{k+1}) if φ is of the form $\exists X_0 \exists X_1 \ldots \exists X_n \psi$ (respectively $\forall X_0 \forall X_1 \ldots \forall X_n \psi$) where ψ is Π^1_k (respectively Σ^1_k).

1.1 The System RCA_0

First we provide the schemes of induction and comprehension.

Definition 1.1 (induction)**.** 1. For each $i = 0, 1$ and $k \in \omega$, the scheme of Σ^i_k *induction* (also denoted by $\mathsf{I}\Sigma^i_k$) consists of all axioms of the form

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

where $\varphi(n)$ is any Σ^i_k formula. The scheme of Π^i_k *induction* is defined similarly.

2. The scheme of Δ^i_k *induction* consists of all axioms of the form

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

where $\varphi(n)$ is any Σ^i_k formula and $\psi(n)$ is any Π^i_k formula.

Definition 1.2 (comprehension)**.** 1. For each $i = 0, 1$ and $k \in \omega$, the scheme of Σ^i_k *comprehension* consists of all axioms of the form

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

where $\varphi(n)$ is any Σ^i_k formula in which X does not occur freely. The scheme of Π^i_k *comprehension* is defined similarly.

2. The scheme of Δ^i_k *comprehension* consists of all axioms of the form

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

where $\varphi(n)$ is any Σ^i_k formula, $\psi(n)$ is any Π^i_k formula and X does not occur freely in $\varphi(n)$.

The axioms of second order arithmetic Z_2 consist of basic axioms of arithmetic, and the schemes of induction and comprehension for every formulae. The subsystem RCA_0 is defined to be the formal system in the language L_2 whose axioms consists of basic axioms of arithmetic, the scheme of Σ^0_1 induction and the scheme of Δ^0_1 (*recursive*) comprehension. RCA_0 plays a role of a base theory in Reverse Mathematics throughout this thesis. The next two facts are convenient to cope with Σ^0_1 notions. 2 is a formalized version of the fact in recursion theory: Every infinite recursively enumerable set contains an infinite recursive subset, cf. [64, Exercise 1.21] and [57].

Lemma 1.3. 1. Let $\varphi(x)$ be a Σ^0_1 formula in which X and f do not occur freely. RCA_0 proves that if $\varphi(n)$ holds for infinitely many $n \in \mathbb{N}$ (i.e., $(\forall n_0)(\exists n > n_0)\varphi(n)$), there exists a one-to-one function $f : \mathbb{N} \rightarrow \mathbb{N}$ such that $(\forall n)(\varphi(n) \leftrightarrow (\exists m)(f(m) = n))$.

2. Let $\varphi(x)$ be a Σ^0_1 formula. RCA_0 proves that if $\varphi(n)$ holds for infinitely many $n \in \mathbb{N}$, there exists an infinite (i.e., $(\forall n_0)(\exists n > n_0)(n \in X)$) set X such that $(\forall n)(n \in X \rightarrow \varphi(n))$.

Proof. 1 is Lemma II.3.7 of [61]. We show 2. Let f be a one-to-one function such that $(\forall n)(\varphi(n) \leftrightarrow (\exists m)(f(m) = n))$. Define a strictly increasing function g by primitive recursion by putting $g(0) = f(0)$, $g(n+1) = f(\mu m[f(m) > g(n)])$. The image of g exists by Δ^0_1 comprehension and it is a desired set. □

We further introduce several schemes of axioms.

Definition 1.4 (bounded comprehension)**.** For each $i = 0, 1$ and $k \in \omega$, the scheme of *bounded* Σ^i_k *comprehension* consists of all axioms of the form

$$\forall n \exists X \forall i(i \in X \leftrightarrow (i < n \wedge \varphi(i)))$$

where $\varphi(n)$ is any Σ^i_k formula in which X does not occur freely. The schemes of Π^i_k *bounded comprehension* and Δ^i_k *bounded comprehension* are defined similarly.

The scheme of induction and the scheme of bounded comprehension is provably equivalent in a following sense.

Theorem 1.5 (Theorem II.3.9, Exercise II.3.13 [61])**.** 1. RCA_0 proves both Σ^0_1 and Π^0_1 bounded comprehension.

2. For each $k \in \omega$, RCA_0 proves that Σ^0_k induction is equivalent to Σ^0_k bounded comprehension.

We describe the connection between induction scheme and the principle by the name of bounding scheme or collection scheme.

Definition 1.6 (bounding)**.** For each $i = 0, 1$ and $k \in \omega$, the scheme of Σ^i_k *bounding* (also denoted by $\mathsf{B}\Sigma^i_k$) consists of all axioms of the form

$$(\forall t)[(\forall n < t)\exists m\varphi(n, m) \to (\exists b)(\forall n < t)(\exists n < b)\varphi(n, m)]$$

where $\varphi(n, m)$ is any Σ^i_k formula. The scheme of Π^i_k *bounding* and Δ^i_k *bounding* defined similarly.

It is known that for each $k \in \omega$, Σ^0_{k+1} bounding is equivalent to Π^0_k bounding over RCA_0. Moreover, we have following results.

Theorem 1.7 (Kirby and Paris [40])**.** 1. For each $k \in \omega$, Σ^0_k induction implies Σ^0_k bounding over RCA_0. But not vice varsa.

2. For each $k \in \omega$, Σ^0_{k+1} bounding implies Σ^0_k induction over RCA_0. But not vice varsa.

Theorem 1.8. For each $k \geq 2$, Σ^0_k bounding is equivalent to Δ^0_k induction over RCA_0.

1.2 The System ACA_0

ACA_0 is defined to be the formal system in the language L_2 whose axioms consist of basic axioms, the schemes of Σ^1_0 induction and Σ^1_0 (*arithmetical*) comprehension. It is known that ACA_0 is strictly stronger than RCA_0, i.e.,

$$\mathsf{RCA}_0 \subsetneq \mathsf{ACA}_0.$$

ACA_0 can be characterized by Σ^0_1 comprehension. The following lemma is frequently used to show that various theorems of ordinary mathematics imply arithmetical comprehension.

Lemma 1.9 ([61] Lemma III.1.3)**.** The following are equivalent over RCA_0.

1. ACA_0.
2. Σ^0_1 comprehension.
3. For any one-to-one function $\alpha : \mathbb{N} \to \mathbb{N}$ there exists a set X such that $\forall i(i \in X \leftrightarrow \exists j(\alpha(j) = i))$, i.e., the image of α exists.

We mention that if the function $\alpha : \mathbb{N} \to \mathbb{N}$ is increasing then RCA_0 proves the existence of the image of α. We also mention that the following fact is useful when we wish to deduce arithmetical comprehension. For example, see Frittaion and Marcone [18, Theorem 3.4].

Definition 1.10 ([61] Theorem III.4.4)**.** The following definition is made in RCA_0. Let $\alpha : \mathbb{N} \to \mathbb{N}$ be a one-to-one function. We say that $n \in \mathbb{N}$ is α-*true* if $(\forall m > n)(\alpha(m) > \alpha(n))$ and α-*false* otherwise.

Lemma 1.11. The following are equivalent over RCA_0.

1. ACA_0.
2. The set of all α-true elements $T = \{n : n \text{ is } \alpha\text{-true}\}$ exists for any one-to-one function $\alpha : \mathbb{N} \to \mathbb{N}$.
3. An infinite set of α-true elements T' exists for any one-to-one function $\alpha : \mathbb{N} \to \mathbb{N}$.

Proof. $(1 \to 2)$. Note that the statement "m is α-true" is Π^0_1.

$(2 \to 3)$. Note that there are infinitely many true elements.

$(3 \to 1)$. Let $\alpha : \mathbb{N} \to \mathbb{N}$ be a one-to-one function. By our assumption 3, there exists a set T' such that $(\forall n)(\exists m \in T')(n < m)$ and $(\forall n \in T')(n$ is α-true). Since α is one-to-one and T' is infinite, it follows that $(\forall n)(\exists m)(m \in T' \wedge n \leq \alpha(m))$. By Σ^0_0 axiom of choice of numbers there exists a function $\beta : \mathbb{N} \to \mathbb{N}$ such that $(\forall n)(\beta(n) \in T' \wedge n \leq \alpha(\beta(n)))$. Then $(\exists m)(\alpha(m) = n) \leftrightarrow (\exists m < \beta(n))(\alpha(m) = n)$ for all $n \in \mathbb{N}$, because $n \leq \alpha(\beta(n)) < \alpha(l)$ for all $l \geq \beta(n)$ since $\beta(n)$ is α-true. The right-hand-side of the equivalence is Σ^0_0. Thus by Δ^0_1 comprehension there exists the image of α. □

1.3 The System WKL_0

WKL_0 is defined to be the formal system in the language L_2 whose axioms consist of those of RCA_0 plus weak König's lemma: every infinite 0-1 tree has a path. It is known that WKL_0 is properly stronger than RCA_0 and properly weaker than ACA_0, i.e.,

$$\mathsf{RCA}_0 \subsetneq \mathsf{WKL}_0 \subsetneq \mathsf{ACA}_0.$$

Weak König's lemma requires somewhat subtle treatment rather than arithmetical comprehension. So in usual mathematics they tend to use arithmetical comprehension instead of weak König's lemma. However as we will see later surprisingly many theorems are provable in WKL_0 and actually are equivalent to WKL_0 (over RCA_0). WKL_0 can be characterized by Σ^0_1 *separation*. The scheme of separation is defined as follows.

Definition 1.12 (separation)**.** For each $i = 0, 1$ and $k \in \omega$, the scheme of Σ^i_k *separation* consists of all axioms of the form

$$\forall n \neg(\varphi_1(n) \wedge \varphi_2(n)) \to \exists X(\forall n(\varphi_1(n) \to n \in X) \wedge \forall n(\neg\varphi(n) \to n \notin X)),$$

where $\varphi_1(n)$ and $\varphi_2(n)$ are any Σ^i_k formulas and X does not occur freely in $\varphi_1(n) \wedge \varphi_2(n)$. The scheme of Π^i_k *separation* is defined similarly.

The following lemma is frequently used to show that various theorems of ordinary mathematics imply weak König's lemma.

Lemma 1.13 ([61] Lemma IV.4.4)**.** The following are equivalent over RCA_0.

1. WKL_0.
2. Σ^0_1 separation.
3. For all one-to-one functions $\alpha, \beta : \mathbb{N} \to \mathbb{N}$ with $\forall i \forall j (\alpha(i) \neq \beta(j))$ there exists a set $X \subset \mathbb{N}$ such that $\forall i (\alpha(i) \in X \wedge \beta(i) \notin X)$.

1.4 Stronger Systems

For each $k \in \omega$, Π^1_k-CA_0 is defined to be the formal system in the language L_2 whose axioms consists of basic axioms, the schemes of Π^1_k induction and Π^1_k comprehension. ATR_0 is defined to be the formal system in the language L_2 whose axioms consists of those of ACA_0 plus the scheme of arithmetical transfinite recursion. RCA_0, WKL_0, ACA_0, ATR_0, and Π^1_1-CA_0 are sometimes called "big five" systems. It is known that ATR_0 is equivalent to Σ^1_1 separation [61, Theorem V.5.1]. Clearly Π^1_k-CA_0 proves Σ^1_k comprehension. In particular, Π^1_1-CA_0 proves Σ^1_1 comprehension as well as Σ^1_1 separation. Thus Π^1_1-CA_0 is stronger than ATR_0. It is known that ATR_0 can not prove Π^1_1 comprehension and that Π^1_k-CA_0 can not prove Π^1_{k+1} comprehension for each $k \in \omega$. Summarizing, we have:

$$\mathsf{RCA}_0 \subsetneq \mathsf{WKL}_0 \subsetneq \mathsf{ACA}_0 \subsetneq \mathsf{ATR}_0 \subsetneq \Pi^1_1\text{-}\mathsf{CA}_0 \subsetneq \Pi^1_2\text{-}\mathsf{CA}_0 \subsetneq \cdots \subsetneq \mathsf{Z}_2.$$

Such strong axioms are required in set theory, Ramsey theory, infinite game theory, and so on. It is worth investigating whether these axioms are essentially used in so-called ordinary mathematics.

2 Countable Sets, Relations, and Functions

This chapter provides the notions of (sequences of) countable sets, relations, and functions within RCA_0. Results in this chapter are used throughout of the rest of the thesis. Section 2.2 does Reverse Mathematics of some propositions of binary relations. In Section 2.3 we consider, in terms of Reverse Mathematics, extensions of partial functions with the scheme of axioms of choice of numbers . Section 2.4 is a brief survey on Ramsey theorems as atypical examples of Reverse Mathematics.

2.1 Basic Notions

It is known that RCA_0 is strong enough to develop a coding method (see Simpson [61, II.2]). In particular we can encode pairs of natural numbers or finite sequences of natural numbers as single natural numbers. We write a code for a pair of natural numbers n and m as (n, m), a code for a sequence of natural numbers $n_0, n_1, \ldots, n_l$ as $\langle n_0, n_1, \ldots, n_l \rangle$ or $\langle n_i : i \leq l \rangle$. The first and second projection function for a code for a pair of natural numbers are denoted by π_1 and π_2 respectively, namely $\pi_1((n, m)) = n$ and $\pi_2((n, m)) = m$ hold. Also we write s_i for the i-th element of the sequence coded by s. By means of the coding method, we can formalize the notions of countable relations, countable functions, finite or infinite sequences of countable sets, and so on.

Definition 2.1 (binary relations)**.** The following definitions are made in RCA_0. A *countable binary relation* R on a set $A \subset \mathbb{N}$ is a set of pairs of elements of A. We write aRb to mean $(a, b) \in R$. A countable binary relation R is said to be *transitive* if R satisfies the condition $(\forall a, b, c \in A)(aRb \wedge bRc \to aRc)$, *reflexive* if R satisfies the condition $(\forall a \in A)(aRa)$, and *symmetric* if R satisfies the condition $(\forall a, b \in A)(aRb \to bRa)$ respectively. A transitive, reflexive and symmetric countable binary relation is said to be an *equivalence relation*. Given an equivalence relation on A, we can form the *quotient set* $A/R = \{a \in A : (\forall b \in A)(b < a \to \neg aRb)\}$.

The following definition are made within RCA_0. A *sequence of countable sets* $\mathcal{A}$ is a set of pairs. We write $n \in A_i$ as $(n, i) \in \mathcal{A}$ and denote such a sequence as $\langle A_i : i \in \mathbb{N} \rangle$. Note that for given $\mathcal{A}$ each i, $A_i = \{n : (n, i) \in \mathcal{A}\}$ exists by Δ^0_1 comprehension. The next theorem shows that arithmetical comprehension is necessary and sufficient to assert the existence of the intersection or the union of a given sequence of countable sets.

Theorem 2.2 (intersections and unions)**.** The following are equivalent over RCA_0.

1. ACA_0.
2. For any sequence of countable sets $\langle A_i : i \in \mathbb{N} \rangle$, $\bigcap_{i \in \mathbb{N}} A_i = \{n : \forall i (n \in A_i)\}$ exists.

3. For any sequence of countable sets $\langle A_i : i \in \mathbb{N}\rangle$, $\bigcup_{i\in\mathbb{N}} A_i = \{n : \exists i(n \in A_i)\}$ exists.

Proof. $1 \to 2$ (as well as $1 \to 3$) is trivial since the defining formula are arithmetical. $2 \to 3$ follows from De Morgan's Law. It remains to show $3 \to 1$. Instead of showing ACA_0 directly, we show Lemma 1.9.2. Let $\varphi(n)$ be a Σ^0_1 formula and write $\varphi(n) \equiv \exists i\theta(n,i)$ where $\theta(n,i)$ is Σ^0_0. Reasoning within RCA_0, define the sequence of sets $\langle A_i : i \in \mathbb{N}\rangle$ as $n \in A_i \leftrightarrow \theta(n,i)$. By our assumption 3, the set $\bigcup_{i\in\mathbb{N}} A_i$ exists. It follows that $n \in \bigcup_{i\in\mathbb{N}} A_i \leftrightarrow \exists i\theta(n,i) \leftrightarrow \varphi(n)$. Thus by Δ^0_1 comprehension $\exists X\forall n(n \in X \leftrightarrow \varphi(n))$. This completes the proof. □

The next theorem shows that arithmetical comprehension is necessary and sufficient to assert the existence of the *equivalence or transitive closure* of a given countable binary relation.

Theorem 2.3 (equivalence and transitive closures)**.** The following are equivalent over RCA_0.

1. ACA_0.
2. For any symmetric binary relation $R \subset A \times A$, there exists the equivalence relation R' including R which is minimal with respect to set inclusion.
3. For any binary relation $R \subset A \times A$, there exists the transitive relation R' including R which is minimal with respect to set inclusion.

Proof. First we show the implication $1 \to 2$. We reason within ACA_0. Let

$$R' = \{(a,a') : \exists\langle a_i \in A : i \le n\rangle[a = a_0 \wedge (\forall i < n)(a_i R a_{i+1}) \wedge a_n = a']\}.$$

Clearly R' has the desired properties.

Next we show the implication $2 \to 1$. We reason within RCA_0. Instead of proving ACA_0 directly, we show Lemma 1.9.3. Let $\alpha : \mathbb{N} \to \mathbb{N}$ be a one-to-one function. Let $A = \{a^i_j : i,j \in \mathbb{N}\} \cup \{b\}$ and

$$R = \{(a^i_j, a^i_{j+1}), (a^i_{j+1}, a^i_j) : i,j \in \mathbb{N}\} \cup \{(a^i_j, b), (b, a^i_j) : \alpha(j) = i\}.$$

By our assumption 2, there exists the minimal equivalence relation R' including R. Then it follows that $a^i_0 R' b \leftrightarrow \exists j(\alpha(j) = i)$ for all $i \in \mathbb{N}$. Hence, by Δ^0_1 comprehension, the image of α exists. This completes the proof of $2 \to 1$.

Similarly we can prove the equivalence between 1 and 3. We mention that to prove $1 \to 3$ $\langle a_i \in A : i \le n\rangle$ should be replaced by $\langle a_i \in A : i \le n+1\rangle$ in order to eliminate unnecessary identity relations in defining R'. □

We remark that the reversals of the theorem above could be described as an easy consequence of Theorem 2.5 of Hirst [31]. On the other hand, weak König's lemma is strong enough to assert the existence of a nontrivial equivalence or transitive extension.

Theorem 2.4 (equivalence and transitive extensions)**.** The following are equivalent over RCA_0.

1. WKL_0.
2. For any symmetric binary relation $R \subset A \times A$ and elements $a, a' \in A$, if there is no sequence of elements of A such that

$$a = a_1 \wedge a_1 R a_2 \wedge a_2 R a_3 \wedge \cdots \wedge a_{n-1} R a_n \wedge a_n = a' \ (2 \leq n, a_i \in A),$$

   then R can be extended to an equivalence relation R' such that $\neg a R' a'$.
3. For any binary relation $R \subset A \times A$ and elements $a, a' \in A$, if there is no sequence of elements of A such that

$$a = a_1 \wedge a_1 R a_2 \wedge a_2 R a_3 \wedge \cdots \wedge a_{n-1} R a_n \wedge a_n = a' \ (2 \leq n, a_i \in A),$$

   then R can be extended to transitive relation R' such that $\neg a R' a'$.

Proof. First we prove $1 \to 2$. We reason within WKL_0. Let $R \subset A \times A$ be a symmetric binary relation on A. Let $(a, a') \in A \times A$ be a pair of an element of A satisfying the condition above. Let T be the set of all $t \in 2^{<\mathbb{N}}$ such that

1. $\forall i < \mathrm{lh}(t)(t(i) = 1 \to i \in A \times A)$,
2. $\forall i < \mathrm{lh}(t)(i \in R \to t(i) = 1)$,
3. $\forall i < \mathrm{lh}(t)(\pi_1(i) = \pi_2(i) \to t(i) = 1)$,
4. $\forall i, j < \mathrm{lh}(t)(\pi_1(i) = \pi_2(j) \wedge \pi_2(i) = \pi_1(j) \wedge t(i) = 1 \to t(j) = 1)$,
5. $\forall i < \mathrm{lh}(t), \forall \langle a_j \in A : j \leq n \rangle < \mathrm{lh}(t)[(\forall j < n)(a_j R_t a_{j+1}) \wedge i = (a_0, a_n) \to t(i) = 1]$ where $x R_t y \equiv (\exists k < \mathrm{lh}(t))(t(k) = 1 \wedge \pi_1(k) = x \wedge \pi_2(k) = y)$,
6. $\forall i < \mathrm{lh}(t)(i = (a, a') \to t(i) = 0)$.

Clearly T is a tree. We claim that T is infinite. To see this, let $m \in \mathbb{N}$ be given. Define a Σ^0_1 formula $\varphi(i) \equiv \exists \langle a_j \in A : j \leq m \rangle [(\forall j < m)(a_j R a_{j+1}) \wedge i = (a_0, a_m)]$. By bounded Σ^0_1 comprehension (Theorem 1.5), letting $Y = \{i < m : \varphi(i)\}$, define $t \in 2^{<\mathbb{N}}$ of length m by

$$t(i) = \begin{cases} 1 & (i \in Y) \\ 0 & (i \notin Y). \end{cases}$$

Then clearly $t \in T$ and $\mathrm{lh}(t) = m$. This proves that T is infinite. Hence, by weak König's lemma, there exists a path f through T. Let R' be the set of all $r \in A \times A$ such that $f(r) = 1$. Then R' is an equivalence relation such that $R' \supset R$ and $\neg a R' a'$. This completes the proof of $1 \to 2$.

Second we prove $2 \to 1$. We reason within RCA_0. Instead of proving weak König's lemma directly, we show Lemma 1.13.3. Let $\alpha, \beta : \mathbb{N} \to \mathbb{N}$ be one-to-one functions such that $\forall i \forall j(\alpha(i) \neq \beta(j))$. Let $A = \{a^i_j : i, j \in \mathbb{N}\} \cup \{b, c\}$ and

$$\begin{aligned} R =& \{(a^i_j, a^i_{j+1}), (a^i_{j+1}, a^i_j) : i, j \in \mathbb{N})\} \cup \\ & \{(a^i_j, b), (b, a^i_j) : \alpha(j) = i\} \cup \{(a^i_j, c), (c, a^i_j) : \beta(j) = i\}. \end{aligned}$$

Note that there does not exist any sequence of elements of A such that

$$b = a_1 \wedge a_1 R a_2 \wedge a_2 R a_3 \wedge \cdots \wedge a_{n-1} R a_n \wedge a_n = c \ (2 \leq n, a_i \in A).$$

By our assumption 2, there exists an equivalence relation $R' \supset R$ such that $\neg b R' c$. Then it follows that $a_0^{\alpha(j)} R' b \wedge \neg a_0^{\beta(j)} R' b$ for all $j \in \mathbb{N}$. Setting $X = \{i : a^i_0 R' b\}$, we obtain $\forall j(\alpha(j) \in X \wedge \beta(j) \notin X)$. This completes the proof of $2 \to 1$.

The equivalence between 1 and 3 is proved in much same way. We mention that to prove $1 \to 3$ the items 3 and 4 should be omitted in constructing T. □

If a relation is defined by an arithmetical but not Δ^0_1 formula, we need arithmetical comprehension to assert the existence of the quotient set.

Theorem 2.5 (quotient sets)**.** The following are equivalent over RCA_0.

1. ACA_0.
2. Let $\varphi(x, y)$ be a Σ^0_1 equivalence relation on a set $A \subset \mathbb{N}$, i.e.,
   - $(\forall a \in A)(\varphi(a, a))$,
   - $(\forall a, b \in A)(\varphi(a, b) \to \varphi(b, a))$,
   - $(\forall a, b, c \in A)(\varphi(a, b) \wedge \varphi(b, c) \to \varphi(a, c))$.

   Then there exists a quotient set $A^* \subset A$ by φ, i.e.,
   - $(\forall a \in A)(\exists b \in A^*)(\varphi(a, b))$,
   - $(\forall a, b \in A^*)(\varphi(a, b) \to a = b)$.
3. Let $\varphi(x, y)$ be a Π^0_1 equivalence relation on a set $A \subset \mathbb{N}$. Then there exists a quotient set $A^* \subset A$ by φ.

Proof. $1 \to 2$ is immediate. Instead of showing ACA_0 directly, we show Lemma 1.9.3. We reason within RCA_0. Let $\alpha : \mathbb{N} \to \mathbb{N}$ be a one-to-one function. Define a Σ^0_1 equivalence relation on $A = \mathbb{N}$ by

$$\varphi(x, y) \equiv (x \in \mathrm{Im}\alpha \wedge y \in \mathrm{Im}\alpha) \vee x = y.$$

By our assumption 2, a quotient set $A^* \subset A$ exists. Let $a^* \in A^*$ be $\varphi(\alpha(0), a^*)$. It follows that $i \in \mathrm{Im}\alpha \leftrightarrow i \notin A^* \setminus \{a^*\})$. Thus by Δ^0_1 comprehension the image of α exists. This completes the proof of $2 \to 1$. The equivalence between 1 and 3 is shown in a similar way. □

2.2 The Scheme of Axiom of Choice of Numbers

A *countable partial function* $f : A \to B$ from a set A to a set B is a countable binary relation which satisfies $(\forall (a,b) \in f)(a \in A \wedge b \in B)$ and $(\forall (a,b),(a',b') \in F)(a = a' \to b = b')$. f is said to be *total* if $(\forall a \in A)(\exists b \in B)((a,b) \in f)$. We write $f(a) = b$ to mean $(a,b) \in f$. In what follows, by a *function* we mean a countable total function except where noted. The scheme of axiom of choice of numbers is defined as follows.

Definition 2.6 (axiom of choice of numbers)**.** For each $i = 0, 1$ and $k \in \omega$, the scheme of Σ^i_k *axiom of choice of numbers* consists of all axioms of the form

$$\forall n \exists m \varphi(n,m) \to \exists f \forall n \varphi(n, f(n)),$$

where f ranges over countable total functions and $\varphi(n,m)$ is any Σ^i_k formula in which f does not occur freely. The scheme of Π^i_k *axiom of choice of numbers* is defined similarly.

Lemma 2.7. 1. For each $k \in \omega$, Σ^0_k axiom of choice of numbers implies Π^0_k separation over RCA_0.

2. For each $k \in \omega$, Π^0_k axiom of choice of numbers implies Π^0_{k+1} separation over RCA_0.

Proof. 1. Let $\varphi_1(n)$ and $\varphi_2(n)$ be Π^0_k formulae with $\forall n \neg(\varphi_1(n) \wedge \varphi_2(n))$. Let

$$\psi(n,m) \equiv (\neg\varphi_1(n) \wedge m = 0) \vee (\neg\varphi_2(n) \wedge m = 1).$$

Notice that $\psi(n,m)$ is Σ^0_k and $\forall n \exists m \psi(n,m)$ holds. By Σ^0_k axiom of choice of numbers we have $\exists f \forall n \psi(n, f(n))$. By Δ^0_1 comprehension let $X = \{n : f(n) = 1\}$. Then clearly X is a separator of φ_1 and φ_2.

2. Let $\varphi_1(n)$ and $\varphi_2(n)$ be Π^0_{k+1} formulae with $\forall n \neg(\varphi_1(n) \wedge \varphi_2(n))$. Let $\varphi_i(n) \equiv \forall m \theta_i(n,m)$ where $\theta_i(m,n)$ is Σ^0_k formula, $i = 0, 1$. Let

$$\psi(n,m) \equiv (\neg\theta_1(n, \pi_1(m)) \wedge \pi_2(m) = 0) \vee (\neg\theta_2(n, \pi_1(m)) \wedge \pi_2(m) = 1).$$

Notice that $\psi(n,m)$ is Π^0_k and $\forall n \exists m \psi(n,m)$ holds. By Π^0_k axiom of choice of numbers we have $\exists f \forall n \psi(n, f(n))$. By Δ^0_1 comprehension let $X = \{n : \pi_2(f(n)) = 1\}$. Then clearly X is a separator of φ_1 and φ_2.

□

A corollary of the lemma is that RCA_0 proves Π^0_1 separation since it is well known that RCA_0 proves Σ^0_1 axiom of choice of numbers. This answers [61, Exercise IV.4.8].

Theorem 2.8. The following are equivalent over RCA_0.

1. ACA_0.
2. Σ^1_0 axiom of choice of numbers.

3. Π^0_1 axiom of choice of numbers.

Proof. $(1 \to 2)$. Let $\varphi(n,m)$ be an arithmetical formula and assume that $\forall n \exists m \varphi(n,m)$. Define a countable total function f by arithmetical comprehension as $f(n) = m \leftrightarrow \varphi(n,m) \wedge (\forall m' < m)(\neg\varphi(n,m'))$. $(2 \to 3)$ is trivial. $(3 \to 1)$. We reason within RCA_0. By the previous lemma Π^0_1 axiom of choice of numbers implies Π^0_2 separation. On the other hand, Π^0_2 separation implies Σ^0_1 comprehension. Thus by Lemma 1.9 we have arithmetical comprehension. □

The next theorem is about the domain of countable partial functions.

Theorem 2.9. The following are equivalent over RCA_0.

1. ACA_0.
2. For any countable partial function $f : \mathbb{N} \to \mathbb{N}$ there exists a set $X \subset \mathbb{N}$ such that $\forall n(n \in X \leftrightarrow \exists m(f(n) = m))$, i.e., the domain of f exists.
3. For any countable partial functions $f : \mathbb{N} \to \mathbb{N}$ there exists a total function $\tilde{f} : \mathbb{N} \to \mathbb{N}$ such that $(\forall n, m)(f(n) = m \to \tilde{f}(n) = m)$, i.e., a total extension of f exists.

Proof. $(1 \to 2)$ is immediate since the defining formula of X is Σ^0_1. To show $(2 \to 3)$, assume that $\mathrm{dom}f$, the domain of f, exists. By Δ^0_1 comprehension, let $\tilde{f} = \{(n,m) : (n,m) \in f \vee (n \notin \mathrm{dom}f \wedge m = 0)\}$. Clearly $\tilde{f}$ is a total extension of f. For $(3 \to 1)$, reasoning within RCA_0, we show Lemma 1.9.3. Let $\alpha : \mathbb{N} \to \mathbb{N}$ be a one-to-one function. Define a countable partial function as $f = \{(n,m) : \alpha(m) = n\}$, i.e., f is a partial inverse function of α. By our assumption 3, let $\tilde{f}$ be a total extension of f. It follows that $\exists m(\alpha(m) = n) \leftrightarrow \alpha(\tilde{f}(n)) = n$ for all n. Thus, by Δ^0_1 comprehension, the image of α exists. This completes the proof. □

The theorem above concerns with the scheme of strong axiom of choice of numbers which is defined as follows.

Definition 2.10 (strong axiom of choice of numbers)**.** For each $i = 0, 1$ and $k \in \omega$, the scheme of Σ^i_k *strong axiom of choice of numbers* consists of all axioms of the form

$$\exists f \forall n(\exists m \varphi(n,m) \to \varphi(n, f(n))),$$

where f ranges over countable total functions and $\varphi(n,m)$ is any Σ^i_k formula in which f does not occur freely. The scheme of Π^i_k *strong axiom of choice of numbers* is defined similarly.

Theorem 2.11. The following are equivalent over RCA_0.

1. ACA_0.
2. Σ^1_0 strong axiom of choice of numbers.
3. Σ^0_0 strong axiom of choice of numbers.

Proof. $(1 \to 2)$. Let $\varphi(n, m)$ be an arithmetical formula. Define a countable total function f by arithmetical comprehension as

$$f(n) = m \leftrightarrow [\varphi(n, m) \wedge (\forall m' < m)\neg\varphi(n, m')] \vee [\neg\exists m\varphi(n, m) \wedge m = 0].$$

$(2 \to 3)$ is trivial. $(3 \to 1)$. We reason within RCA_0. Let $f : \mathbb{N} \to \mathbb{N}$ be a countable partial function. Letting $\varphi(n, m) \equiv (f(n) = m)$, by our assumption 3, we have a totalization of f Thus, by Theorem 2.9, we have arithmetical comprehension. □

2.3 Extensions of Consistent Partial Functions

This section provides Reverse Mathematics results concerning the compactness-like property of families of countable functions. Note that if a finite countable partial function is finite then it can be coded by a single number as a finite sequence of pairs of numbers.

Definition 2.12. The following definitions are made in RCA_0.

1. A sequence of countable partial functions $\langle f_i : i \in \mathbb{N}\rangle$ is *consistent* if

$$(\forall i, j)(\forall a, b, b')((a, b) \in f_i \wedge (a, b') \in f_j \to b = b').$$

2. A set of (codes of) finite countable partial functions F is *consistent* if

$$(\forall \sigma, \tau \in F)(\forall a, b, b')((a, b) \in \sigma \wedge (a, b') \in \tau \to b = b').$$

3. A countable partial function f is an *extension* of a countable partial function g if $(\forall a, b)((a, b) \in g \to (a, b) \in f)$.

4. A sequence $\langle (a_i, b_i) : i \in \mathbb{N}\rangle$ of pairs is said to be Σ^0_1 *partial function* if $(\forall i, j)(a_i = a_j \to b_i = b_j)$, cf. Definition 6.35.

Theorem 2.13. The following are equivalent over RCA_0.

1. WKL_0.

2. Every consistent sequence of countable partial functions $\langle f_i : i \in \mathbb{N}\rangle$ has a partial extension, i.e., there exists a countable partial function f such that $(\forall i)(f_i \subset f)$.

3. Every consistent set of (codes of) finite countable partial functions F has a partial extension, i.e., there exists a countable partial function f such that $(\forall \sigma \in F)(\sigma \subset f)$.

4. Every Σ^0_1 partial function $\langle p_i : i \in \mathbb{N}\rangle$ has a partial extension, i.e., there exists a countable partial function f such that $(\forall i)(p_i \in f)$.

Proof. $(1 \to 2)$. We reason within WKL_0. Let $\varphi(p) \equiv \exists i(p \in f_i)$ and $\psi(p) \equiv \exists i \exists b((\pi_1(p), b) \in f_i \wedge \pi_2(p) \neq b)$. (It is maybe easy to understand if we write $\varphi(a, b) \equiv \exists i(f_i(a) = b)$ and $\psi(a, b) \equiv \exists i(f_i(a) \neq b)$). Observing that both $\varphi(p)$ and $\psi(p)$ are Σ^0_1, by Σ^0_1 separation (Lemma 1.13), we have a set X such that $\forall p((\varphi(p) \to p \in X) \wedge (p \in X \to \neg\psi(p)))$. By Δ^0_1 comprehension let $f = \{p : p \in X \wedge p \text{ is a pair} \wedge (\forall b < \pi_2(p))(\pi_1(p), b) \notin X\}$. It follows that f is a desired countable partial function.

$(2 \to 3)$. Reasoning within RCA_0, let $\langle \sigma_i : i \in \mathbb{N} \rangle$ be an enumeration of F. By our assumption 2, we have a desired countable partial function.

$(3 \to 4)$. By Δ^0_1 comprehension define a consistent set of (codes of) finite countable partial functions F as follows.

$$\sigma \in F \leftrightarrow \sigma \text{ is a finite sequence } \langle q_i : i < k \rangle \text{ and } (\forall i < k)(q_i = (a_i, b_i)).$$

By our assumption 3, we have a desired countable partial function.

$(4 \to 1)$. We reason within RCA_0. Instead of WKL_0 we show the equivalent statement 3 of lemma 1.13. Let $\alpha, \beta : \mathbb{N} \to \mathbb{N}$ be one-to-one functions such that $(\forall i, j)(\alpha(i) \neq \beta(j))$. Define a Σ^0_1 partial function $\langle p_i : i \in \mathbb{N} \rangle$ as $p_{2i} = (\alpha(i), 0), p_{2i+1} = (\beta(i), 1)$. By our assumption 4, we have a partial extension f. Letting $X = \{n : (n, 0) \in f\}$ it follows that $\forall n((\exists m(\alpha(m) = n) \to n \in X) \wedge (n \in X \to \neg\exists m(\beta(m) = n)))$. This completes the proof. □

In the case of $\{0, 1\}$-valued partial functions, an extension f can be taken as a total one. Especially the equivalence between 1 and 4 can be viewed as an analog of the fact in degree theory which says that *a Turing degree* $\boldsymbol{a}$ *is low degree if and only if every* $\{0, 1\}$*-valued computable partial function has a total* $\boldsymbol{a}$*-computable extension.* On the other hand, if we force f to be total in the previous theorem, assertion 2, 3 and 4 obviously turns out to be equivalent to ACA_0 over RCA_0, see Theorem 2.9.

Theorem 2.14. The following are equivalent over RCA_0.

1. WKL_0.
2. Every consistent sequence of countable partial $\{0, 1\}$-valued functions has a total extension f.
3. Every consistent set of (codes of) finite countable partial $\{0, 1\}$-valued functions F has a total extension f.
4. Every Σ^0_1 partial $\{0, 1\}$-valued function has a total extension f.

Proof. We show $1 \to 2$. We reason within WKL_0. Let T be the set of all $t \in 2^{<\mathbb{N}}$ such that $\forall i, k < \mathrm{lh}(t)((\forall v < 2)((k, v) \in f_i \to t(i) = v)$. Clearly T is an infinite tree. A path f through T is a desired function. Other implications are proven in much same way as the previous proof. Note that the Σ^0_1 partial function of the previous proof is $\{0, 1\}$-valued. This completes the proof. □

2.4 Ramsey Theorem

Ramsey theory has been widely applied in combinatorics, functional analysis et al. Infinite Ramsey theorems are parametrized and rich in variety. They give anomalous examples from the perspective of Reverse Mathematics, namely, there are examples from Ramsey theorems whose logical strength can not be classified into "big five" systems.

Definition 2.15. The following definitions are made in RCA_0. For $X \subset \mathbb{N}$ and $k \in \mathbb{N}\setminus\{0\}$, let $[X]^k = \{s \in \mathbb{N}^k : (\forall i < k)(s_i \in X) \wedge (\forall i < k-1)(s_i < s_{i+1})\}$. By $\mathrm{RT}(k,l)$ $(0 < k, l)$, i.e., *Ramsey theorem for exponent k with l colors*, we mean the assertion that for all $f : [\mathbb{N}]^k \to \{0, 1, 2, \ldots l-1\}$, there exists there exists $i < l$ and an infinite set $X \subset \mathbb{N}$ such that $(\forall s \in [X]^k)(f(s) = i)$. We denote $(\forall l > 0)\mathrm{RT}(k,l)$ as $\mathrm{RT}(k)$.

RT(1) is the so-called (infinite version of) pigeon hall principle. Hirst [30] showed that RT(1) is equivalent to Π^0_1 bounding. (Hence it is also equivalent to Σ^0_2 bounding.)

Proposition 2.16. RCA_0 proves the following.

1. $(\forall k)\mathrm{RT}(k,1)$.
2. $(\forall k, k', l, l')(k' < k \wedge l' < l \to (\mathrm{RT}(k,l) \to \mathrm{RT}(k',l')))$.
3. $(\forall k)(\mathrm{RT}(k+1,2) \to \mathrm{RT}(k))$.
4. $(\forall k)(\forall l \geq 2)(\mathrm{RT}(k,2) \wedge \mathrm{RT}(k,l) \to \mathrm{RT}(k,l+1))$.

Proof. 1 and 2 are trivial. We show 3. Fix $l \in \mathbb{N}$ and let $f : [\mathbb{N}]^k \to l$. Define $f' : [\mathbb{N}]^{k+1} \to 2$ as

$$f'(\bar{a}) = \begin{cases} 0 & \text{if } f(\bar{a}') = f(\bar{a}'') \text{ for all } \bar{a}', \bar{a}'' \subset \bar{a}, \\ 1 & \text{otherwise.} \end{cases}$$

By $\mathrm{RT}(k+1,2)$, we have a homogeneous set X. It is easy to see that $f'(X) = 0$. Thus X is a desired homogeneous set.

Next we show 4. For given $f : [\mathbb{N}]^k \to l+1$ define $f' : [\mathbb{N}]^k \to l$ as

$$f'(\bar{a}) = \begin{cases} f(\bar{a}) & \text{if } f(\bar{a}) < l, \\ l-1 & \text{otherwise.} \end{cases}$$

By $\mathrm{RT}(k,l)$, we have a homogeneous set X. If $f'(X) < l-1$ then X is a desired homogeneous set. If $f'(X) = l-1$ then define $f'' : [X]^k \to 2$ as follows

$$f''(\bar{a}) = \begin{cases} 0 & \text{if } f(\bar{a}) = l-1, \\ 1 & \text{otherwise.} \end{cases}$$

By $\mathrm{RT}(k,2)$, we have a homogeneous set Y. Clearly Y is a desired homogeneous set. □

Specker [67] constructed a computable coloring of $[\mathbb{N}]^2$ with no computable homogeneous set. It follows that RCA_0 does not imply $\mathrm{RT}(2,2)$. On the other hand, Jockusch [38] constructed a computable coloring of $[\mathbb{N}]^3$ such that every homogeneous set computes $\mathbf{0}'$. This fact is the essence of the proof that $\mathrm{RT}(3)$ implies ACA_0 over RCA_0, see Simpson [61, Theorem III.7.6]. Using a result of Jockusch, Hirst [30] showed that WKL_0 does not imply $\mathrm{RT}(2,2)$. Seetapun [56] proved a theorem in recursion theory that entails that $\mathrm{RT}(2,2)$ does not imply ACA_0 over WKL_0. More recently, Liu [44] proved that $\mathrm{RT}(2,2)$ does not imply WKL_0 over RCA_0.

We turn to the tree version of Ramsey theorem.

Definition 2.17 (Simpson [61], page 21)**.** 1. Two sequences in $\mathbb{N}^{<\mathbb{N}}$ are said to be *compatible* if they are equal or one is an initial segment of the other.

2. A subset S of a tree T (S is need not to be a subtree of T) is *perfect* if every $\sigma \in S$ has a pair of incompatible extensions $\tau_1, \tau_2 \in S$.

Note that the statement "S is perfect" is Π^0_2.

Definition 2.18. The following definitions are made in RCA_0. By $\mathrm{TT}(k,l)$ $(0 < k,l)$, i.e., *Ramsey theorem for trees for exponent k with l colors*, we mean the assertion that for all perfect tree T and $f : [T]^k \to \{0,1,2,\ldots,l-1\}$, there exists $i < l$ and a perfect subset $S \subset T$ such that $f(\sigma_1,\ldots,\sigma_k) = i$ for all $\langle \sigma_1,\ldots,\sigma_k\rangle \in [2^{<\mathbb{N}}]$. We denote $(\forall l > 0)\mathrm{TT}(k,l)$ as $\mathrm{TT}(k)$.

It is known that the logical strength of $\mathrm{TT}(1)$ is between Σ^0_2 bounding and Σ^0_2 induction over RCA_0 [7].

3 Countable Partially Ordered Sets (Posets)

In this chapter we do Reverse Mathematics of countable order theory, in particular we shed light on fixed point theorems. It is notable that famous equivalence between the axiom of choice, Zorn's lemma, and well-ordering theorem, which is a prehistoric result of Reverse Mathematics, appears in order theory. Some other statements (including fixed point theorems) in order theory equivalent to axiom of choice are known (cf. [71]). The first "orthodox" Reverse Mathematics result on fixed point theorem is Shioji-Tanaka [58], which showed that Brouwer fixed point theorem is equivalent to WKL_0 over RCA_0. However, we remark that their setting is considerably different from ours for we focus on countable posets. Section 3.1 provides basic notions with Reverse Mathematics results. Section 3.2 is devoted to Reverse Mathematics of order theoretical fixed point theory. Section 3.3 is a brief survey on combinatorial principles as atypical examples of Reverse Mathematics.

For more details on concepts of order theory, cf., e.g., Birkhoff's classic [4] or modern textbooks [11, 53, 55]. Monographs of fixed point theorems are also available, cf., [23, 24].

3.1 Basic Notions

Definition 3.1 (countable posets)**.** The following definitions are made in RCA_0. A *countable poset* (also called a *countable partially ordered set*) P consists of a set $|P| \subset \mathbb{N}$ together with a binary relation $\leq_P$ such that the system $(|P|, \leq_P)$ obeys the usual partially ordered set axioms, i.e.,

$$(\forall x \in P)(x \leq_P x)(\textit{reflexivity}),$$
$$(\forall x, y \in P)((x \leq_P y) \wedge (y \leq_P x) \to x = y)(\textit{antisymmetricity}),$$
$$(\forall x, y, z \in P)((x \leq_P y) \wedge (y \leq_P z) \to x \leq_P z)(\textit{transitivity}).$$

For notational convenience we write $|P|$ as P. We shall write $(x \leq_P y) \wedge (x \neq y)$ as $x <_P y$. A nonempty subset S of P is a *chain* if S is totally ordered by $\leq_P$, i.e., $(\forall x, y \in S)(x \leq_P y \vee y \leq_P x)$.

Lemma 3.2 (maximal chains)**.** RCA_0 proves that every countable poset has a maximal chain.

Proof. We reason within RCA_0. Let $\langle a_i : i \in \mathbb{N} \rangle$ be an enumeration of the elements of a countable poset P. Define $f : \mathbb{N} \to \{0, 1\}$ by primitive recursion by putting $f(n) = 1$ if $(\forall i < n)(f(i) = 1 \to ((a_i \leq_P a_n) \vee (a_n \leq_P a_i)))$, $f(n) = 0$ otherwise. Let M be the set of all a_i such that $f(i) = 1$. Clearly M is a maximal chain of P. This completes the proof. □

Definition 3.3 (countable lattices and countable complete lattices)**.** The following definitions are made in RCA_0. A countable poset L is called a *countable lattice* if any two elements of L have a least upper bound and a greatest lower bound. A countable lattice L is *complete* if any subset of L has a least upper bound and a greatest lower bound.

The following proposition states that arithmetical comprehension is required to obtain binary functions $\sup_L$ and $\inf_L$ which take two elements to respectively a least upper bound and a greatest lower bound of them. On the other hand, if the order is total we can obtain $\sup_L$ and $\inf_L$ within RCA_0 by defining $\sup_L(x, y) = \max_L \{x, y\}$ and $\inf_L(x, y) = \min_L \{x, y\}$.

Proposition 3.4. The following are equivalent over RCA_0.

1. ACA_0.
2. For any countable lattice L the binary function $\sup_L$ exists.
3. For any countable lattice L the binary function $\inf_L$ exists.

Proof. The implications $1 \to 2$ and $1 \to 3$ follow immediately since the defining formulae of a least upper bound and a greatest upper bound are arithmetical. We shall show the implication $2 \to 1$. (The implication $3 \to 1$ is shown dually.) We reason in RCA_0. Instead of proving ACA_0 directly, we will prove the equivalent statement [61, Lemma III.1.3.3]. Let $\alpha : \mathbb{N} \to \mathbb{N}$ be a one-to-one function. Define a countable lattice L by putting $|L| = \{\bot, \top, a_i, b^k_j : i, j, k \in \mathbb{N}\}$ where $\bot$ and $\top$ are the bottom and the top respectively,

1. $b^k_j \leq_L b^k_{j'} \leftrightarrow j \leq j'$,
2. $a_i \leq_L b^i_j \leftrightarrow (\exists j' < j)(\alpha(j') = i)$.

By our assumption 2, we have the binary function $\sup_L : L^2 \to L$. It follows that $(\exists j)(\alpha(j) = i) \leftrightarrow \sup_L(a_i, \bot) \neq \top$. Thus the image of α exists by Δ^0_1 comprehension. This completes the proof. □

At this time we introduce within RCA_0 a specific ordering on $\mathbb{N}$ essentially due to Frittaion and Marcone [18]. Let $\alpha : \mathbb{N} \to \mathbb{N}$ be a one-to-one function. Recall that $n \in \mathbb{N}$ is said to be α-*true* if $(\forall m > n)(\alpha(m) > \alpha(n))$ and α-*false* otherwise. Then define an ordering $\prec_\alpha$ on $\mathbb{N}$ as follows: for $n < m$,

$$m \prec_\alpha n \Leftrightarrow \alpha(n) > \alpha(k) \text{ for some } n < k \leq m,$$

$$n \prec_\alpha m \Leftrightarrow \alpha(n) < \alpha(k) \text{ for all } n < k \leq m.$$

We shall write $(x \prec_\alpha y) \vee (x = y)$ as $x \preceq_\alpha y$. By the definition, the following hold: a) $\preceq_\alpha$ is total, b) if $n \in \mathbb{N}$ is α-true then $\{x : x \prec_\alpha n\}$ is finite, c) if $n \in \mathbb{N}$ is α-false then $\{x : n \prec_\alpha x\}$ is finite, d) $k \leq \#\{x > n : n \prec_\alpha x\}$ if and only if $n \prec_\alpha n + k$, and hence the statement $k \leq \#\{x : n \prec_\alpha x\}$ is Σ^0_0, and e) if $n \in \mathbb{N}$ is α-true and $m \in \mathbb{N}$ is α-false then $n \prec_\alpha m$. We will apply this ordering to deduce arithmetical comprehension using Lemma 1.11. This idea is due to Professor Takeshi Yamazaki.

The following criterion for completeness on lattices is known as an example of the Dual Principles for posets. It is not difficult to prove, but we need arithmetical comprehension.

Proposition 3.5. The following are equivalent over RCA_0.

1. ACA_0.
2. Let L be a countable lattice. If there exists a least upper bound for every subset S of L, then there exists a greatest lower bound for every subset S of L, i.e., L is complete.
3. Let L be a countable lattice. If there exists a greatest lower bound for every subset S of L, then there exists a least upper bound for every subset S of L, i.e., L is complete.

Proof. First we show the implication $1 \to 2$. By arithmetical comprehension, let $S' = \{x \in L : (\forall y \in S)(x \leq_L y)\}$ for given $S \subset L$. It is easily verified that a least upper bound for S' is a greatest lower bound for S.

Second we show the implication $2 \to 1$. We reason in RCA_0. Instead of proving ACA_0 directly, we will prove the equivalent statement Lemma 1.11.3. Let $\alpha : \mathbb{N} \to \mathbb{N}$ be a one-to-one function. We may assume that there are infinitely many α-false elements. Define a countable lattice L by letting $|L| = \mathbb{N}$ and $n \leq_L m \leftrightarrow n \prec_\alpha m$. Observing that "$n$ is α-false" is Σ^0_1, by Lemma 1.3.2, let $X \subset L$ be an infinite set of α-false elements. Clearly X does not have any greatest lower bound. By our assumption 2, there exists a subset $Y \subset L$ with no least upper bound. Clearly Y is an infinite set of α-true elements.

The equivalence between 1 and 3 is shown dually. This completes the proof. □

Next we turn our attention to completeness on posets.

Definition 3.6 (CPOs)**.** The following definitions are made within RCA_0. A nonempty subset D of a countable poset P is *directed* if

$$(\forall x, y \in D)(\exists z \in D)((x \leq_P z) \wedge (y \leq_P z)).$$

A countable poset P is *complete* or a *CPO* if P has the smallest element $\bot_P$ and every directed subset D of P has a least upper bound. The least upper bound of D is denoted by $\sup D$. A subset S of a CPO P is a *sub-CPO* of P if $\bot_P \in S$ and $\sup D \in S$ for any directed subset D of S.

The following proposition is convenient to think of completeness.

Proposition 3.7. The following is provable within RCA_0. Let P be a countable poset. Then the following are equivalent.

1. Any directed subset of P has a least upper bound.
2. Any chain of P has a least upper bound.
3. Any $\leq_P$-increasing sequence of P has a least upper bound.

We can also show the similar result on greatest lower bounds.

Proof. The implication $1 \to 2$ is immediate since any chain is directed. First we show the implication $2 \to 3$. Let $\langle a_i : i \in \mathbb{N} \rangle$ be a $\leq_P$-increasing sequence of P. If $\langle a_i : i \in \mathbb{N} \rangle$ has a largest element a_i, then this a_i is a least upper bound of $\langle a_i : i \in \mathbb{N} \rangle$. Otherwise let C be an infinite subset of the range of $\langle a_i : i \in \mathbb{N} \rangle$. It follows that C is a chain of P and $\sup C = \sup \langle a_i : i \in \mathbb{N} \rangle$. Finally we show the contraposition of the implication $3 \to 1$. Assume that a directed subset D of P does not have any least upper bound. Observing that D is infinite, let $\langle d_i : i \in \mathbb{N} \rangle$ be an enumeration of D. Define a $\leq_P$-increasing sequence $\langle a_i : i \in \mathbb{N} \rangle$ of elements of P by primitive recursion by putting $a_0 = d_0$, $a_{n+1} =$ the least $d \in D$ such that $a_n \leq_P d$ and $d_{n+1} \leq_P d$. (Here "least" refers to the ordering of $\mathbb{N}$.) It follows that $\langle a_i : i \in \mathbb{N} \rangle$ does not have any least upper bound since if it had one then it would be a least upper bound for D. This completes the proof. □

In next section we investigate fixed point theorems. Before that we introduce the notions of maps on countable posets.

Definition 3.8 (maps)**.** The following definitions are made in RCA_0. Let $(P, \leq_P)$ be a countable poset and let $F : P \to P$ be a self-map on P. F is *order-preserving* if $(\forall x, y \in P)(x \leq_P y \to F(x) \leq_P F(y))$. F is *inflationary* if $(\forall x \in P)(x \leq_P F(x))$. F is *continuous* if for each $\leq_P$-increasing sequence $\langle a_i : i \in \mathbb{N} \rangle$ of elements of P having a least upper bound, the sequence $\langle F(a_i) : i \in \mathbb{N} \rangle$ has a least upper bound and it equals $F(\sup \langle a_i : i \in \mathbb{N} \rangle)$. Note that every continuous function is order-preserving.

3.2 Fixed Point Theorems

This section is devoted to develop Reverse Mathematics of fixed point theory of countable lattices and posets. First we discuss the fixed point theory on countable complete lattices. The results on countable CPOs will be discussed in the latter part of this section.

The Knaster-Tarski fixed point theorem is fundamental and has tremendous applications. The theorem is first stated by Knaster and Tarski [41] in the restricted form, thereafter by Tarski [70] in its general form. We show that the countable version of the theorem is provable in RCA_0.

Proposition 3.9 (Knaster-Tarski fixed point theorem)**.** The following is provable in RCA_0. Let L be a nonempty countable complete lattice. If $F : L \to L$ is order-preserving, then the set of all fixed points of F is nonempty and forms a countable complete lattice. In particular there are a least and a greatest fixed point of F.

Proof. Reasoning within RCA_0, let P be the set of all fixed points. It is easily seen that $\inf\{x \in L : x \leq_L F(x)\} \in P$ and hence P is not empty. [1] To show

[1] Details are following: Let $Q = \{x \in L : x \leq_L F(x)\}$ and $a = \inf\{x \in L : x \leq_L F(x)\}$. Note that Q is not empty since it contains the bottom. For any $x \in Q$ we have $x \leq_L a$ and hence $x \leq_L F(x) \leq_L F(a)$. Therefore $F(a)$ is an upper bound of Q and hence $a \leq_L F(a)$. Since $F(a) \leq_L F(F(a))$ we have $F(a) \in Q$ and hence $F(a) \leq_L a$. Thus we have $F(a) = a$.

that P is complete, take a subset $X \subset P$ and take $a = \sup X$ $(\in L)$. Letting $Y = \{y \in L : a \leq_L y \wedge F(y) \leq_L y\}$, take $b = \inf Y$ $(\in L)$. It follows that $b \in P$ and b is a least upper bound for X in P. [2] The existence of a greatest lower bound for X in P is shown dually. This completes the proof. □

The Knaster-Tarski fixed point theorem within RCA_0 does not provide the binary functions $\sup_P$ and $\inf_P$ on the set P of all fixed points (even if $\sup_L$ and $\sup_L$ are equipped by the lattice). In fact, we have

Proposition 3.10. The following are equivalent over RCA_0.

1. ACA_0.
2. Let L be a countable complete lattice with binary functions $\sup_L$ and $\inf_L$. Let $F : L \to L$ be an order-preserving self-map on L. Then the binary function $\sup_P$ exists where P is the set of all fixed points of F.
3. Let L be a countable complete lattice with binary functions $\sup_L$ and $\inf_L$. Let $F : L \to L$ be an order-preserving self-map on L. Then the binary function $\inf_P$ exists where P is the set of all fixed points of F.

Proof. The implications $1 \to 2$ and $1 \to 3$ are trivial. We only show the implication $2 \to 1$ for the implication $3 \to 1$ is shown dually. We reason within RCA_0. Instead of proving ACA_0 directly, we will prove the equivalent statement [61, Lemma III.1.3.3]. Let $\alpha : \mathbb{N} \to \mathbb{N}$ be a one-to-one function. Define a countable complete lattice by putting $|L| = \{\bot, \top, a_i, b_j, c^l_k : i, j, k, l \in \mathbb{N}\}$ where $\bot$ and $\top$ are the bottom and the top respectively,

1. $c^l_k \leq_L c^l_{k'} \leftrightarrow k \leq k'$,
2. $a_i \leq_L c^i_k$,
3. $b_i \leq_L c^i_k$.

Define an order-preserving self-map F on L by putting

1. $F(\bot) = \bot$,
2. $F(\top) = \top$,
3. $F(a_i) = a_i$,
4. $F(b_j) = b_j$,
5. $F(c^l_k) = c^l_k$ if $\alpha(k) = l$, $F(c^l_k) = c^l_{k+1}$ otherwise.

[2] $x \leq a$, $x \leq F(x) \leq F(a)$ $(\forall x \in X)$, i.e., $F(a)$ is an upper bound for X, thus $a \leq F(a)$. $b \leq y, F(b) \leq F(y) \leq y$ $(\forall y \in Y)$, i.e., $F(b)$ is a lower bound for Y, thus $F(b) \leq b$. $x \leq a \leq y$ $(\forall x \in X, \forall y \in Y)$, then x is a lower bound for Y, thus $x \leq b$, then b is an upper bound for X, thus $a \leq b$. It follows that $a \leq F(a) \leq F(b) \leq b$, $F(F(b)) \leq F(b)$, $F(b) \in Y$, $b \leq F(b)$, $b = F(b)$, $b \in P$. For any upper bound $u \in P$ of X, since $a \leq u$ and $F(u) = u$, $u \in Y$. Thus $b \leq u$.

Clearly the binary functions $\sup_L$ and $\inf_L$ exist. By our assumption 2, we have the binary function $\sup_P : P^2 \to P$ where P is the set of all fixed points of F. It follows that $(\exists j)(\alpha(j) = i) \leftrightarrow \sup_P(a_i, b_i) \neq \top$. Thus the image of α exists by Δ^0_1 comprehension. This completes the proof. □

There is a nice converse to Knaster-Tarski theorem by Davis [12]. We give a proof of the converse in countable case within ACA_0. Moreover, we show that arithmetical comprehension is required to prove the converse.

Theorem 3.11 (Davis' converse)**.** The following are equivalent over RCA_0.

1. ACA_0.
2. If L is a countable lattice such that every order-preserving self-map $F : L \to L$ has a fixed point, then L is complete.

Proof. $(1 \to 2)$. We reason in ACA_0. Let L be an incomplete countable lattice. We shall construct an order-preserving self-map on L with no fixed point. By Proposition 3.7, let $\langle a_i : i \in \mathbb{N}\rangle$ be a $\leq_L$-increasing sequence with no least upper bound. (In the case that $\langle a_i : i \in \mathbb{N}\rangle$ is a $\leq_L$-decreasing sequence with no greatest lower bound, the argument goes dually.) We may assume that $\langle a_i : i \in \mathbb{N}\rangle$ has no duplicates and so is strictly increasing. By arithmetical comprehension, let $U = \{x \in L : (\forall i)(a_i \leq_L x)\}$ be a set of all upper bounds of $\langle a_i : i \in \mathbb{N}\rangle$. Observing that U is infinite, let $\langle u_i : i \in \mathbb{N}\rangle$ be an enumeration of U. Define a sequence $\langle b_i : i \in \mathbb{N}\rangle$ of elements of L by primitive recursion by putting $b_0 = u_0$, $b_{n+1} = \inf_L(b_n, u_{n+1})$. (Note that the binary function $\inf_L$ exists by arithmetical comprehension.) It follows that $(\forall i)(b_i \in U)$ by Σ^0_0 induction on i. [3] Note that $(\exists i)(x \not\leq_L b_i)$ for all $x \in U$ since if there is a counter example x then this x would be a least upper bound of $\langle a_i : i \in \mathbb{N}\rangle$. Now we define a self-map F on L as follows. For $x \notin U$, let $F(x) = a_i$ where i is the least number such that $a_i \not\leq_L x$; and for $x \in U$, let $F(x) = b_i$ where i is the least number such that $x \not\leq_L b_i$. It follows that F is order-preserving and does not have any fixed point. This completes the proof of $1 \to 2$.

$(2 \to 1)$. We reason in RCA_0. Instead of proving ACA_0 directly, we will prove the equivalent statement Lemma 1.11.2. Let $\alpha : \mathbb{N} \to \mathbb{N}$ be a one-to-one function. We may assume that there are infinitely many α-false elements. Define a countable lattice L by letting $|L| = \mathbb{N}$ and $n \leq_L m \leftrightarrow n \prec_\alpha m$. Observing that "$n$ is α-false" is Σ^0_1, by Lemma 1.3.2, let $X \subset L$ be an infinite set of α-false elements. Clearly X does not have any greatest lower bound. Therefore L is incomplete. By our assumption 2, there exists an order-preserving self-map $F : L \to L$ with no fixed point. It follows that $T = \{n : n <_L F(n)\}$ is the set of all α-true elements. This completes the proof of $2 \to 1$. □

Next we turn our attention to fixed point theorems on CPOs. The following theorem can be found in Kantorovitch [39, Theorem I] (1939). The theorem is also known as Kleene fixed point theorem.

[3] Assume that $b_n \in U$. Take $i \in \mathbb{N}$ arbitrary. Since $a_i \leq_L b_n$ and $a_i \leq u_{n+1}$ $a_i \leq_L \inf_L(b_n, u_{n+1}) = b_{n+1}$. Thus, $b_{n+1} \in U$.

Proposition 3.12 (Tarski-Kantorovitch fixed point theorem)**.** The following is provable in RCA_0. Let P be a CPO and $F : P \to P$ be a continuous self-map on P. Then the set of all fixed points of F is a CPO.

Proof. We reason within RCA_0. First we show that the set of all fixed points of F has the smallest element. Define a $\leq_P$-increasing sequence $\langle a_i : i \in \mathbb{N}\rangle$ by primitive recursion by putting $a_0 = \bot_P$ and $a_{i+1} = F(a_i)$. Let a be a least upper bound of $\langle a_i : i \in \mathbb{N}\rangle$. It follows that

$$a = \sup\langle a_i : i \in \mathbb{N}\rangle = \sup\langle F(a_i) : i \in \mathbb{N}\rangle = F(\sup\langle a_i : i \in \mathbb{N}\rangle) = F(a).$$

Therefore a is a fixed point of F. To show that a is the smallest, let a' be a fixed point of F. It follows by Σ^0_0 induction that $(\forall i)(a_i \leq_P a')$ namely a' is an upper bound of $\langle a_i : i \in \mathbb{N}\rangle$. So we have $a \leq_P a'$. Next we show 3 of Proposition 3.7 to show the completeness. Let $\langle b_i : i \in \mathbb{N}\rangle$ be a $\leq_P$-increasing sequence of fixed points. Since

$$F(\sup\langle b_i : i \in \mathbb{N}\rangle) = \sup\langle F(b_i) : i \in \mathbb{N}\rangle = \sup\langle b_i : i \in \mathbb{N}\rangle,$$

$\sup\langle b_i : i \in \mathbb{N}\rangle$ is a fixed point. Thus $\langle b_i : i \in \mathbb{N}\rangle$ has a least upper bound in the set of all fixed points. This completes the proof. □

The following statement can be found in Bourbaki [5] (1949) and Witt [74] (1951). The countable version of the theorem is easily proven in RCA_0.

Proposition 3.13 (Bourbaki-Witt fixed point theorem)**.** The following is provable within RCA_0. Let P be a CPO and $F : P \to P$ be an inflationary self-map on P. Then F has a maximal fixed point. [4]

Proof. We reason in RCA_0. By Lemma 3.2, let $M \subset P$ be a maximal chain. It follows by the maximality of M that $a = \sup M$ is a maximal fixed point of F. This completes the proof. □

Abian and Brown [1] (1961) proved a fixed point theorem of order-preserving maps on CPOs. The proof is much convoluted than the former theorems. We divide Abian-Brown theorem into two statements. We can prove the following version with maximality within RCA_0.

Proposition 3.14 (Abian-Brown Fixed Point Theorem I)**.** The following is provable within RCA_0. Let P be a CPO and $F : P \to P$ be an order-preserving self-map on P. Then F has a maximal fixed point.

Proof. Reasoning within RCA_0, let $Q = \{x \in P : x \leq_P F(x)\}$. By Lemma 3.2, let M be a maximal chain of Q. Let $a = \sup M$ and fix any $x \in M$. Since F is order-preserving, $x \leq_P a$ implies $F(x) \leq_P F(a)$. On the other hand, since $x \in Q$ we have $x \leq_P F(x)$. Therefore we have $x \leq_P F(a)$. So $F(a)$ is an upper

[4] There is a CPO P and an inflationary self-map on P with no least (or even minimal) fixed point; $P = \{\bot \leq \cdots \leq a_n \leq \cdots \leq a_1 \leq a_0\}$, $F(a_i) = a_i$, $F(\bot) = a_0$. This is a counter example of Davey [11, 8.23].

bound of M and we have $a \leq_P F(a)$. Since F is order-preserving, we have $F(a) \leq_P F(F(a))$ and $F(a) \in Q$. Since M is maximal, we have $F(a) \in M$ and $F(a) \leq_P a$. Thus we have $a = F(a)$ and clearly a is maximal. This completes the proof. □

To prove the version with minimality, we need arithmetical comprehension. Here we give a characterization of the statement of the theorem in terms of the existence of a certain kind of substructure. Note that the conditions (a), (b), and (c) of 2 are Π^0_1 while the statement "Q is a sub-CPO of P" is Π^1_1. Although the proof in some literature concerns with notions of ordinals, cf., e.g., [55], our proof can be carried out in ACA_0 sidestepping the notions of ordinals thanks to the countability.

Theorem 3.15 (Abian-Brown Fixed Point Theorem II)**.** The following are equivalent over RCA_0.

1. ACA_0.
2. Let P be a CPO and $F : P \to P$ be an order-preserving self-map on P. Then there exists a sub-CPO Q of P such that
   (a) $(\forall x \in Q)(x \leq_P F(x))$,
   (b) Q is F-invariant, i.e., $(\forall x \in Q)(F(x) \in Q)$,
   (c) $(\forall x \in Q)(\forall y \in P)(y = F(y) \to x \leq_P y)$.
3. Let P be a CPO and $F : P \to P$ be an order-preserving self-map on P. Then F has a least fixed point.
4. Let P be a CPO and $F : P \to P$ be an order-preserving self-map on P. If F has a fixed point, then F has a least fixed point.

Proof. $(1 \to 2)$. The set

$$Q = \{x \in P : x \leq_P F(x) \wedge (\forall y \in P)(y = F(y) \to x \leq_P y)\}$$

exists by arithmetical comprehension. Clearly Q includes $\bot_P$ and satisfies the condition (a) and (c) by the definition. To show that Q satisfies the condition (b), let $x \in Q$. Since $x \leq_P F(x)$ and F is order-preserving, we have $F(x) \leq_P F(F(x))$. Let $y \in P$ be a fixed point of F. Since $x \leq_P y$ and F is order-preserving, we have $F(x) \leq_P F(y) = y$. Therefore we have $F(x) \in Q$ and thus Q satisfies the condition (b). Finally to show that Q is complete, let $D \subset Q$ be a directed subset and let $a = \sup D$. We shall show that $a \in Q$. Firstly take an element $x \in D$. Since $x \leq_P a$ and F is order-preserving, we have $F(x) \leq_P F(a)$. On the other hand, we have $x \leq_P F(x)$. Therefore we have $x \leq_P F(a)$ and consequently $F(a)$ is an upper bound of D. So we have $a \leq_P F(a)$. Secondly take a fixed point y of F. Since y is an upper bound of D, we have $a \leq_P y$. Thus we have $a \in Q$. This completes the proof of $1 \to 2$.

$(2 \to 3)$. By Lemma 3.2, let M be a maximal chain of Q. Let $a = \sup M$. Since Q is a sub-CPO of P, we have $a \in Q$. For any $x \in M$, we have $x \leq_P a$.

Since F is order-preserving, we have $F(x) \leq_P F(a)$. On the other hand, by (a), we have $x \leq_P F(x)$. Therefore we have $x \leq_P F(a)$, and consequently $F(a)$ is an upper bound of M. So we have $a \leq_P F(a)$. On the other hand, by (b), $F(a) \in Q$. By the maximality of M, we have $F(a) \in M$. So it follows that $F(a) \leq_P a$. Finally we have $a = F(a)$ and a is a least fixed point of F by (c). This completes the proof of $2 \to 3$.

$(3 \to 4)$ is trivial.

$(4 \to 1)$. We reason in RCA_0. Instead of proving ACA_0 directly, we will prove the equivalent statement Lemma 1.11.3. Let $\alpha : \mathbb{N} \to \mathbb{N}$ be a one-to-one function. We may assume that there are infinitely many α-false elements. Define a countable poset by putting $|P| = \{a_i^j, b_k : i, j, k \in \mathbb{N}\}$ and

1. $a_i^j \leq_P a_{i'}^{j'} \leftrightarrow (j \prec_\alpha j') \vee (j = j' \wedge i \leq i')$,
2. $b_k \leq_P b_{k'} \leftrightarrow k' \leq k$,
3. $a_i^j <_P b_k \leftrightarrow k \leq \#\{x : j \prec_\alpha x\}$,
4. $b_k <_P a_i^j \leftrightarrow \#\{x : j \prec_\alpha x\} < k$.

Define an order-preserving self-map $F : P \to P$ by $F(a_i^j) = a_{i+1}^j$, $F(b_k) = b_k$. Clearly F has a fixed point, but does not have any least fixed point. By our assumption 4, P is incomplete. Therefore there exists a directed subset D of P with no least upper bound. Let X be an infinite set of elements $j \in \mathbb{N}$ such that $(\exists i)(a_i^j \in D)$. It follows that X is an infinite set of α-true elements. This completes the proof of $4 \to 1$. □

The converse of the theorem is known, cf. Markowsky [46]. To prove this, we again need arithmetical comprehension.

Theorem 3.16 (Markowsky's Converse)**.** The following are equivalent over RCA_0.

1. ACA_0.
2. If P is a countable poset such that every order-preserving self-map $F : P \to P$ has a least fixed point, then P is a CPO.

Proof. $(1 \to 2)$. We reason in ACA_0. Let P be a countable poset such that every order-preserving self-map has a least fixed point. P has the least element since any element is a fixed point of the identity map. To obtain a contradiction, suppose that P is not complete. By Proposition 3.7, let $\langle a_i : i \in \mathbb{N}\rangle$ be a $\leq_P$-increasing sequence with no least upper bound. We may assume that $\langle a_i : i \in \mathbb{N}\rangle$ is strictly increasing. By arithmetical comprehension, let $U = \{x \in P : (\forall i)(a_i \leq_P x)\}$ be a set of all upper bounds for $\langle a_i : i \in \mathbb{N}\rangle$. Now we define a self-map F on P by $F(x) = a_i$ where i is the least number such that $a_i \not\leq_P x$ if $x \notin U$, $F(x) = x$ if $x \in U$. Clearly F is order-preserving and does not have a least fixed point, a contradiction. This completes the proof of $1 \to 2$.

$(2 \to 1)$. We reason in RCA_0. Instead of proving ACA_0 directly, we will prove the equivalent statement Lemma 1.11.3. Let $\alpha : \mathbb{N} \to \mathbb{N}$ be a one-to-one function. We may assume that there are infinitely many α-false elements. Define a countable poset P by letting $|P| = \mathbb{N}$ and $n \leq_P m \leftrightarrow n \succeq_\alpha m$. Observing that "$n$ is α-false" is Σ^0_1, by Lemma 1.3.2, let $X \subset P$ be an infinite set of α-false elements. Clearly X is a directed set with no least upper bound. Therefore P is incomplete. By our assumption 2, there exists an order-preserving self-map $F : P \to P$ with no least fixed point. It is easy to check that if n is α-false then n is not a fixed point and $n <_P F(n)$. We will claim that a set of α-true elements $Y = \{n : F(n) \leq_P n\}$ is infinite. If F has a fixed point then F has infinitely many ones. So Y is infinite. If F does not have a fixed point then n is α-true $\leftrightarrow F(n) <_P n$. Thus in both case the claim holds. This completes the proof of $2 \to 1$. □

3.3 Combinatorial Principles

In this section we refer to combinatorial principles which are not classified into "big five" systems.

Definition 3.17 (CAC and ADS, [59])**.** Let S be a subset of a countable partially ordered set $(P, <_P)$. S is said to be a *chain* if $(\forall a, b \in S)(a <_P b \vee a = b \vee b <_P a)$. S is said to be an *antichain* if $(\forall a, b \in S)(\neg(a <_P b) \wedge \neg(b <_P a))$. S is said to be an ascending sequence if $(\forall a, b \in S)(a < b \to a <_P b)$. S is said to be a descending sequence if $(\forall a, b \in S)(a < b \to a >_P b)$.

CAC (Chain AntiChain) states that every countable infinite partially ordered set has an infinite subset that is either a chain or an antichain. ADS (Ascending or Descending Sequence) states that every countable infinite linear ordered set has an infinite subset S that is either an ascending sequence or a descending sequence.

It is possible that we define an ascending or a descending sequence as a function rather than a set. However it does not make difference in the sense that for example if we have an ascending sequence as a set then we have an ascending sequence as a function and vise versa via Lemma 1.3. As they say in [59], by a nice application of $\mathrm{RT}(2, 2)$, CAC is shown.

Proposition 3.18. $\mathsf{RCA}_0 + \mathrm{RT}(2, 2)$ proves CAC.

Proof. Let P be a countable infinite partially ordered set. Define $f : [\mathbb{N}]^2 \to \{0, 1\}$ as

$$f((a, b)) = \begin{cases} 0 & (a \in P \wedge b \in P \wedge (a <_P b \vee b <_P a)), \\ 1 & (\text{otherwise}). \end{cases}$$

By $\mathrm{RT}(2, 2)$, we have infinite subset X of $\mathbb{N}$ and $i \in \{0, 1\}$ such that $(\forall \langle a, b\rangle \in [X]^2)(f(\langle a, b\rangle) = i)$.

In the case of $i = 0$, clearly $X \subset P$ and X is an infinite chain.

In the case of $i = 1$, let $Y = X \cap P$. Clearly $Y \subset P$ and Y is an infinite antichain. □

It is known that the following diagram holds and WKL_0 is incomparable with CAC nor ADS over RCA_0 [43, 59]

$$\mathsf{RCA}_0 \subsetneq \mathsf{RCA}_0 + \mathrm{ADS} \subsetneq \mathsf{RCA}_0 + \mathrm{CAC} \subsetneq \mathsf{RCA}_0 + \mathrm{RT}(2,2).$$

The statement argued in the following proposition is from [11, 2.40 Theorem].

Proposition 3.19. RCA_0 proves that ADS is equivalent to the following statement. A countable partially ordered set has an infinite chain if and only if it has an ascending chain or a descending chain.

Proof. First we prove the statement within $\mathsf{RCA}_0 + \mathrm{ADS}$. Let P be a countable partially ordered set. If P has an ascending or a descending sequence, then it is an infinite chain. (We don't need ADS to show this direction.) Conversely, assume that we have an infinite chain C of P. Observing that C is a countable infinite linear ordered set, by ADS, we have an ascending or a descending chain of C.

Second we prove within RCA_0 that the statement implies ADS. Let $(L, <_L)$ be a countable infinite linear ordered set. Observing L itself is an infinite chain of L, by the statement L has an ascending or a descending sequence. This completes the proof. □

4 Countable Semigroups and Monoids

In this chapter we do Reverse Mathematics of countable semigroup theory. In Section 2.2, we show that Isbell's zaig-zag theorem is equivalent to WKL_0 over RCA_0. In Section 2.3, we explore the Reverse Mathematics of the Rees theorem. We see that ACA_0 proves the Rees theorem for countable semigroups. The research for the reversal is ongoing.

4.1 Basic Notions

The following definitions are made in RCA_0. A *countable semigroup* S consists of a nonempty set $|S| \subset \mathbb{N}$ together with a binary operation $\cdot_S : |S|^2 \to |S|$ which is associative, that is, $(\forall s,t,r \in S)((s \cdot_S t) \cdot_S r = s \cdot_S (t \cdot_S r))$. For notational convenience we write $|S|$ as S, $s \cdot_S t$ as st for $s,t \in S$, $(st)r (= s(tr))$ as str, and so on. If there exists a distinguished element $1_S \in S$ which satisfies $1_S s = s1_S = s$ for all $s \in S$, we say that the element is an *identity* and that the system $(S, \cdot_S, 1_S)$ is a *countable monoid*. A distinguished element $0_S \in S$ which satisfies $0_S s = s0_S = 0_S$ for all $s \in S$ is called a *zero*. A element $e \in S$ which satisfies $ee = e$ is called an *idempotent*. A subset $I \subset S$ which satisfies $(\forall s \in S)(\forall a \in I)(sa \in I \wedge as \in I)$ is called an *ideal*. Furthermore, If $I \neq S$ then I is called a *proper* ideal. A relation R on a semigroup is called *left compatible* if $(\forall s,t,a \in S)(sRt \to asRat)$ and *right compatible* if $(\forall s,t,a \in S)(sRt \to saRta)$. It is called *compatible* if $(\forall s,t,s',t' \in S)(sRt \wedge s'Rt' \to ss'Rtt')$. One can see that a relation is compatible if and only if it is both left and right compatible. An compatible equivalence relation is called *congruence*. A congruence on a semigroup S give rise to a *quotient semigroup* S/R. Notions of *homomorphisms* and *isomorphisms* on semigroups or monoids are made in a straightforward way. For more information for semigroup theory see, for example, Higgins [28], Howie [36], or Tamura [68]. The following lemma is an analog of Lemma 2.4.

Lemma 4.1. The following is provable within WKL_0. Let S be a semigroup and R be a reflexive, symmetric, and compatible relation on S. Let $s,t \in S$ not have a sequence $a_1, a_2, \ldots, a_n \in S$ such that

$$s = a_1 \wedge a_1 R a_2 \wedge \cdots \wedge a_{n-1} R a_n \wedge a_n = t.$$

Then R can be extended to a congruence R' such that $\neg sR't$.

Proof. The same ideas as for Theorem 2.4 applies. In defining the binary tree T, add the following two clauses for left and right compatibility.

$$\forall i,j < \mathrm{lh}(t), \forall a < \mathrm{lh}(t)[a \in M \wedge t(i) = 1 \wedge \pi_1(j) = a\pi_1(i) \wedge \pi_2(j) = a\pi_2(i) \to t(j) = 1],$$
$$\forall i,j < \mathrm{lh}(t), \forall a < \mathrm{lh}(t)[a \in M \wedge t(i) = 1 \wedge \pi_1(j) = \pi_1(i)a \wedge \pi_2(j) = \pi_2(i)a \to t(j) = 1].$$

□

4.2 Dominions and Isbell's Zig-Zag Theorem

In this section we determine the exact logical strength of the existence of dominions and Isbell's zig-zag theorem for countable monoids. If A and B are monoids and $A \subset B$, then we say both that A is a *submonoid* of B and B is a *monoid extension* of A. Below we define the notions of *dominions* and *zig-zags*. Note that the assertion "b is dominated by A" is Π^1_1 while "b has a zig-zag over A" is Σ^0_1.

Definition 4.2 (dominions)**.** The following definitions are made in RCA_0. Let $A \subset B$ be monoids and $b \in B$. b is *dominated* by A if for any monoid C and for any pair of homomorphisms $f, g : B \to C$, if $(\forall a \in A)(f(a) = g(a))$, abbreviated $f \restriction_A = g \restriction_A$, then $f(b) = g(b)$. The *dominion* of A is the set of all elements of B that is dominated by A. The dominion of A forms a submonoid of B including A.

Definition 4.3 (zig-zags)**.** Let $A \subset B$ be monoids and $b \in B$. A *zig-zag* of b over A is a triple of sequences $\langle\langle a_0, a_1, \ldots, a_{2m}\rangle, \langle x_1, x_2, \ldots, x_m\rangle, \langle y_1, y_2, \ldots, y_m\rangle\rangle$ such that

1. $a_i \in A$ and $x_j, y_j \in B$ $(0 \leq i \leq 2m, 1 \leq j \leq m)$,
2. $b = x_1 a_0 = a_{2m} y_m$,
3. $a_0 = a_1 y_1$, $a_{2i} y_i = a_{2i+1} y_{i+1} (1 \leq i < m)$,
4. $x_i a_{2i-1} = x_{i+1} a_{2i} (1 \leq i < m)$, $x_m a_{2m-1} = a_{2m}$.

For example, the system $(\mathbb{Z}, +_{\mathbb{Z}}, 0_{\mathbb{Z}})$ forms a countable monoid. Let $A = \{0, j+1, j+2, \ldots\}$ $(0 \leq j)$ and $B = \mathbb{Z}$. A is a submonoid of B and $1 \in B$ has a zig-zag

$$a_0 = j+2, a_1 = j+1, a_2 = 0, x_1 = -j-1, y_1 = 1$$

over A. It is convenient to illustrate this by the equations below

$$\begin{aligned} 1 &= (-j-1) + (j+2) \\ &= (-j-1) + (j+1) + 1 \\ &= \qquad\qquad\quad 0 + 1. \end{aligned}$$

We see that 1 is dominated by A since

$$\begin{aligned} f(1) &= f((-j-1)+(j+2)) \\ &= f(-j-1)+f(j+2) \\ &= f(-j-1)+g(j+2) \\ &= f(-j-1)+g((j+1)+1) \\ &= f(-j-1)+g(j+1)+g(1) \\ &= f(-j-1)+f(j+1)+g(1) \\ &= f((-j-1)+(j+1))+g(1) \\ &= f(0)+g(1) \\ &= g(0)+g(1) \\ &= g(0+1) \\ &= g(1) \end{aligned}$$

for any countable monoid C and any homomorphisms $f, g : B \to C$ such that $f \restriction_A = g \restriction_A$. On the other hand, if we let $A' = \{0\}$, then $1 \in B$ does not have a zig-zag over A' and is not dominated by A'. This simple difference between the two cases is a key idea to show the reversals.

In general, it is provable in RCA_0 that if b has a zig-zag over A then b is dominated by A by Δ^0_1 induction on the length of the zig-zag. *Isbell's zig-zag theorem for countable monoids* states that the converse direction is also hold. That is, *if A is a submonoid of B, then $b \in B$ is dominated by A if and only if b has a zig-zag over A.* We show that the zig-zag theorem is equivalent to WKL_0 over RCA_0.

Theorem 4.4. The following are equivalent over RCA_0.

1. WKL_0.
2. Isbell's zig-zag theorem for countable monoids.

Proof. $(1 \to 2)$. We show "only if" part reasoning within WKL_0. Let $A \subset B$ be monoids and $b^* \in B$ not have any zig-zag over A. We shall construct a monoid C and two homomorphisms $f, g : B \to C$ such that $f \restriction_A = g \restriction_A$ and $f(b^*) \neq g(b^*)$. Let L be the set of all elements of B plus a new element $|$. Let M be the monoid of all finite words over the alphabet L. Define a relation $R \subset M \times M$ by

1. $\sigma\tau\rho R \sigma\tau'\rho$ if τ and τ' do not contain $|$ and the computation of τ in B equals to the computation of τ' in B,
2. $\sigma a|\rho R \sigma|a\rho$, $\sigma|a\rho R \sigma a|\rho$ if $a \in A$,
3. $\sigma||\tau R \sigma\tau$, $\sigma\tau R \sigma||\tau$.

By the argument in Hoffman's proof in [32], there does not exist any sequence of M such that

$$b^*| = w_1 \wedge w_1 R w_2 \wedge w_2 R w_3 \wedge \cdots \wedge w_{n-1} R w_n \wedge w_n = |b^* \ (2 \leq n, w_i \in M).$$

By Lemma 4.1, there exists a congruence $R' \supset R$ such that $\neg b^* | R' | b^*$. Thus we can form a quotient monoid $C = M/R'$. Define $f, g : B \to C$ by $f(b) = b$ and $g(b) = |b|$ for all $b \in B$. Clearly C, α and β have the desired properties. This completes the proof of $1 \to 2$.

$(2 \to 1)$. We reason within RCA_0. Instead of proving weak König's lemma directly, we will prove the equivalent statement Lemma 1.13.3. Let $\alpha, \beta : \mathbb{N} \to \mathbb{N}$ be one-to-one functions such that $(\forall j, j')(\alpha(j) \neq \beta(j'))$. Let $B = \bigoplus_{i \in \mathbb{N}} \mathbb{Z} x_i + \mathbb{Z} y$, the free abelian group generated by a set of indeterminates $\{x_0, x_1, x_2, \ldots, y\}$. Define a sequence of submonoids $\langle A_i : i \in \mathbb{N} \rangle$ of B as $A_i = \{0_B\} \cup \{j x_i : (\exists j' < m)(f(j') = i)\}$ where 0_B is the identity of B. It follows that

$$A_i = \begin{cases} \{0_B, (j+1)x_i, (j+2)x_i, \ldots\} & \text{if } \alpha(j) = i, \\ \{0_B\} & \text{if no such } j \text{ exists.} \end{cases}$$

Let $A = \bigoplus_{i \in \mathbb{N}} A_i$ as a subset of B. Note that A is a submonoid of B. Now we shall see that the subgroup S of B generated by $\{(j+1)x_{\beta(j)} - y : j \in \mathbb{N}\}$ exists. Given an element b of B, say $b = \sum_{i=0}^{n} c_i x_{l_i} - cy \ (c_i, c \in \mathbb{Z}, c_i \neq 0)$, we see that $b \in S$ if and only if for each $i \leq n$ there exists $k_i \leq |c_i|$ such that $\beta(k_i) = l_i$ and $\sum_{i=0}^{n} c_i/(k_i + 1) = c$. Thus S exists by Δ^0_1 comprehension and we can form the quotient group $B' = B/S$. Let $A' = \{\bar{a} : a \in A\}$ where $\bar{a}$ is an element of B' corresponding to a (however from now on we shall use the same symbols as the elements of B to denote elements of B' and shall not use overbar symbols for our convenience). Note that A' is a submonoid of B' and y does not have a zig-zag over A'. By our assumption 2, let C be a monoid and $f, g : B' \to C$ be homomorphisms such that $f \restriction_{A'} = g \restriction_{A'}$ and $f(y) \neq g(y)$. Let $D = \{b \in B' : f(b) = g(b)\}$. It follows that $x_{\alpha(j)} \in D$ and $x_{\beta(j)} \notin D$ for all $j \in \mathbb{N}$. Setting $X = \{i : x_i \in D\}$ we obtain $(\forall j)(\alpha(j) \in X \wedge \beta(j) \notin X)$. Thus by Lemma 1.13, we have weak König's lemma. This completes the proof of $2 \to 1$. □

Next we state the equivalence between ACA_0 and the existence of dominions.

Theorem 4.5. The following are equivalent over RCA_0.

1. ACA_0.
2. If A is a submonoid of B, the dominion of A exists.

Proof. $(1 \to 2)$. We reason within ACA_0. By Theorem 4.4, we have Isbell's zig-zag theorem for countable monoids. Then, b is dominated by A if and only if b has a zig-zag over A. The right-hand side of this equivalence is arithmetical. Hence, by arithmetical comprehension, we obtain the dominion of A. This completes the proof of $1 \to 2$.

$(2 \to 1)$. We reason within RCA_0. Instead of proving ACA_0 directly, we will prove the equivalent statement Lemma 1.9.3. Let $\alpha : \mathbb{N} \to \mathbb{N}$ be a given one-to-one function. Let $B = \bigoplus_{i\in\mathbb{N}} \mathbb{Z}x_i$ be the free abelian group generated by a set of indeterminates $\{x_0, x_1, x_2, \dots\}$. Define a sequence of submonoids $\langle A_i : i \in \mathbb{N}\rangle$ of B as $A_i = \{0_B\} \cup \{jx_i : (\exists j' < j)(f(j') = i)\}$ where 0_B is the identity of B. It follows that $A_i = \begin{cases} \{0_B, (j+1)x_i, (j+2)x_i, \dots\} & \text{if } \alpha(j) = i, \\ \{0_B\} & \text{if no such } j \text{ exists.} \end{cases}$ Let $A = \bigoplus_{i\in\mathbb{N}} A_i$ as a subset of B. Note that A is a submonoid of B. By our assumption 2, let D be the dominion of A. We shall show that $x_i \in D \leftrightarrow (\exists j)(\alpha(j) = i)$ for all $i \in \mathbb{N}$. If $(\exists j)(\alpha(j) = i)$ then x_i has a zig-zag and hence dominated by A. To show the converse direction, let $\neg(\exists j)(\alpha(j) = i)$. Define a pair of homomorphisms $f, g : B \to B$ as f is the identity map and $g(\sum j_k x_k) = \sum_{k\neq i} j_k x_k$. It follows that $f \restriction_A = g \restriction_A$ and $f(x_i) = x_i \neq 0_B = g(x_i)$. Thus x_i is not dominated by A. Hence, by Δ^0_1 comprehension, we obtain $(\exists X)(\forall i)(i \in X \leftrightarrow (\exists j)(\alpha(j) = i))$. Thus by Lemma 1.9, we have arithmetical comprehension. This completes the proof of $2 \to 1$. □

Finally, we show that in standard literatures they show the strictly stronger assertion (2 of the proposition below) than the zig-zag theorem.

Theorem 4.6. The following are equivalent over RCA_0.

1. ACA_0.
2. If A is a submonoid of B, then there exist a monoid C and a pair of homomorphisms $f, g : B \to C$ satisfying following two conditions
   - $f \restriction_A = g \restriction_A$,
   - $f(b) = g(b)$ if and only if b has a zig-zag over A $(b \in B)$.

Proof. $(1 \to 2)$. We carry out Hoffman's proof [32] within ACA_0. For given monoids $A \subset B$, let M and R be the monoid and the binary relation on M same as the proof of Theorem 4.4. By the argument in Hoffman's proof in [32], b has a zig-zag over A if and only if there is a sequence of M such that

$$b| = w_1 \wedge w_1 R w_2 \wedge w_2 R w_3 \wedge \cdots \wedge w_{n-1} R w_n \wedge w_n = |b \ (2 \leq n, w_i \in M).$$

By Theorem 2.3, there exists the transitive closure R' of R. R' is a congruence of M, giving rise to a quotient monoid $C = M/R'$. Define $f, g : B \to C$ by $f(b) = b$ and $g(b) = |b|$ for all $b \in B$. Clearly C, f and g have the desired properties. This completes the proof of $1 \to 2$.

$(2 \to 1)$. We reason within RCA_0. By Theorem 4.5, it suffices to show that for a given monoids $A \subset B$ there exists the dominion of A. Let $A \subset B$ be monoids. By our assumption 2, let C be a monoid and $f, g : B \to C$ be homomorphisms such that $f(b) = g(b)$ if and only if b has a zig-zag over A. Letting $D = \{b \in B : f(b) = g(b)\}$, we see that D is the dominion of A. This completes the proof of $2 \to 1$. □

4.3 Rees Theorem

In this section we explore the logical strength of the Rees theorem for countable semigroups. Similarly as the Artin-Wedderburn theorem which motivated the Rees theorem, this theorem reveals the structure of a certain class of semigroups.

The following definitions are made in RCA_0. Let S be a semigroup without zero. S is called *simple* if $(\forall s, t \in S)(\exists a, b \in S)(asb = t)$. If S is simple then S has no proper ideals. Define the partial order on the set of all idempotents in S as $e \leq_S f$ if $ef = fe = e$. S is called *complete* if there exists a minimal element with respect to this order. The next is the example of a complete and simple semigroup.

Definition 4.7 (Rees Matrix Semigroup)**.** The following definitions are made in RCA_0. Let G be a countable group (for the notion of countable groups, see Section 5), I and Λ be nonempty sets, and $P : \Lambda \times I \to G$. Let $|S| = I \times G \times \Lambda$ and define the binary operation $\cdot_S$ on $|S|$ by putting $(i, a, \lambda) \cdot_S (j, b, \mu) = (i, aP(\lambda, j)b, \mu)$. The system $(|S|, \cdot_S)$ forms a countable semigroup and is called a *Rees matrix semigroup* and denoted by $M(G; I, \Lambda, P)$.

We can easily prove within RCA_0 that a Rees matrix semigroup does not have a zero, simple, and complete. In fact, every idempotent of a Rees matrix semigroup is minimal. the Rees Theorem states that the converse holds, namely that every simple and complete semigroup without zero is isomorphic to some Rees matrix semigroup. (The Rees theorem for semigroups with 0 is also available. However we do not treat this part to simplify the argument.) We can prove the theorem within ACA_0.

Proposition 4.8. ACA_0 proves the Rees theorem for countable semigroups.

Proof. The proof of Theorem 3.2.3 in Howie [36] can be carried out within ACA_0 by means of Theorem 2.5. □

It is expected that the reversal holds, that is, the Rees theorem implies arithmetical comprehension over RCA_0. Reasoning within RCA_0, there exists the left equivalence $\{(s, t) \in S \times S : (\exists x, y \in S)(xs = t \wedge yt = s)\}$ of a Rees matrix semigroup $S = M(G; I, \Lambda, P)$ for we know the structure of the semigroup. In fact, (i, a, λ) and (j, b, μ) are left equivalent if and only if $\lambda = \mu$. So one strategy is to find a simple and complete semigroup without zero whose left equivalence computes the image of a given injection. More precisely, it is enough to show following in order to show the reversal.

Conjecture 4.9. The following implies ACA_0 over RCA_0. Let S be a simple and complete semigroup without zero. Then the left equivalence $\{(s, t) \in S \times S : (\exists x, y \in S)(xs = t \wedge yt = s)\}$ exists.

We have only partial results.

Proposition 4.10. The following implies ACA_0 over RCA_0. Let S be a complete semigroup without zero. Then the left equivalence $\{(s, t) \in S \times S : (\exists x, y \in S)(xs = t \wedge yt = s)\}$ exists.

Proof. Reasoning within RCA_0 we show arithmetical comprehension via Lemma 1.9. Let $\alpha : \mathbb{N} \to \mathbb{N}$ be a one-to-one function. By Δ^0_1 comprehension, let $S = \bigoplus_{i \in \mathbb{N}} \mathbb{N}x_i / (2j+3)x_{\alpha(j)} = 0, j \in \mathbb{N}$. Define an associative operation $+_S$ on S as a usual component-wise addition. An identity of S is an only idempotent of S hence S is complete. Clearly S does not have a zero. By our assumption, let L be a left equivalence on S. It follows that $i \in \mathrm{Im}\alpha$ if and only if $x_i L x_i$. Therefore by Δ^0_1 comprehension the image of α exists. This completes the proof. (Note that S is not simple.) □

Question 4.11. Does or does not the Rees theorem for countable semigroups imply ACA_0?

5 Countable Groups

In this chapter we do Reverse Mathematics of countable group theory. Section 5.1 is strongly effected by Downey et al. [13, 14]. Section 5.2 develops theory of neat subgroups by Honda in second order arithmetic. Section 5.3 and 5.4 is respectively devoted to Reverse Mathematics of normalizers and abelianizers. Abelianizers are as known as derived subgroups or commutator groups.

5.1 Basic Notions

The following definitions are made in RCA_0. A *countable group* G consists of a nonempty set $|G| \subset \mathbb{N}$ together with a binary operation $\cdot_G : |G|^2 \to |G|$, a unary operation ${}^{-1_G} : |G| \to |G|$, and a distinguished element $e_G \in |G|$ such that the system $(|G|, \cdot_G, {}^{-1_G}, e_G)$ obeys the usual group axioms. For notational convenience we write $|G|$ as G and $g \cdot_G h$ as gh for $g, h \in G$. If the binary operation satisfies the commutativity, then G is said to be a *countable abelian group*. In this case we often write $\cdot_G$ as $+_G$, ${}^{-1_G}$ as $-_G$, and e_G as 0_G additively.

Various notions such as *subgroups*, *normal subgroups*, *homomorphisms*, or *isomorphisms* are made in a straightforward way. Moreover, RCA_0 establishes the following facts (cf. Solomon [65, Appendix]);

1. Given a normal subgroup N of a countable group G we can form the *quotient group* G/N of G by N.
2. Given a (possibly infinite) sequence of countable groups $\langle G_i : i \in \mathbb{N} \rangle$ we can form the *direct sum* $\bigoplus_{i \in \mathbb{N}} G_i$ of $\langle G_i : i \in \mathbb{N} \rangle$.
3. Given two countable groups G_0 and G_1 we can form the *free product* $G_0 * G_1$ of G_0 and G_1.
4. Given a (possibly infinite) set $S \subset \mathbb{N}$ we can form the free group and the free abelian group generated by S. We call S the set of *indeterminates* or *alphabets*.

For 1, we define the elements of G/N as the minimal (with respect to the order on the natural numbers) representatives of the equivalence classes under the equivalence relation induced by N. The operations on G/N are defined appropriately, cf. Simpson [61, Definition III.5.2]. For 2, 3, and 4, note that the elements in each case can be encoded as finite sequences of elements of given countable groups or alphabets. Especially, an element of the free group generated by S (as known as a *word*) is of a form $aabca^{-1}bbac^{-1}$ where $a, b, c \in S$. We define the *exponent* of each occurrence of an alphabet in a word as follows; the exponents of x is 1 and the exponents of x^{-1} is -1. We can also define the appropriate operations in each case.

Definition 5.1 (presented groups)**.** The following definition is made in RCA_0. Let $G = F(\{x_0, x_1, \dots\})$ be a free group with infinite alphabets and $R \subset G$. Assume $(\exists N)(N = \langle\langle R \rangle\rangle)$ where $\langle\langle R \rangle\rangle$ denotes the normal subgroup generated

by R, i.e., the subgroup generated by elements of R and their conjugates. We say that G/N is a *presented group by the generator* $\{x_0, x_1, \dots\}$ *and the relator* R and write it as $\langle\{x_0, x_1, \dots\} \mid R\rangle$.

Note that proving $(\exists N)(N = \langle\langle R\rangle\rangle)$ within RCA_0 corresponds to showing that the *word problem* for $G/\langle\langle R\rangle\rangle$ is solvable.

In the rest of this section we consider the existence of subgroups in terms of Reverse Mathematics. In ordinary group theory it is known that the class of subgroups of a group forms a lattice with respect to set inclusion. Given two subgroups of a group, the *meet* of them is the intersection of them and the *join* of them is the group generated by them. The join of subgroups are also known as the *sum* of them. It is fairly easy to see that the existence of the meet can be proved in RCA_0. We show that proving the existence of the join requires ACA_0 even in the case of a direct sum of an abelian group. Note that the direct sum in this context differs from the previous notion. The direct sum in question is a subset of the original group. Eventually within RCA_0 we can form a group isomorphic to the direct sum outside of the original group since the direct sum is definable by a Σ^0_1 formula, see Simpson [61, Lemma II.3.7].

Proposition 5.2. The following are equivalent over RCA_0.

1. ACA_0.
2. $H + I$, the generated subgroup by $H \cup I$ exists for any subgroups H, I of any countable group G.
3. $B \oplus C$, the generated subgroup by $B \cup C$ exists for any subgroups B, C of any countable abelian group A provided that $B \cap C = \{0_A\}$.

Proof. The implications $1 \to 2$ is easy and $2 \to 3$ is trivial. It remains to prove $3 \to 1$. We reason within RCA_0. Instead of showing ACA_0 we shall prove the equivalent statement Lemma 1.9.2. Let $\alpha : \mathbb{N} \to \mathbb{N}$ be a one-to-one function. Let $A = (\bigoplus_{i\in\mathbb{N}} \mathbb{Z}x_i) \oplus (\bigoplus_{i\in\mathbb{N}} \mathbb{Z}y_i)$ be the free abelian group generated by the infinite set of indeterminates $\{x_i, y_i : i \in \mathbb{N}\}$. Let B be the subgroup of A generated by $\{(j+1)x_{\alpha(j)} + (j+1)y_{\alpha(j)} : j \in \mathbb{N}\}$. B is defined by Δ^0_1 comprehension as follows: An element $\sum_{i=0}^m q_i x_i + \sum_{i=0}^m r_i y_i$ $(q_i, r_i \in \mathbb{Z})$ belongs to B if and only if

- $(\forall i \le m)(q_i = r_i)$, and
- $(\forall i \le m)[q_i \neq 0 \to (\exists j, s \le |q_i|)(\alpha(j) = i \wedge (j+1)s = |q_i|)]$.

Similarly, let C be the subgroup of A generated by $\{(j+2)x_{\alpha(j)} + (j+1)y_{\alpha(j)} : j \in \mathbb{N}\}$. It follows that $B \cap C = \{0_A\}$ and hence $B \oplus C$ exists by our assumption 3. Then for all $i \in \mathbb{N}$ we have $(\exists j)(\alpha(j) = i) \leftrightarrow x_i \in B \oplus C$. It follows by Δ^0_1 comprehension that the image of α exists. This completes the proof. □

In [13,14], Downey, Hirschfeldt, Kach, Lempp, Mileti, and Montálban showed the following.

- Over RCA_0, WKL_0 is equivalent to the statement "Every countable commutative ring with identity that is not a field has a nontrivial proper ideal".
- Over RCA_0, ACA_0 is equivalent to the statement "Every countable commutative ring with identity that is not a field has a finitely generated nontrivial proper ideal"
- Over RCA_0, WKL_0 is equivalent to the statement "Every countable vector space of dimension greater than one (over an infinite field) has a nontrivial proper subspace".
- Over RCA_0, ACA_0 is equivalent to the statement "Every countable vector space of dimension greater than one (over an infinite field) has a finite-dimensional nontrivial proper subspace".

We shall show similar results of countable groups by slightly modifying the construction of [13].

Theorem 5.3. The following are equivalent over RCA_0.

1. WKL_0.
2. Every nontrivial countable group that is not a cyclic group of prime order has a nontrivial proper subgroup.
3. Every nontrivial countable abelian group that is not a cyclic group of prime order has a nontrivial proper subgroup.

Proof. The implication $1 \to 2$ is easy and $2 \to 3$ is trivial. It remains to prove $3 \to 1$. We reason within RCA_0. Instead of showing WKL_0 we shall prove the equivalent statement Lemma 1.13.2. Let $\alpha, \beta : \mathbb{N} \to \mathbb{N}$ be functions such that $\mathrm{Im}\alpha \cap \mathrm{Im}\beta = \emptyset$. We may assume that $\mathrm{Im}\alpha \cup \mathrm{Im}\beta \neq \mathbb{N}$. Let $\mathrm{Im}^s\alpha = \{n : (\exists m < s)(\alpha(m) = n)\}$ and $\mathrm{Im}^s\beta = \{n : (\exists m < s)(\beta(m) = n)\}$. Let $V^\infty = \bigoplus_{i\in\mathbb{N}} \mathbb{Q}e_i = \langle v_i : i \in \mathbb{N}\rangle$ be the vector space over rational numbers on the basis $e_0, e_1, \ldots$ and suppose that the elements are listed as $v_0, v_1, \ldots$. Fix a one-to-one function $g : \mathbb{N}^3 \to \mathbb{N}$ such that $g(i, j, n) >$ maximum of the index numbers of the basis appears in the expression of v_i and v_j for any $i, j, n \in \mathbb{N}$. For example, if $v_1 = 2e_3 + 4e_5 + 6e_7$ and $v_{10} = 20e_{30} + 40e_{50} + 60e_{70}$ then $g(1, 10, 100) > 70$. This is the very same setting as in Proof of Theorem 1.5 of [13] where $F = \mathbb{Q}$. Note that $\mathrm{Im}\alpha$, $\mathrm{Im}^s\alpha$, $\mathrm{Im}\beta$, and $\mathrm{Im}^s\beta$ correspond to A, A_s, B, and B_s in the proof respectively. In the construction of $U_2, U_3, U_4, \ldots$, each λ can be taken as an integer in the case of $n \in \mathrm{Im}^s\alpha$. Meanwhile, in the case of $n \in \mathrm{Im}^s\beta$, each λ can be of the form $1/k$ where k is an integer. Therefore it follows that there exists a nontrivial proper subspace U of V^∞ such that for any $i, j, n \in \mathbb{N}$ if $v_i, v_j \notin U$ then

- $n \in \mathrm{Im}\alpha \to (\exists k \in \mathbb{Z})(x_{h(i,j,n)} - kv_i \in U)$ for some nonzero $k \in \mathbb{Z}$, and
- $n \in \mathrm{Im}\beta \to (\exists k \in \mathbb{Z})(kx_{h(i,j,n)} - v_j \in U)$ for some nonzero $k \in \mathbb{Z}$.

Viewing V^∞ as an abelian group with respect to the addition and U as a subgroup of V^∞, let $G = V^\infty/U$ be the quotient group of V^∞ by U. Since $e_{g(1,2,n)}$ has infinite order modulo U, G is not a cyclic group of prime order. Apply the assumption 3 to obtain a nontrivial proper subgroup H of G. Let W be a subgroup of V^∞ corresponding to H and take $v_i \in W \setminus U$ and $v_j \in V^\infty \setminus W$. It follows that $S = \{n : e_{g(i,j,n)} \in W\}$ is a separator of Imα and Imβ. This completes the proof. □

In the proof above, W may not be a subspace of V^∞ viewed as a vector space although it is a subgroup of V^∞ viewed as an abelian group. The theorem above suggests that RCA_0 is not strong enough and WKL_0 is sufficiently strong to develop the usual basic group theory using notions of subgroups. In fact, Theorem 5.7, Theorem 5.13, and Theorem 5.17 illustrates this. Similarly as [13], we have the following theorem combining the above results with Arslanov's Completeness Criterion [2].

Theorem 5.4. The following are equivalent over RCA_0.

1. ACA_0.
2. Every nontrivial countable group which is not a cyclic group of prime order has a finitely generated nontrivial proper subgroup.
3. Every nontrivial countable abelian group which is not a cyclic group of prime order has a finitely generated nontrivial proper subgroup.

5.2 Neat Subgroups

In this section we develop the theory of neat subgroups of countable abelian groups in second order arithmetic. We also give some Reverse Mathematics results. This work is intended as a survey or an introduction of the topic of abelian group theory, for now it is hard to find organized reports about it. The notion of essential subgroups and neat subgroups appears in Honda [33](1956), where he used the different terminology "rich" instead of "essential". See also Fuchs [19, section 28](1958), Honda-Nagata [34](1969), and Fuchs [20](1970). The notion of neat hulls appears implicitly in Fuchs [19, page 92, i)]. Rangaswamy continued to study neat hulls, cf., for example, [51]. The definition of divisible closures of Simpson [61, Definition III.6.3] mentions essentiality.

Definition 5.5. The following definitions are made in RCA_0.

1. A subgroup A of a countable abelian group G is an *essential subgroup* of G if
$$(\forall g \in G)(g \neq 0_G \to (\exists n \in \mathbb{N})(ng \in A \setminus \{0_G\})).$$
2. A subgroup M of a countable abelian group G is an *essentially closed subgroup* of G or is *essentially closed* in G if
$$(\forall g \in G \setminus M)(\exists n \in \mathbb{Z})(\exists h \in M)(ng+h \neq 0_G \wedge (\forall m \in \mathbb{N})(m(ng+h) \notin M \setminus \{0_G\})).$$

3. A subgroup N of a countable abelian group G is a *neat subgroup* of G or is *neat* in G if

$$N \cap pG = pN, \text{i.e., } (\forall g \in G)(pg \in N \to (\exists a \in N)(pg = pa))$$

for any prime p.

4. Let A and M be subgroups of a countable abelian group G. We say that M is an *essential closure* of A in G if A is an essential subgroup of M and M is essentially closed.

5. Let A, N be subgroups of a countable abelian group G. We say that N is a *neat hull* of A in G if A is a subgroup of N, N is a neat subgroup of G, and there does not exist a neat subgroup N' of G such that $A \subset N' \subsetneq N$.

Although the definitions above may appear more intricate than the standard ones, we choose the equivalent formulations to avoid second order quantification in the light of our weak base theory. For instance, the last part of the second clause states the maximality of M; M is no longer an essential subgroup of the subgroup generated by $M \cup \{g\}$. The proposition below itemizes the results we can prove within RCA_0.

Proposition 5.6. The following are provable in RCA_0.

1. The property of being a neat subgroup is transitive, that is, the following holds. Let A be a neat subgroup of a countable abelian group G and B be a neat subgroup of A. Then B is a neat subgroup of G.

2. Let A be a subgroup of a countable abelian group G. A is essentially closed in G if and only if A is a neat subgroup in G.

3. Let A, M be subgroups of a countable abelian group G. If M is an essential closure of A in G then M is a neat hull of A in G.

Proof. (1). Let p be a prime and $g \in G$ satisfy $pg \in B$ ($\subset A$). Since A is neat in G, there exists $a \in A$ such that $pa = pg \in B$. Since B is neat in A, there exists $b \in B$ such that $pb = pa = pg$. Thus B is neat in G. This completes the proof of 1.

(2). First suppose that A is a neat subgroup of G and, for a contradiction, that A is not essentially closed in G. Take $g \in G \setminus A$ such that A is an essential subgroup of the subgroup generated by $A \cup \{g\}$. By Σ^0_0 induction, let $n \geq 2$ be the smallest natural number such that $ng \in A$. Put $n = pn'$ where p is a prime. Since $pn'g \in A \cap pG$ and A is a neat subgroup of G, we have $a \in A$ such that $pn'g = pa$. Put $g' = n'g - a$ and suppose, for a contradiction, that $g' \notin A$. Let $m \geq 2$ be a natural number such that $mg' \in A \setminus \{0_G\}$ (such m exists since g' is generated by $A \cup \{g\}$ and $g' \neq 0_G$). Since $pg' = 0_G$ it follows that $p \not| m$. By Euclid's algorithm which is provable in RCA_0, let $k, l \in \mathbb{Z}$ be such that $kp + lm = 1$. We have $A \ni lmg' = (1 - kp)g' = g' - kpg' = g'$, a contradiction. It follows that $g' \in A$. Therefore $n'g \in A$, a contradiction with the minimality of n.

Next suppose that A is not a neat subgroup of G and take a prime p and $g \in G$ such that $(pg \in A) \wedge (pg \notin pA)$. We show that A is an essential subgroup of the subgroup generated by $A \cup \{g\}$, which implies that A is not essentially closed. Take a non-zero element g' generated by $A \cup \{g\}$ with the plan of finding a natural number n such that $ng' \in A \setminus \{0_G\}$. If $g' \in A$ nothing is to be proved. If not, it follows that $(\exists n \geq 2)(ng' \in A)$. If $ng' \neq 0_G$ nothing is to be proved. If not, by Σ^0_0 induction, take the smallest natural number $n \geq 2$ such that $ng' = 0_G$. Put $n = qn'$ where q is a prime. We have $qn'g' = 0_G$ and $n'g' \neq 0_G$ by the minimality of n. Suppose, for a contradiction, that $n'g' \notin A$ and let $n'g' = a + kg$ $(a \in A, 0 < k < p)$. Suppose, for a contradiction, that $q = p$. We have $0_G = qn'g' = pn'g' = p(a + kg) = pa + kpg$. Therefore we have $pa = -kpg$. By Euclid's algorithm, let $l, m \in \mathbb{Z}$ be such that $lp + mk = 1$. We have $mpa = -mkpg = (lp - 1)pg$. Therefore we have $pg = p(lpg - ma) \in pA$, a contradiction. It follows that $q \neq p$. Again by Euclid's algorithm, let $i, j \in \mathbb{Z}$ be such that $ip + jq = 1$. We have $0_G = jqn'g' = (1 - ip)n'g' = n'g' - ipn'g'$ and hence $n'g' = ipn'g' \in A$, a contradiction. (Note that $pg' \in A$.) It follows that $n'g' \in A \setminus \{0_G\}$. This completes the proof of 2.

(3). By the definition, M is essentially closed in G. It follows from 1 that M is a neat subgroup in G. Suppose that M' is a subgroup of G such that $A \subset M' \subsetneq M$ and let $g \in M \setminus M'$. It follows that M' is an essential subgroup of the subgroup generated by $M' \cup \{g\}$ since, by the definition, A is an essential subgroup of M. Therefore M' is not essentially closed in G. It follows again from 1 that M' is not a neat subgroup in G. Thus M is a neat hull of A in G. This completes the proof of 3. □

The theorem below indicates that WKL_0 is strong enough to conclude that essential closures and neat hulls are the same notion. One possible reason why weak König's lemma is required is that in the definition of neat hulls we do mention set quantifiers. However, unlike maximality, it does not seem easy to define minimality of a subgroup without mentioning other subgroups.

Theorem 5.7. The following is provable in WKL_0. Let A, M be subgroups of a countable abelian group G. If M is a neat hull of A in G then M is an essential closure of A in G.

Proof. [5] Suppose that M is a neat hull of A in G. Since M is neat in G, it follows that M is essentially closed in G by Proposition 5.6.2. It remains to show that A is an essential subgroup of M.

First we show that M/A is torsion via weak König's lemma. Suppose not, for a contradiction, and let $g^* \in M \setminus A$ witness that M/A is not torsion. We shall construct a neat subgroup M' of M such that $A \subset M'$ and $g^* \notin M'$. Let $\langle g_i : i \in \mathbb{N} \rangle$ be a one-to-one enumeration of the elements of M such that $g_0 = 0_G$ and $g_1 = g^*$. Let T be the set of all $t \in 2^{<\mathbb{N}}$ such that

1. $0 < \mathrm{lh}(t) \to t(0) = 1$;

[5] The proof is essentially by Fumiya Nakashima.

2. $1 < \mathrm{lh}(t) \to t(1) = 0$;

3. $\forall i < \mathrm{lh}(t)(g_i \in A \to t(i) = 1)$;

4. $\forall i, j, k < \mathrm{lh}(t)(g_i -_G g_j = g_k \wedge t(i) = t(j) = 1 \to t(k) = 1)$;

5. $\forall i, j, k < \mathrm{lh}(t)(p_i g_j = g_k \wedge t(k) = 1 \to t(j) = 1)$ where p_i is the i-th prime.

Clearly T is a tree. We claim that T is infinite. To see this, let $m \in \mathbb{N}$ be given. Define a Σ^0_1 formula $\varphi(i) \equiv (\exists n > 0)(ng_i \in A)$. By bounded Σ^0_1 comprehension, let $Y = \{i < m : \varphi(i)\}$. Define $t \in 2^{<\mathbb{N}}$ of length m by putting $t(i) = 1$ if $i \in Y$, $t(i) = 0$ otherwise. Then $t \in T$ and $\mathrm{lh}(t) = m$. This proves that T is infinite. By weak König's lemma, let f be a path through T. Let M' be the set of all $g_i \in M$ such that $f(i) = 1$. Clearly M' is a neat subgroup of M. Since M is neat in G it follows that M' is neat in G. This contradicts minimality of M. Thus M/A is torsion.

Second we show that A is an essential subgroup of M. Suppose, for a contradiction, that A is not an essential subgroup of M. Then we can take $g^* \in M \setminus A$ and a prime p such that $pg^* = 0_G$ (cf. [33, Proposition 5]). In fact, since M/A is torsion and A is not an essential subgroup of M, there exists $g \in M \setminus A$ and $n \geq 2$ such that $ng = 0_G$. By Σ^0_0 induction, we may assume that n is the smallest natural number such that $ng = 0_G$. Put $n = pn'$ where p is a prime and $g^* = n'g$. Clearly g and p have desired property. Now we shall construct a maximal subgroup $M' \subset M$ such that $A \subset M'$ and $g^* \notin M'$. Let us say that a finite set $X \subset M$ is *good* if $g^* \notin \langle X \cup A \rangle$. We show that "$X$ is good" is Δ^0_1. Let $X = \{h_0, h_1, \ldots, h_n\}$. From the fact that $(\forall i \leq n)(\exists m > 0)(mh_i \in A)$, by Σ^0_0 bounding, we have $(\exists b)(\forall i \leq n)(0 < \exists m < b)(mh_i \in A)$. Thus "$X$ is good" is equivalent to the bounded sentence $(\exists k_0, k_1, \ldots, k_n < b)(g^* - \sum_{i=0}^n k_i h_i \in A)$. Let $\langle g_i : i \in \mathbb{N} \rangle$ be a one-to-one enumeration of the elements of M. Define $f : \mathbb{N} \to \{0, 1\}$ by primitive recursion putting $f(i) = 1$ if $\{g_j : j < i \wedge f(j) = 1\} \cup \{g_i\}$ is good, $f(i) = 0$ otherwise. Let M' be the set of all $g_i \in M$ such that $f(i) = 1$. This completes the construction of M'. We show that M' is essentially closed in M. We have$(\forall g \in M \setminus M')(g^* \in \langle M' \cup \{g\} \rangle)$ by maximality of M'. It is enough to show that $(1 < \forall k < p)(kg^* \notin M')$. By Euclidean algorithm, we have $(\exists n, m \in \mathbb{Z})(np + mk = 1)$. It follows that $m(kg^*) = (1 - np)g^* = g^*$ and $kg^* \notin M'$. Therefore M' is essentially closed in M, and it follows by Proposition 5.6.2 that M' is a neat subgroup of M. Thus, by Proposition 5.6.1, M' is a neat subgroup of G and this contradicts the minimality of M. This completes the proof.

□

It is expected that the reversal of the theorem above also holds. The method of Proof of Theorem 5.3 is not applicable for the subgroup U is unfortunately neat in V^∞.

Question 5.8. Does the following statement implies WKL_0 over RCA_0? Let A, M be subgroups of a countable abelian group G. If M is a neat hull of A in G then M is an essential closure of A in G.

In ordinary abelian group theory, it is common to use Zorn's lemma to prove that every subgroup of an abelian group has an essential closure or a neat hull. We show that (countable version of) this statement is equivalent to ACA_0 over RCA_0.

Theorem 5.9. The following are equivalent over RCA_0.

1. ACA_0.
2. If A, B, and C are subgroups of a countable abelian group G such that B is an essential subgroup of C and $B \subset A \subset C$, then there exists an essential closure M of A in G such that $C \subset M$.
3. For a subgroups A of a countable abelian group G, there exists an essential closure M of A in G.
4. Let A be a subgroup of a countable abelian group G. Then there exists a neat hull N of A in G.

Proof. $(1 \to 2)$. We reason within ACA_0. Let us say that a subset X of G is *good* if any element $g \neq 0_G$ generated by elements of X satisfies $(\exists n \in \mathbb{N})(ng \in A \setminus \{0_G\})$. Note that the predicate "good" is arithmetical. Obviously C is good. Let $\langle g_i : i \in \mathbb{N} \rangle$ be a one-to-one enumeration of $G \setminus C$. Using arithmetical comprehension, define a function $f : \mathbb{N} \to \{0, 1\}$ by primitive recursion putting $f(i) = 1$ if $C \cup \{g_j : j < i \wedge f(j) = 1\} \cup \{g_i\}$ is good, $f(i) = 0$ otherwise. Let M be C plus the set of all g_i such that $f(i) = 1$. Clearly $C \subset M$. By checking $(\forall g, h \in M)(g -_G h \in M)$ we see that M forms a group. It is also easy to check that M is an essential closure of A in G. This completes the proof of $1 \to 2$.

$(2 \to 3)$. Let $A = B = C$ and apply 2.

$(3 \to 4)$. If we have an essential closure M of A in G, then, by Theorem 5.7 and weak König's lemma which is provable in ACA_0, M is a neat hull of A in G.

$(4 \to 1)$. We reason within RCA_0. Instead of showing arithmetical comprehension directly, we will show the equivalent statement Lemma 1.9.2. Let $\alpha : \mathbb{N} \to \mathbb{N}$ be a one-to-one function. Let $G = \bigoplus_{i=0}^{\infty} \mathbb{Z}x_i$ be the free abelian group generated by the infinite set of indeterminates $\{x_i : i \in \mathbb{N}\}$. By Δ_1^0 comprehension, define a subgroup A of G as

$$\sum_{i=0}^{n} q_i x_i \in A \leftrightarrow (\forall i \leq n)(q_i \neq 0 \to (\exists j, s \leq |q_i|)(\alpha(j) = i \wedge p_j s = |q_i|))$$

where p_j is the j-th prime.

By our assumption 2 there exists a neat hull N of A in G. We claim that $(\forall i)(i \in \mathrm{Im}\alpha \leftrightarrow x_i \in N)$. First suppose that $i \in \mathrm{Im}\alpha$ and $\alpha(j) = i$. Then $p_j x_i \in N$ and since N is neat there exists $g \in N$ such that $p_j x_i = p_j g$. It follows that $g = x_i$ and this belongs to N. Next suppose that $i \notin \mathrm{Im}\alpha$. By Δ_1^0 comprehension, define a subgroup N' of G as

$$g \in N' \leftrightarrow g \in N \wedge \text{the } i\text{-th component of } g \text{ equals } 0.$$

It is easily seen that $N' \subset N$ and N' is neat. By the minimality of N we have $N' = N$ and $x_i \notin N$. Hence, by Δ^0_1 comprehension, the image of α exists. This completes the proof of $4 \to 1$. □

It should be noted that under the assumption that an essential closure of a subgroup exists, we can easily prove in RCA_0 that essential closures and neat hulls are the same notion. We establish this for convenience of the reader who has little interest in Reverse Mathematics.

Proposition 5.10. The following are provable in RCA_0. Assume that every subgroup of a countable abelian group has an essential closure. Let A, M be subgroups of a countable abelian group. If M is a neat hull of A in G then M is an essential closure of A in G.

Proof. Suppose that M is a neat hull of A in G. Since M is neat in G, by Proposition 5.6.2, it follows that M is essentially closed in G. It remains to show that A is an essential subgroup of M. By our assumption, let M' be an essential closure of A in M. By Proposition 5.6.2, M' is neat in M. Therefore M' is neat in G by Proposition 5.6.1. By the minimality of M, we have $M = M'$. Since A is an essential subgroup of M', A is an essential subgroup of M. This completes the proof. □

5.3 Normalizers

In this section we consider the existence and the characterization of normalizers in terms of Reverse Mathematics. Solomon [66] showed that the existence of the center of a countable group is equivalent to ACA_0 over RCA_0. We show that the existence of the normalizer of a subgroup of a countable group is also equivalent to ACA_0 over RCA_0. We also show that a certain formulation of the characterization of normalizers is equivalent to WKL_0 over RCA_0. There are several ways in defining normalizers, which are all equivalent in ordinary mathematics. In the light of our weak base theory, we must be attentive to differences between such definitions for we often require set existence axioms to show the equivalence of different definitions.

Definition 5.11. The following definitions are made in RCA_0. Let G be a countable group, H be a subgroup of G, and N be a subgroup of G including H. We say that

1. N is *a normalizer* of H if H is a normal subgroup of N, (We sometimes abbreviate this by $H \lhd N$.)
2. N is *the largest normalizer* of H if N is a normalizer of H and $N' \subset N$ for any normalizer N' of H,
3. N is a *the* Σ^1_1*-definable normalizer* of H if $(\forall g \in G)(g \in N \leftrightarrow \exists$ normalizer N' of H such that $g \in N'$, (We abbreviate the right-hand side as $g \in \bigcup_{H \lhd N'} N'$.)

4. and N is *the* Π^0_1*-definable normalizer* of H if $(\forall g \in G)(g \in N \leftrightarrow (\forall h \in H)(ghg^{-1} \in H \wedge g^{-1}hg \in H))$.

Reasoning in RCA_0, it is easy to see that

1. N is the largest normalizer if and only if N is the Σ^1_1-definable normalizer,
2. if N is the Π^0_1-definable normalizer then N is the largest normalizer,
3. and if N is the Σ^1_1-definable normalizer then $(\forall g \in G)(g \in N \rightarrow (\forall h \in H)(ghg^{-1} \in H \wedge g^{-1}hg \in H))$,

for given G, H, and N. It seems not to be able to prove the converse implication of 3 in RCA_0—we will consider this matter later. Therefore it is reasonable to take the stronger definition 4 of Definition 5.11 as a standard definition of the normalizer in RCA_0. We show that the existence of normalizers even in the weakest sense requires arithmetical comprehension.

Theorem 5.12. The following are equivalent over RCA_0.

1. ACA_0.
2. For each countable group G and its subgroup H, the largest normalizer of H exists.

Proof. $(1 \rightarrow 2)$. The Π^0_1-definable normalizer $N = \{g \in G : (\forall h \in H)(ghg^{-1} \in H \wedge g^{-1}hg \in H)\}$ of H exists by arithmetical comprehension and N is the largest normalizer of H.

$(2 \rightarrow 1)$. We reason within RCA_0. Instead of proving ACA_0 directly, we will prove the equivalent statement Lemma 1.9.2. Let $\alpha : \mathbb{N} \rightarrow \mathbb{N}$ be a one-to-one function. Define a sequence of sets $\langle H_i : i \in \mathbb{N} \rangle$ by putting $j \in H_i \leftrightarrow (j \neq 0 \rightarrow \alpha(j-1) = i)$. Define a sequence of binary operations on H_i's so that each H_i become a cyclic group of order 2, say $\{e_i, h_i\}$, if $i \in \mathrm{Im}\alpha$, a trivial group otherwise. Define a sequence of groups $\langle G_i : i \in \mathbb{N} \rangle$ by putting $G_i = H_i * \mathbb{Z}$, the free product of H_i and $\mathbb{Z}$.

Now let $G = \bigoplus_{i \in \mathbb{N}} G_i$ and H be a subgroup of G consisting of all elements in which integers do not occur. By our assumption 2, let N be the largest normalizer of H. We show that $i \in \mathrm{Im}\alpha \leftrightarrow (\epsilon_0, \ldots, \epsilon_{i-1}, 1) \notin N$ where each ϵ_k is the identity of G_k. First suppose that $i \in \mathrm{Im}\alpha$. Then $(\epsilon_0, \ldots, \epsilon_{i-1}, 1) \cdot (\epsilon_0, \ldots, \epsilon_{i-1}, h_i) \cdot (\epsilon_0, \ldots, \epsilon_{i-1}, 1)^{-1} \notin H$. It follows that $(\epsilon_0, \ldots, \epsilon_{i-1}, 1) \notin N$ since H is a normal subgroup of N. Second suppose that $i \notin \mathrm{Im}\alpha$. By Δ^0_1 comprehension, define a subgroup N' of G consisting of an element $g \in G$ such that when we replace the i-th component of g by ϵ_i it belongs to N. It is easy to see that N' is a normalizer of H including N. It follows by the maximality of N that $N = N'$ and hence $(\epsilon_0, \ldots, \epsilon_{i-1}, 1) \in N$. Thus the image of α exists by Δ^0_1 comprehension. This completes the proof. □

Note that G in the proof above also serves for showing that the existence of the center implies arithmetical comprehension, since it follows that $i \in \mathrm{Im}\alpha \leftrightarrow (\epsilon_0, \ldots, \epsilon_{i-1}, 1) \notin C$ where C is the center of G.

Now we consider the postponed matter, the Π^0_1-characterization of the normalizer. Consider the logical strength of the following statement, which claims the equivalence between two definitions of normalizers.

> †: Let G be a countable group, H be a subgroup of G, and N be a subgroup of G including H. N is the largest normalizer of G if and only if N is the Π^0_1-definable normalizer.

The statement † can be logically equivalently transformed within RCA_0 and splits into the existential and the characterization problem of normalizers:

$$\begin{aligned}
\dagger &\Longleftrightarrow (\forall G)(\forall H)(\forall N)[N = \bigcup_{H \lhd N'} N' \leftrightarrow N = \{g \in G : (\forall h \in H)(ghg^{-1} \in H \wedge g^{-1}hg \in H)\}] \\
&\Longleftrightarrow (\forall G)(\forall H)(\forall N)[N = \bigcup_{H \lhd N'} N' \rightarrow N \supset \{g \in G : (\forall h \in H)(ghg^{-1} \in H \wedge g^{-1}hg \in H)\}] \\
&\Longleftrightarrow (\forall G)(\forall H)(\forall N)[N = \bigcup_{H \lhd N'} N' \rightarrow \bigcup_{H \lhd N'} N' \supset \{g \in G : (\forall h \in H)(ghg^{-1} \in H \wedge g^{-1}hg \in H)\}] \\
&\Longleftrightarrow (\forall G)(\forall H)[\neg(\exists N)(N = \bigcup_{H \lhd N'} N') \vee (\forall g \in G)(g \in \bigcup_{H \lhd N'} N' \leftarrow (\forall h \in H)(ghg^{-1} \in H \wedge g^{-1}hg \in H)]
\end{aligned}$$

where G, H, and N range over countable groups, subgroups of G, and subgroups of G including H respectively. The left-hand-side of the last disjunction says that there does not exist the largest normalizer. We show that the right-hand-side of the disjunction—the Π^0_1 characterization of the largest normalizer—is provable in WKL_0, and in fact equivalent to WKL_0 over RCA_0.

Theorem 5.13. The following is equivalent over RCA_0.

1. WKL_0.
2. $(\forall g \in G)(g \in \bigcup_{H \lhd N'} N' \leftrightarrow (\forall h \in H)(ghg^{-1} \in H \wedge g^{-1}hg \in H))$ for any countable group G and its subgroup H.

Proof. $(1 \rightarrow 2)$. We have already seen that the implication from left to right is provable in RCA_0. Reasoning in WKL_0, we show the converse direction. Let $\langle g_i : i \in \mathbb{N}\rangle$ be an enumeration of G and assume that g_0 satisfies $(\forall h \in H)(g_0 h g_0^{-1} \in H \wedge g_0^{-1} h g_0 \in H)$. We shall construct a normalizer N' of G such that $g_0 \in N'$ via weak König's lemma. Let T be the set of all $t \in 2^{<\mathbb{N}}$ such that

1. $0 < \mathrm{lh}(t) \rightarrow t(0) = 1$,
2. $\forall i < \mathrm{lh}(t)(g_i \in H \rightarrow t(i) = 1)$,
3. $\forall i, j, k < \mathrm{lh}(t)(t(i) = t(j) = 1 \wedge g_i g_j^{-1} = g_k \rightarrow t(k) = 1)$,
4. $\forall i, j < \mathrm{lh}(t)(g_i \in H \wedge t(j) = 1 \rightarrow g_j g_i g_j^{-1} \in H)$.

Clearly T is a tree. To see that T is infinite, let $m \in \mathbb{N}$ be given. By bounded Π^0_1 comprehension (Theorem 1.5), letting $Y = \{i : i < m \wedge (\forall h \in H)(g_i h g_i^{-1} \in H \wedge g_i^{-1} h g_i \in H)\}$, define $t \in 2^{<\mathbb{N}}$ by $t = \begin{cases} 1 & (i \in Y) \\ 0 & (i \notin Y). \end{cases}$ We see $t \in T$ and hence T is infinite. By weak König's lemma there exists a path f through T. It follows that $N' = \{g_i : f(i) = 1\}$ is a normalizer with desired properties. This completes the proof of $1 \to 2$.

$(2 \to 1)$. Instead of WKL_0 we show the equivalent statement Lemma 1.13.3. Let $\alpha, \beta : \mathbb{N} \to \mathbb{N}$ be one-to-one functions such that $\mathrm{Im}\alpha \cap \mathrm{Im}\beta = \emptyset$. Let G and H be the same as in Proof of Theorem 5.12. Write $(\epsilon_0, \ldots, \epsilon_{i-1}, c)$ as cx_i where $i \in \mathbb{N}$ and $c \in \mathbb{Z}$ and let $R = \{j! x_{\beta(0)} - x_{\beta(j)} : j \in \mathbb{N}\}$. Reasoning in RCA_0, we show that the normal subgroup $\langle\langle R \rangle\rangle$ generated by R exists. Note that the conjugate of an element of R again belongs to R. Given $g \in G \setminus \{0_G\}$, if g is not of the form

$$cx_{\beta(0)} + \sum_{i=0}^{n} c_i x_{k_i} \ (c \in \mathbb{Z}, c_i \in \mathbb{Z} \setminus \{0_{\mathbb{Z}}\})$$

then $g \notin \langle\langle R \rangle\rangle$. Suppose that g is of the form above. We show that $g \in \langle\langle R \rangle\rangle$ if and only if

$$(\exists j_0, j_1, \ldots, j_n \leq |c| + \sum_{i=0}^{n} |c_i|)[(\forall i \leq n)(\beta(j_i) = k_i) \wedge \sum_{i=0}^{n} c_i j_i! = c].$$

In fact, if $g \in \langle\langle R \rangle\rangle$ then

$$(\exists j_0, j_1, \ldots, j_n)[(\forall i \leq n)(\beta(j_i) = k_i) \wedge \sum_{i=0}^{n} c_i j_i! = c].$$

It is enough to show that $(\forall i \leq n)(j_i \leq |c| + \sum_{i=0}^{n} |c_i|)$. Let $j_{i^*} = \max\{j_0, j_1, \ldots, j_n\}$. From

$$c_{i^*} j_{i^*}! = c - \sum_{i \neq i^*} c_i j_i!$$

we have

$$\begin{aligned} |c_{i^*}| j_{i^*}! &\leq |c| + \sum_{i \neq i^*} |c_i| j_i! \\ &\leq |c|(j_{i^*} - 1)! + \sum_{i \neq i^*} |c_i|(j_{i^*} - 1)!. \end{aligned}$$

Therefore we have

$$j_{i^*} \leq (1/|c_{i*}|)(|c| + \sum_{i \neq i^*} |c_i|) \leq |c| + \sum_{i=0}^{n} |c_i|$$

hence

$$(\forall i \leq n)(j_i \leq |c| + \sum_{i=0}^{n} |c_i|).$$

Thus $\langle\langle R\rangle\rangle$ exists by Δ^0_1 comprehension. Let $G' = G/\langle\langle R\rangle\rangle$ and H' be the subgroup of G' consisting of all elements in which integers do not occur. From now on, we identify an element of G with the corresponding element in G'. Since $g = x_{\beta(0)} = (\epsilon_0, \ldots, \epsilon_{\beta(0)-1}, 1)$ satisfies the condition $(\forall h \in H')(ghg^{-1} \in H \wedge g^{-1}hg \in H)$, by our assumption 2, there exists a subgroup N' of G' such that $H' \lhd N' \wedge g \in N'$. It follows that if $i \in \mathrm{Im}\alpha$ then $x_i \notin N'$ and if $i \in \mathrm{Im}\beta$ then $x_i \in N'$. Thus, setting $S = \{n : x_n \in N'\}$ by Δ^0_1 comprehension, a separator of $\mathrm{Im}\alpha$ and $\mathrm{Im}\beta$ exists. This completes the proof of $2 \to 1$. □

By the previous theorem, it follows that the statement †—weaker statement than 2 of the Theorem 5.13— is provable in WKL_0. Although it is expected that the statement † is equivalent to WKL_0 over RCA_0, it seems to require more "recursion theoretic" construction like [13] rather than our method to prove it. Maybe it is not good to stick to calibrate the logical strength of not so natural statement such as †. If we still want to explore, a key to the solution is a kind of non-abelian version of Theorem 5.3. To show the statement † implies WKL_0 over RCA_0 it suffices to show the conjecture below. If we have such a subgroup H then we have a proper subgroup N' of G which strictly includes H by the statement † where $N = H$. It follows that N' encodes a separator of $\mathrm{Im}\alpha$ and $\mathrm{Im}\beta$.

Conjecture 5.14. The following is provable in RCA_0. Let $\alpha, \beta : \mathbb{N} \to \mathbb{N}$ be one-to-one functions such that $\mathrm{Im}\alpha \cap \mathrm{Im}\beta = \emptyset$. Let G be the free group generated by the infinite set of indeterminates $\{x_i : i \in \mathbb{N}\}$. Fix a one-to-one enumeration $\langle g_i : i \in \mathbb{N}\rangle$ of G and a one-to-one function $h : \mathbb{N}^3 \to \mathbb{N}$ such that $h(i,j,k) >$ maximum of the index numbers of the basis occurring in g_i and g_j for any $i, j, k \in \mathbb{N}$. Then there exists a nontrivial proper subgroup H of G such that

- if $n \in \mathrm{Im}\alpha$ then there exists $k \in \mathbb{Z}$ such that $x_{h(i,j,n)} g_i^{-k} \in H$,
- if $n \in \mathrm{Im}\beta$ then there exists $k \in \mathbb{Z}$ such that $x_{h(i,j,n)}^{-k} g_j \in H$,

for all $i, j, n \in \mathbb{N}$ with $g_i, g_j \notin H$,

- H is not a normal subgroup of G, and
- $(\exists g \in G \setminus H)(\forall h \in H)(ghg^{-1} \in H)$.

One of difficulties to prove the conjecture is to show that $g \in \langle Z\rangle$ is Δ^0_1 for an element $g \in G$ and a finite subset $Z \subset G$. Fortunately, Nielsen [50] had solved the *generalized word problem* for free groups (see also [45, pages 131 and 132], [6, page 116], and [47, page 4]). So we only have to check that the algorithm is uniform with respect to Z and does not depend on strong induction.

5.4 Abelianizers (a. k. a. Derived Subgroups or Commutator Groups)

Abelianizers, derived subgroups, and commutator groups all denote the same notion in ordinary group theory. In this section we consider the existence and

the characterization of them. Interestingly enough, we can find the correspondence between the results of normalizers and abelianizers. Consciously of the correspondence we adopt the terminology "abelianizer" although it is less popular than the others.

Definition 5.15. Let G be a countable group and A be a normal subgroup of G. We say that

1. A is *an abelianizer* of G if G/A is abelian, (We sometimes abbreviate this by $A \propto G$. This is a temporary notation only in this thesis.)
2. A is *the smallest abelianizer* of G if A is an abelianizer of G and $A \subset A'$ for any abelianizer A' of G,
3. A is *the* Π^1_1*-definable abelianizer* of G if

$$(\forall g \in G)(g \in A \leftrightarrow g \in A' \text{ for any abelianizer } A' \text{ of } G),$$

   (We abbreviate the right-hand-side as $g \in \bigcap_{A' \propto G} A'$.)

4. and A is *the* Σ^0_1*-definable abelianizer* if A is the subgroup generated by *commutators*, elements of the form $g_0 g_1 g_0^{-1} g_1^{-1}$ $(g_0, g_1 \in G)$. (Note that the subgroup generated by commutators is always normal since

$$c(aba^{-1}b^{-1})c^{-1} = (cac^{-1})(cbc^{-1})(cac^{-1})^{-1}(cbc^{-1})^{-1}.$$

   We abbreviate the right-hand-side as $g \in \langle g_0 g_1 g_0^{-1} g_1^{-1} : g_0, g_1 \in G \rangle$. With this notations the condition of the definition of the Σ^0_1-definable abelianizer is stated as $(\forall g \in G)(g \in A \leftrightarrow g \in \langle g_0 g_1 g_0^{-1} g_1^{-1} : g_0, g_1 \in G \rangle)$.)

Reasoning in RCA_0, it is easy to see that

1. A is the smallest abelianizer if and only if A is the Π^1_1-definable abelianizer,
2. if A is the Σ^0_1-definable abelianizer then A is the smallest abelianizer,
3. and if A is the Π^1_1-definable abelianizer then $(\forall g \in G)(g \in A \leftarrow g \in \langle g_0 g_1 g_0^{-1} g_1^{-1} : g_0, g_1 \in G \rangle)$,

for given G and A. Similarly as in the case of normalizers, it is convenient to adopt the strongest definition when we develop group theory in a weak fragments of second order arithmetic. We first show that the existence of abelianizers even in the weakest sense requires arithmetical comprehension. The characterization of abelianizers will be discussed later.

Theorem 5.16. The following are equivalent over RCA_0.

1. ACA_0.
2. For each countable group G, the set of all commutators exists.
3. For each countable group G, the smallest abelianizer of G exists.

Proof. $(1 \to 2)$. The set of all commutators is definable by a Σ^0_1 formula and exists by arithmetical comprehension. $(1 \to 3)$. The Σ^0_1-definable abelianizer $A = \langle g_0 g_1 g_0^{-1} g_1^{-1} : g_0, g_1 \in G \rangle$ exists by arithmetical comprehension and A is the smallest abelianizer of G.

We show $2 \to 1$ and $3 \to 1$ via Lemma 1.9. Let $\alpha : \mathbb{N} \to \mathbb{N}$ be a one-to-one function. Reasoning in RCA_0, $G = \langle \{a_i, b_i, c_i : i \in \mathbb{N}\} \mid \{a_{\alpha(j)} c_j b_j c_j^{-1} b_j^{-1} : j \in \mathbb{N}\} \rangle$ exists. To see this, let G_0 be the free group generated by the alphabets $\{a_i, b_i, c_i : i \in \mathbb{N}\}$. We shall show that the normal subgroup N generated by $\{a_{\alpha(j)} c_j b_j c_j^{-1} b_j^{-1} : j \in \mathbb{N}\}$ exists. For given $w \in G_0$, let m be the maximum index of b's and c's occurring in w and n be the number of all the occurrences of a's in w. It follows that $w \in N$ if and only if there exists a finite sequence $j_0, j_1, \ldots, j_l \leq m$ $(l < n)$ and occurrences $a_{i_0}, a_{i_1}, \ldots, a_{i_l}$ in w such that $\alpha(j_k) = i_k$ $(0 \leq \forall k \leq l)$ and w is reduced to the empty sequence when each a_{i_k} is replaced by $b_{i_k} c_{i_k} b_{i_k}^{-1} c_{i_k}^{-1}$. Thus N exists by Δ^0_1 comprehension. From now on, we identify an alphabet of G_0 with the corresponding element in G.

$(2 \to 1)$. Let C be the set of all commutators of G. We show that $a_i \in C \leftrightarrow i \in \mathrm{Im}\alpha$. If $i \in \mathrm{Im}\alpha$ we have $a_i = b_j c_j b_j^{-1} c_j^{-1} \in C$ for some $j \in \mathbb{N}$. Suppose that $i \notin \mathrm{Im}\alpha$ and $a_i \in C$ for a contradiction. Then $a_i = ghg^{-1}h^{-1}$ for some $g, h \in G$. Note that the sum of the exponents of a_i's in the right-hand-side equals 0 and a_i will never newly appear by transforming the right-hand-side using relators. So the right-hand-side will never be a_i, a contradiction. Thus by Δ^0_1 comprehension the image of α exists. This completes the proof of $2 \to 1$.

$(3 \to 1)$. Let A be the smallest abelianizer of G. We show that $a_i \in A \leftrightarrow i \in \mathrm{Im}\alpha$. If $i \in \mathrm{Im}\alpha$ we have $a_i = b_j c_j b_j^{-1} c_j^{-1} \in A$ for some $j \in \mathbb{N}$. Suppose that $i \notin \mathrm{Im}\alpha$. It follows that

$$A' = \{g \in G : \text{the sum of the exponent of } a_i\text{'s occurring in } g \text{ equals } 0\}$$

is a normal subgroup of G and G/A' is abelian. It follows that $A \subset A'$ by the minimality of A. Since obviously $a_i \notin A'$ it follows that $a_i \notin A$. Thus by Δ^0_1 comprehension the image of α exists. This completes the proof of $3 \to 1$. □

Now we consider the Σ^0_1-characterization of the abelianizer. The following equivalences hold within RCA_0.

> ‡: Let G be a countable group and A be a normal subgroup of G. A is the smallest abelianizer if and only if A is the Σ^0_1-definable abelianizer.

$$\begin{aligned}
‡ &\Longleftrightarrow (\forall G)(\forall A)[A = \bigcap_{A' \propto G} A' \leftrightarrow A = \langle g_0 g_1 g_0^{-1} g_1^{-1} : g_0, g_1 \in G \rangle] \\
&\Longleftrightarrow (\forall G)(\forall A)[A = \bigcap_{A' \propto G} A' \to A \subset \langle g_0 g_1 g_0^{-1} g_1^{-1} : g_0, g_1 \in G \rangle] \\
&\Longleftrightarrow (\forall G)(\forall A)[A = \bigcap_{A' \propto G} A' \to \bigcap_{A' \propto G} A' \subset \langle g_0 g_1 g_0^{-1} g_1^{-1} : g_0, g_1 \in G \rangle] \\
&\Longleftrightarrow (\forall G)[\neg(\exists A)(A = \bigcap_{A' \propto G} A') \vee (\forall g \in G)(g \in \bigcap_{A' \propto G} A' \to g \in \langle g_0 g_1 g_0^{-1} g_1^{-1} : g_0, g_1 \in G \rangle)]
\end{aligned}$$

where G and A ranges over countable groups and normal subgroups of G respectively. The left-hand-side of the disjunction says that there does not exists the smallest abelianizer. We show that the right-hand-side of the disjunction—the Σ^0_1 characterization of the smallest abelianizer—is equivalent to WKL_0 over RCA_0.

Theorem 5.17. The following are equivalent over RCA_0.

1. WKL_0.
2. $(\forall g \in G)(g \in \bigcap_{A' \propto G} A' \leftrightarrow g \in \langle g_0 g_1 g_0^{-1} g_1^{-1} : g_0, g_1 \in G\rangle)$ for any countable abelian group G.

Proof. $(1 \to 2)$. We have already seen that the implication from right to left is provable in RCA_0. Reasoning in WKL_0, we show the converse direction. Let $\langle g_i : i \in \mathbb{N}\rangle$ be an enumeration of G such that $g_0 \notin \langle ghg^{-1}h^{-1} : g, h \in G\rangle$. We shall construct an abelianizer A' of G such that $g_0 \notin A'$ via weak König's lemma. Let T be the set of all $t \in 2^{<\mathbb{N}}$ such that

1. $0 < \mathrm{lh}(t) \to t(0) = 0$,
2. $\forall i, j, k < \mathrm{lh}(t)(t(i) = t(j) = 1 \wedge g_i g_j^{-1} = g_k \to t(k) = 1)$,
3. $\forall i, j, k < \mathrm{lh}(t)(t(i) = 1 \wedge g_k = g_j g_i g_j^{-1} \to t(k) = 1)$,
4. $\forall i, j, k < \mathrm{lh}(t)(g_k = g_i g_j g_i^{-1} g_j^{-1}) \to t(k) = 1$.

Clearly T is a tree. To see that T is infinite, let $m \in \mathbb{N}$ be given. By bounded Σ^0_1 comprehension (Theorem 1.5), letting $Y = \{i : i < m \wedge g_i \in \langle ghg^{-1}h^{-1} : g, h \in G\rangle\}$, define $t \in 2^{<\mathbb{N}}$ by $t = \begin{cases} 1 & (i \in Y) \\ 0 & (i \notin Y). \end{cases}$ We see $t \in T$ and hence T is infinite. By weak König's lemma there exists a path f through T. $A' = \{g_i : f(i) = 1\}$ is an abelianizer with desired properties. This completes the proof of $1 \to 2$.

$(2 \to 1)$. Instead of WKL_0 we show the equivalent statement Lemma 1.13.3. Let $\alpha, \beta : \mathbb{N} \to \mathbb{N}$ be one-to-one functions such that $\mathrm{Im}\alpha \cap \mathrm{Im}\beta = \emptyset$. Reasoning in RCA_0, $G = \langle \{a_i, b_i, c_i, d : i \in \mathbb{N}\} \mid \{a_{\alpha(j)} c_j b_j c_j^{-1} b_j^{-1}, a_{\beta(j)}^{j+1} d^{-1} : j \in \mathbb{N}\}\rangle$ exists. To see this, we give a recursive procedure to determine whether or not a word from alphabets $\{a_i, b_i, c_i, d : i \in \mathbb{N}\}$ is an element of the normal subgroup N generated by $\{a_{\alpha(j)} c_j b_j c_j^{-1} b_j^{-1}, a_{\beta(j)}^{j+1} d^{-1} : j \in \mathbb{N}\}$. Let G_0 be the free group generated by the alphabets $\{a_i, b_i, c_i, d : i \in \mathbb{N}\}$. For a given word $w \in G_0$, let m_a be the maximum index of a's occurring in w and $m_{b,c}$ be the maximum index of b's and c's occurring in w. With the plan of reducing w to the empty sequence, we try the following procedure. First find every pair of $i \leq m_a$ and $j \leq m_{b,c}$ such that $\alpha(j) = i$ and replace every occurrence of a_i with $b_j c_j b_j^{-1} c_j^{-1}$. Second for each occurrence of d find a pair of $i \leq m_a$ and $j \leq \mathrm{lh}(w)$ such that $\beta(j) = i$ and replace d with a_i^{j+1}. The possible choice of first step is at most one and that of second step is at most finite. If we succeed then $w \in N$ and vice versa.

From now on, we identify an alphabet of G_0 and its corresponding element in G. Since $d \notin \langle ghg^{-1}h^{-1} : g, h \in G\rangle$, by our assumption 2, there exists an abelianizer A' of G such that $d \notin A'$. It follows that $S = \{n : a_n \in A'\}$ is a separator of Imα and Imβ. This completes the proof of $2 \to 1$. $\square$

By the previous theorem, it follows that the statement $\ddagger$ is provable in WKL_0. To show the reversal it is enough to show the conjecture below. The exploration for a proof seems to be harder than in the case of normalizers since RCA_0 does not prove that $g \in \langle\langle Z\rangle\rangle$ is Δ^0_1 for an element $g \in G$ and a finite subset $Z \subset G$ where $\langle\langle Z\rangle\rangle$ denotes the normal subgroup generated by Z. This negative result is followed by the undecidability of the *decision problem* for groups.

Conjecture 5.18. The following is provable in RCA_0. Let $\alpha, \beta : \mathbb{N} \to \mathbb{N}$ be one-to-one functions such that Im$\alpha \cap$ Im$\beta = \emptyset$. Let G be the free group generated by countably infinitely many indeterminates $\{x_i : i \in \mathbb{N}\}$. Fix a one-to-one enumeration $\langle g_i : i \in \mathbb{N}\rangle$ of G and a one-to-one function $h : \mathbb{N}^3 \to \mathbb{N}$ such that $h(i, j, k) >$ maximum of the index numbers of the basis occurring in g_i and g_j for any $i, j, k \in \mathbb{N}$. Then there exists a nontrivial proper subgroup H of G such that

- if $n \in$ Imα then there exists $k \in \mathbb{Z}$ such that $x_{h(i,j,n)}g_i^{-k} \in H$,
- if $n \in$ Imβ then there exists $k \in \mathbb{Z}$ such that $x^{-k}_{h(i,j,n)}g_j \in H$,

for all $i, j, n \in \mathbb{N}$ with $g_i, g_j \notin H$,

- H is a normal subgroup of G,
- Not all elements of G/H are the product of commutators, and
- G/H is not abelian.

In this chapter we study the existence of three notions—essential closures (or neat hulls), normalizers and abelianizers. The logical strength of the existence is equivalent to ACA_0 in each case. We also study characterizations of normalizers and abelianizers. The logical strength of them is equivalent to WKL_0 in each case. (Any characterization of essential closures is not expressive in such way since an essential closure does not always exist uniquely.) 2 of Theorem 5.13 and 2 of Theorem 5.17 are considered to be almost trivial in ordinary group theory. It is interesting to note that WKL_0 is actually equivalent to them despite the appearance.

6 Countable Commutative Rings

In this chapter we do Reverse Mathematics of countable commutative ring theory or ideal theory. Section 6.2 shows that arithmetical comprehension is the appropriate axiom to develop countable ideal theory. Section 6.3 is a survey with somewhat new results on Reverse Mathematics of polynomial rings based on Friedman, Simpson, and Smith [16]. Section 6.4 and 6.5 develop theories of certain classes of commutative rings in weak second order arithmetic. Section 6.5 is a survey on other topics.

6.1 Basic Notions

The following definitions are made in RCA_0. A *countable commutative ring* R consists of a nonempty set $R \subset \mathbb{N}$ together with binary operations $+_R, \cdot_R : |R|^2 \to |R|$, a unary operation $-_R : |R| \to |R|$, and distinguished elements $0_R, 1_R \in |R|$ such that the system $(|R|, +_R, \cdot_R, -_R, 0_R, 1_R)$ obeys the usual commutative ring axioms. For notational convenience we write $|R|$ as R, $a +_R (-_R b)$ as $a -_R b$, and $a \cdot_R b$ as ab for $a, b \in R$. Various notions such as *subrings, ideals, quotient rings, homomorphisms*, or *isomorphisms* are made in a straightforward way. The notion of *countable R-modules* can be made in a similar way as countable vector spaces in Definition III.4.1 of Simpson [61]. The notion of a *ring of polynomials over R* for given countable commutative ring R is also can be made via a coding method. For more information for commutative ring theory see any textbooks, for example, Nagao [49], Hotta [35], Morita [48], and Reid [52].

Definition 6.1. The following definitions are made in RCA_0. Let R be a countable commutative ring and $a \in R$ be an elements of R.

1. a is said to be a *unit* or *invertible* if $(\exists b \in R)(ab = 1_R)$.
2. a is said to be a *zero divisor* if $(\exists b \in R)(b \neq 0_R \wedge ab = 0_R)$.
3. a is said to be *irreducible* if $a \neq 0_R$, a is not a unit, and
$$(\forall b, c \in R)(a = bc \to b \text{ is a unit} \vee c \text{ is a unit}).$$
4. a is said to be *prime* if $a \neq 0_R$, a is not a unit, and
$$(\forall b, c \in R)(a|bc \to a|b \vee a|c)$$
where $u|v$ denotes $(\exists w \in R)(uw = v)$ for $u, v \in R$.

The following additional notions are also developable within RCA_0. A countable commutative ring is said to be a *field* if every element other than 0_R is a unit, and a *domain* if 0_R is the only zero divisor. Clearly every field is a domain. It is easily verified that every prime element of a countable domain is irreducible.

We summarize the fact that the existence of the set of all elements of various notions is equivalent to arithmetical comprehension.

Theorem 6.2. The following are equivalent over RCA_0.

1. ACA_0.
2. The set of all units exists for each countable commutative ring.
3. The set of all zero divisors exists for each countable commutative ring.
4. The set of all irreducible elements exists for each countable commutative ring.
5. The set of all prime elements exists for each countable commutative ring.

Proof. Clearly 1 implies the other items since each notion of units, zero divisors, irreducible elements, and prime elements is defined by respectively Σ^0_1, Σ^0_1, Π^0_2, and Π^0_2 formula. Reasoning within RCA_0, we show arithmetical comprehension from each item via Lemma 1.9. Let $\alpha : \mathbb{N} \to \mathbb{N}$ be a one-to-one function.

$(2 \to 1)$. Let R_0, K_0, R, h be the same as in the proof of Theorem III.5.5 of Simpson [61]. By our assumption, let U the set of all units of R. It follows that $i \in \mathrm{Im}\alpha$ if and only if $h^{-1}(x_i) \in U$ for each $i \in \mathbb{N}$. Thus the image of α exists by Δ^0_1 comprehension. This completes the proof.

$(3 \to 1)$. Let $R = \mathbb{Q}[\langle x_i : i \in \mathbb{N} \rangle]$ and I be the ideal of R generated by the polynomials $x^{j+1}_{\alpha(j)}, j \in \mathbb{N}$. By our assumption, let Z be the set of all zero divisors of R/I. It follows that $i \in \mathrm{Im}\alpha$ if and only if $x_i \in Z$. Thus the image of α exists by Δ^0_1 comprehension. This completes the proof.

$(4 \to 1)$ is shown in the proof of Theorem 4.1 of Friedman, Simpson, and Smith [16].

$(5 \to 1)$. The proof in [16], the commutative ring is taken as the polynomial ring over a countable field. It will be shown within RCA_0 that the notions of irreducible element and the prime element are the same in polynomial rings over countable fields (Theorem 6.38). Thus 5 implies 1. □

A countable commutative ring is said to be *local* if the ring has at most one maximal ideal. 2 of the theorem above implies arithmetical comprehension even if we restrict R to be a local ring. In fact, R in the proof of $(2 \to 1)$ is a local ring since it is provable within RCA_0 that all elements of units have the property of ideals, cf. Proposition 6.20. As it is mentioned, 4 and 5 of the theorem above implies arithmetical comprehension even if we restrict R to be the polynomial ring over a countable field.

The rest of this section is devoted to study construction of rings of fractions in weak second order arithmetic. Firstly we show that such constructions for countable commutative domains can be carried out within RCA_0.

Definition 6.3. The following definitions are made in RCA_0. Let R be a countable commutative ring. A subset $S \subset R$ is *multiplicatively closed* if $(\forall a, b \in S)(ab \in S)$. Let S be a multiplicatively closed set including 1_R. A *ring of fractions of R with respect to S* consists of a ring R' with a homomorphism $h : R \to R'$ satisfying following clauses

1. $(\forall a \in R)(h(a) = 0_{R'} \to a$ is a zero divisor),
2. $(\forall s \in S)(h(s)$ is a unit),
3. $(\forall a' \in R')(\exists a \in R)(\exists s \in S)(a' = h(a)h(s)^{-1})$.

Note that if R is a countable domain namely 0_R is an only zero divisor then $\ker h = \{0_R\}$ namely h is an injective homomorphism.

Proposition 6.4. The following is provable in RCA_0. Let R be a commutative ring and $S \subset R$ be a multiplicatively closed set including 1_R. If S does not contain any zero divisor, then a ring of fractions of R with respect to S exists.

Proof. Reasoning within RCA_0, define an equivalence $(r, s) \sim (r', s')$ on $R \times S$ by $rs' -_R r's = 0_R$. Define a countable commutative ring R' by $|R'| = R \times S/\sim$, $(r, s) +_{R'} (r', s') = (rs' +_R r's, ss')$, $(r, s) \cdot_{R'} (r', s') = (rr', ss')$, $0_{R'} = (0_R, 1_R)$, and $1_{R'} = (1_R, 1_R)$. Define a homomorphism $h : R \to R'$ by $h(a) = (a, 1_R)$. It is easily verified that (R', h) forms a ring of fractions of R with respect to S. This completes the proof. □

If R is a countable commutative domain then $S = R \setminus \{0_R\}$ is multiplicatively closed, includes 1_R, and does not contain any zero divisor. A ring of fractions R' of R with respect to S forms a field. R' is called a *field of fractions* of R.

If R is a countable commutative domain and P is a prime ideal of R (the formal definition of prime ideals is given in Definition 6.9) then $R \setminus P$ is multiplicatively closed, includes 1_R, and does not contain any zero divisor. A ring of fractions R' of R with respect to $R \setminus P$ forms a local ring. Moreover, the existence of the unique maximal ideal of R' is provable within RCA_0. R' is called a *localization* of R.

Proposition 6.5. The following is provable within RCA_0. Let R be a countable commutative domain and P be a prime ideal of R. Let R' be a ring of fractions of R with respect to $S = R \setminus P$. Then the unique maximal ideal of R' exists.

Proof. We reason within RCA_0. Let $a' \in R'$ and $a' = h(a)h(s)^{-1}$ $(a \in R, s \in S)$. Clearly if $a \in S$ then a' is a unit. Conversely suppose that a' is a unit. Let $b' = h(b)h(t)^{-1}$ $(b' \in R', b \in R, t \in S)$ be such that $a'b' = 1_{R'}$. We have $1_{R'} = h(a)h(s)^{-1}h(b)h(t)^{-1}$ and $ab = st$ since h is injective. Therefore we have $a \in S$ since $a \notin S$ implies $ab \notin S$. Thus a is not a unit if and only if $a \in P$. Observing that there exists a function which takes an element $a' \in R'$ to a pair of elements $a \in R$ and $s \in S$ such that $a' = h(a)h(s)^{-1}$, let $M = \{a' = h(a)h(s)^{-1} \in R' : a \in P\}$. Let $a' = h(a)h(s)^{-1}, b' = h(b)h^t, a +_{R'} b = h(c)h(u)^{-1}, ab = h(d)h(v)^{-1}$ $(a, b, c, d \in R, s, t, u, v \in S)$. We have $P \ni atu + bsu = cst$, therefore $c \in P$, and $P \ni abv = dst$, therefore $d \in P$ since P is prime. Thus M is an ideal of R'. It is easily verified that M is the unique maximal ideal. This completes the proof. □

Secondly we show that the existence of rings of fractions in general case is equivalent to ACA_0 over RCA_0.

Theorem 6.6. The following are equivalent over RCA_0.

1. ACA_0.
2. For any commutative ring R and multiplicatively closed set $S \subset R$ including 1_R, a ring of fractions of R with respect to S exists.
3. For any commutative R and multiplicatively closed set $S \subset R$ including 1_R, a ring R' with a homomorphism $h : R \to R'$ satisfying clause 1 and 2 of definition 6.3 exists.

Proof. $(1 \to 2)$. The usual construction of a ring of fractions works in ACA_0. Define a binary relation on $R \times S$ as $(r, s) \sim (r', s') \leftrightarrow (\exists s \in S)(s(rs' -_R r's) = 0_R)$ where $(r, s), (r', s') \in R \times S$. Note that this relation is Σ^0_1 definable. We can easily see that this is an equivalence relation.

$(2 \to 3)$ is trivial.

$(3 \to 1)$. Instead of showing ACA_0, we shall show the equivalent assertion 3 of lemma 1.9. Let $\alpha : \mathbb{N} \to \mathbb{N}$ be a one-to-one function. Let $R_0 = \mathbb{Q}[x_i, y_i : i \in \mathbb{N}]$ be the polynomial ring over the rational fields $\mathbb{Q}$ with countably infinitely many indeterminates $x_i, y_i, i \in \mathbb{N}$. Let $I \subset R_0$ be the ideal generated by the polynomials $x_{\alpha(j)} y^{j+1}_{\alpha(j)}, j \in \mathbb{N}$. I exists by Δ^0_1 comprehension (we can show this fact in the same way as Simpson [61, Theorem IV.6.4]). Form a quotient ring $R = R_0/I$. Let S be the set of all monomials of the form $q y^{e_1}_{m_1} y^{e_2}_{m_2} \cdots y^{e_k}_{m_k}$ with $q \in \mathbb{Q}, q \neq 0, 0 \leq k$. Observing that S is multiplicatively closed set including 1_R, let R' and $h : R \to R'$ be a ring and a homomorphism obtained by our assumption 3. It follows that $(\exists j)(\alpha(j) = 0) \leftrightarrow h(x_i) = 0'_R$ for all i. Thus by Δ^0_1 comprehension, the image of α exists. This completes the proof. □

Definition 6.7. The following definition is made in RCA_0. Let R be a commutative ring. A *total ring of fractions* of R consists of a ring R' with a monomorphism $h : R \to R$ satisfying following clauses

1. $(\forall a \in R)(a$ is not a zero divisor $\to h(a)$ is a unit),
2. $(\forall a' \in R')(\exists a \in R)(\exists s \in R)(s$ is not a zero divisor $\wedge\, a'h(s) = h(a))$.

Theorem 6.8. The following are equivalent over RCA_0.

1. ACA_0.
2. For any commutative ring R, a total ring of fractions of R exists.
3. For any commutative ring R, a ring R' with a monomorphism $h : R \to R'$ satisfying clause 1 of definition 6.7 exists.

Proof. $(1 \to 2)$. The set of all zero divisors Z exists by arithmetical comprehension. Observing that $R \setminus Z$ does not have any zero divisor, we can construct R' and h by the same method as we did in proposition 6.4.

$(2 \to 3)$ is trivial.

$(3 \to 1)$. By Proposition 6.2 it is enough to show that for any commutative ring R the set of all divisors exists. Let R be a commutative ring and by our assumption 3 (R', h) be a total ring of fractions of R. It follows that $(\forall a \in R)(a$ is a zero divisor $\leftrightarrow h(a)$ is not a unit). Notice that the righthand side is Π^0_1 while lefthand side is Σ^0_1. Thus by Δ^0_1 comprehension there exists the set of all zero divisors. This completes the proof of 3 to 1. □

6.2 Reverse Ideal Theory

Firstly, we summarize Reverse Mathematics results on the existence of various kinds of ideals.

Definition 6.9. The following definitions are made in RCA_0. Let I be a nontrivial proper ideal of a countable commutative ring R.

1. I is said to be *prime* if $(\forall a, b \in R)(ab \in I \to a \in I \vee b \in I)$.
2. I is said to be *radical* if $(\forall a \in R)(\forall n)(a^n \in I \to a \in I)$.
3. I is said to be *primary* if $(\forall a, b \in R)(ab \in I \wedge a \notin I \to (\exists n)(b^n \in I))$.
4. I is said to be *irreducible* if $(\forall a, b \in R)(I = (I \cup \{a\}) \cap (I \cup \{b\}) \to a \in I \vee b \in I)$.
5. I is said to be *maximal* if $(\forall a \in R \setminus I)((I \cup \{a\}) = R)$.
6. I is said to be *principal* if $(\exists a \in R)(I = (a))$.
7. I is said to be *finitely generated* if $(\exists a_0, \ldots, a_k \in R)(I = (a_0, \ldots, a_k))$.

Here (S) and $(r_0, \ldots, r_k)$ denote the ideal generated by respectively S and $\{r_0, \ldots, r_k\}$ for $S \subset R$ and $r_0, \ldots, r_k \in R$.

Clearly every prime ideal is radical, primary, and irreducible.

Theorem 6.10. The following are equivalent over RCA_0.

1. WKL_0.
2. Every countable commutative ring which is not a field has a prime ideal.
3. Every countable commutative ring which is not a field has a radical ideal.
4. Every countable commutative ring which is not a field has a primary ideal.
5. Every countable commutative ring which is not a field has an irreducible ideal.
6. Every countable commutative ring which is not a field has a nontrivial proper ideal.

Proof. The equivalence between 1, 2 and 3 is Theorem IV.6.4 of Simpson [61]. (See also Theorem 3.1 of Freedman, Simpson, and Smith [16].) The implications $2 \to 4$, $2 \to 5$, $4 \to 6$, and $5 \to 6$ are trivial. The equivalence between 1 and 6 is shown in Downey, Lempp, and Militei [14]. □

Theorem 6.11. The following are equivalent over RCA_0.

1. ACA_0.
2. Every countable commutative ring which is not a field has a maximal ideal.
3. Every countable commutative ring which is not a field has a principal nontrivial proper ideal.
4. Every countable commutative ring which is not a field has a finitely generated nontrivial proper ideal.

Proof. The equivalence between 1 and 2 is Theorem III.5.5 of Simpson [61]. (See also Theorem 4.2 of Freedman, Simpson, and Smith [16].) The implications $1 \to 3$ and $3 \to 4$ are trivial. The equivalence between 1 and 4 is shown in Downey, Lempp, and Mileti [14]. □

Secondly, we discuss the basic theory of nilradicals, Jacobson radicals, annihilators, and local rings from the standpoint of Reverse Mathematics.

Theorem 6.12. The following are equivalent over RCA_0.

1. ACA_0.
2. $\mathrm{Nil}(R) = \{r \in R : (\exists n > 0)(r^n = 0_R)\}$, the *nilradical* of R exists for any countable commutative ring R.
3. $\mathrm{Jac}(R) = \{r \in R : (\forall a \in R)(\exists b \in R)(ra - 1_R)b = 1_R\}$, the *Jacobson radical* of R exists for any countable commutative ring R.
4. Let R be a countable commutative ring and S be a subset of an R-module. Then
$$\mathrm{Ann}_R(S) = \{r \in R : (\forall s \in S)(rs = 0_R)\},$$
the *annihilator* of S exists.

Proof. The implications $1 \to 2$, $1 \to 3$, and $1 \to 4$ are trivial. The implication $2 \to 1$ is shown by a similar method as in the proof of Theorem 4.2 of Downey et al. [14]. It remains to show the implication $3 \to 1$ and $4 \to 1$.

(3→1). Assume 3. Reasoning within RCA_0, we show arithmetical comprehension via Lemma 1.9. Let $\alpha : \mathbb{N} \to \mathbb{N}$ be a one-to-one function. Let R_0, K_0, R, h be the same as in the proof of Theorem III.5.5 of Simpson [61]. By 3 the Jacobson radical $\mathrm{Jac}(R)$ of R exists. We show that $i \in \mathrm{Im}\alpha$ if and only if $h^{-1}(x_i) \notin \mathrm{Jac}(R)$. If $i \in \mathrm{Im}\alpha$ then $h^{-1}(x_i)$ is invertible in R, hence $h^{-1}(x_i) \notin \mathrm{Jac}(R)$. Conversely, if $h^{-1}(x_i) \in \mathrm{Jac}(R)$, let $a \in R$ be such that $a \cdot h^{-1}(x_i) - 1_R$ is not invertible in R. Put $h(a) \cdot x_i - 1_R = r/s$ where

$r, s \in R_0, s \neq 0_R$. It follows that r does not contain any monomial of the form $qx_{\alpha(m_1)}^{e_1} x_{\alpha(m_2)}^{e_2} \dots x_{\alpha(m_k)}^{e_k}$ $(q \in \mathbb{Q}, q \neq 0, k \geq 0)$. Put $h(a) = t/u$ where $t, u \in R_0, u \neq 0_R$ and have $stx_i = ru + su$. The right-hand-side contains at least one monomial of the form $qx_{\alpha(m_1)}^{e_1} x_{\alpha(m_2)}^{e_2} \dots x_{\alpha(m_k)}^{e_k}$ $(q \in \mathbb{Q}, q \neq 0, k \geq 0)$. Thus we conclude that $i \in \mathrm{Im}\alpha$. By Δ_1^0 comprehension $\mathrm{Im}\alpha$ exists. This completes the proof of 3→1.

(4→1). Assume 4. Reasoning within RCA_0, we show arithmetical comprehension via Lemma 1.9. Let $\alpha : \mathbb{N} \to \mathbb{N}$ be a one-to-one function. Let $R = \mathbb{Z}[x_i : i \in \mathbb{N}]/(\{x_i x_j : i, j \in \mathbb{N}, i \neq j\})$ and $J = \{(j+1)x_{\alpha(j)} : j \in \mathbb{N}\}$. By 4, $\mathrm{Ann}_R(J)$ exists. It follows that $i \in \mathrm{Im}\alpha$ if and only if $x_i \notin \mathrm{Ann}_R(J)$. Thus $\mathrm{Im}\alpha$ exists by Δ_1^0 comprehension. This completes the proof of 4→1. □

Recall that R in the proof of 3→1 is a local ring, hence the Jacobson radical of R equals the unique maximal ideal of R.

In ordinary mathematics, the nilradical can also be characterized as the intersection of all prime ideals of the ring. Note that this statement is of the form $(\forall R)(\forall a \in R)(\varphi(R, a) \leftrightarrow \psi(R, a))$ where R ranges countable commutative rings, φ is Σ_1^0, and ψ is Π_1^1. We show that WKL_0 is needed to develop such an argument.

Proposition 6.13. RCA_0 proves the following. If R is a countable commutative ring and $r \in R$ is nilpotent, then r belongs to every prime ideal of R.

Proof. We reason within RCA_0. Let $r \in R$ be nilpotent and $P \subset R$ be a prime ideal. From $r^n = 0_R \in P$ we have $r \in P$ by Σ_0^0 induction. This completes the proof. □

Proposition 6.14. WKL_0 proves the following. If R is a countable commutative ring and $r \in R$ belongs to every prime ideal of R, then r is nilpotent.

Proof. We reason within WKL_0. We use Exercise 4.6.6 of Simpson [61] to show the contraposition of the statement. Let $r \in R$ be not nilpotent. Letting $\varphi(x) \equiv (x = 0_R)$ and $\psi(x) \equiv (\exists n)(r^n = x)$, we have a prime ideal $P \subset R$ such that $r \notin P$. This completes the proof. □

Theorem 6.15. The following are equivalent over RCA_0.

1. WKL_0.
2. If R is a countable commutative ring and $r \in R$ belongs to every prime ideal of R, then r is nilpotent.

Proof. The implication 1 → 2 is the previous proposition. It remains to show that 2 implies 1. By Theorem 4.6.4 of Simpson [61], it is enough to show that for any commutative ring R which is not a field there exists a prime ideal of R. Since 1_R is not nilpotent, using our assumption 2, there exists a prime ideal $P \subset R$ such that $1_R \notin P$. This completes the proof. □

Remark 6.16. We have presented several mathematical statements which are equivalent to WKL_0: Isbell's zig-zag theorem (Theorem 4.4), a characterization of normalizers (Theorem 5.13), a characterization of abelianizer (Theorem 5.17), and a characterization of nilradicals (Theorem 6.15). Each of statements plus weak König's lemma itself asserts the equivalence between a Σ^1_1 sentence and a Π^0_1 sentence. More precisely, it is of the form

$$(\forall x \in |M|)(\exists X \varphi(x, X) \leftrightarrow \psi(x))$$

where M is an algebraic (or more generally a mathematical) system, and φ and ψ is Π^0_1. Theorems or claims with such logical structure are seen here and there in ordinary mathematics. It is expected that a general relationship between such characterizations and WKL_0 lurks. One possible future work is to investigate a relationship between characterizations and set existence axioms more extensively and find meta-theorems about this phenomenon. See also Lemma VIII.2.4.2 of [61].

The argument on Jacobson radicals works parallel as we did in the case of nilradicals. In this case, instead of WKL_0, we need ACA_0. In ordinary mathematics, the Jacobson radical can also be characterized as the intersection of all maximal ideals of the ring. Note that this statement is of the form $(\forall R)(\forall a \in R)(\varphi(R, a) \leftrightarrow \psi(R, a))$ where R rages countable commutative rings, φ is Π^0_2, and ψ is Π^1_1. We show that ACA_0 is needed to develop such argument.

Proposition 6.17. RCA_0 proves the following. If R is a countable commutative ring and $r \in R$ satisfies the condition $(\forall a \in R)(\exists b \in R)((ra - 1_R)b = 1_R)$, then r belongs to every maximal ideal of R.

Proof. We reason within RCA_0. Let $r \in R$ satisfy the condition $(\forall a \in R)(\exists b \in R)((ra - 1_R)b = 1_R)$ and $M \subset R$ be a maximal ideal of R. Suppose for a contradiction that $r \notin M$. Since M is maximal, there exists $m \in M$ and $a \in R$ such that $m + ra = 1_R$. It follows that $ra - 1_R \in M$, a contradiction for M can not contain a unit. So we have $r \in M$ and this completes the proof. □

Proposition 6.18. ACA_0 proves the following. If R is a countable commutative ring and $r \in R$ belongs to every maximal ideal of R, then r satisfies the condition $(\forall a \in R)(\exists b \in R)((ra - 1_R)b = 1_R)$.

Proof. Reasoning within ACA_0, we show the contraposition of the statement. Letting $r \in R$ not satisfy the condition $(\forall a \in R)(\exists b \in R)((ra - 1_R)b = 1_R)$, we have $a \in R$ such that $ra - 1_R$ is not a unit of R. By ACA_0, there exists a maximal ideal $M \subset R$ such that $ra - 1_R \in M$. If $r \in M$ then $1_R = ra - (ra - 1_R) \in M$, a contradiction. It follows that $r \notin M$. This completes the proof. □

Theorem 6.19. The following are equivalent over RCA_0.

1. ACA_0.

2. If R is a countable commutative ring and $r \in R$ belongs to every maximal ideal of R, then r satisfies the condition $(\forall a \in R)(\exists b \in R)((ra - 1_R)b = 1_R)$.

Proof. The implication $1 \to 2$ is the previous proposition. It remains to show that 2 implies 1. By Theorem 3.5.5 of Simpson [61], it is enough to show that for any commutative ring R which is not a field there exists a maximal ideal of R. Since $1_R \cdot 1_R - 1_R = 0_R$ and 0_R is not a unit, 1_R does not satisfy the condition $(\forall a \in R)(\exists b \in R)((ra - 1_R)b = 1_R)$. Using our assumption 2, there exists a maximal ideal $M \subset R$ such that $1_R \notin M$. This completes the proof. □

Recall that a countable commutative ring is said to be local if the ring has at most one maximal ideal. The locality of a commutative ring is characterized as the property that all elements of units have the property of ideals. Note that this statement is of the form $(\forall R)(\varphi(R) \leftrightarrow \psi(R))$ where R ranges countable commutative rings, φ is Π^0_2, and ψ is Π^1_1. Such argument can be developed within ACA_0. The reversal is not known.

Proposition 6.20. RCA_0 proves the following. Let R be a countable commutative ring. If

$(\forall a, b, r \in R)(a \text{ is not a unit} \wedge b \text{ is not a unit} \to a +_R b \text{ is not a unit} \wedge ra \text{ is not a unit})$

holds then R is local.

Proof. We reason within RCA_0. Let M be any maximal ideal of R. It follows that $a \in M$ if and only if a is not a unit for any $a \in R$. Thus any two maximal ideal of R are equal to each other. This completes the proof. □

Proposition 6.21. ACA_0 proves the following. Let R be a countable commutative ring. If R is local then

$(\forall a, b, r \in R)(a \text{ is not a unit} \wedge b \text{ is not a unit} \to a +_R b \text{ is not a unit} \wedge ra \text{ is not a unit})$

holds.

Proof. We reason within ACA_0. We may assume that R is not a field. Take a maximal ideal M of R. It is enough to show that $a \in M$ if and only if a is not a unit for any $a \in R$. If $a \in M$ then clearly a is not a unit. Suppose that a is not a unit. Take a maximal ideal M' such that $a \in M'$. By our assumption we have $M = M'$. Therefore it follows that $a \in M$. This completes the proof. □

Question 6.22. Does the statement of the previous proposition imply ACA_0 over RCA_0?

Thirdly, we end this section by showing that arithmetical comprehension is just strong enough to guarantee various ideal operations.

Theorem 6.23. The following are equivalent over RCA_0.

1. ACA_0.
2. $I + J = \{a +_R b : a \in I, b \in J\}$, the *sum* of I and J exists for any ideals I, J of any countable commutative ring.
3. $I \cdot J = \{\sum_i a_i b_i : a_i \in I, b_i \in J\}$, the *product* of I and J exists for any ideals I, J of any countable commutative ring.
4. $I^k = \{\sum_i a_{i_1} a_{i_2} \dots a_{i_k} : a_{i_0}, \dots, a_{i_k} \in I\}$, the *power* of I exists for any ideal I of any countable commutative ring, $2 \leq k \in \omega$.
5. $\bigcap_{k=0}^{\infty} I^k$ exists for any ideal I of any countable commutative ring.
6. $I : J = \{r \in R : (\forall a \in J)(ra \in I)\}$, the *ideal quotient* of I by J exists for any ideal I of any countable commutative ring.
7. $\sqrt{I} = \{r \in R : (\exists n > 0)(r^n \in I)\}$, the *radical* of I exists for any ideal I of any countable commutative ring.

Proof. The implications from 1 to the other items are trivial. We show reversals via Lemma 1.9.

(2→1). We reason within RCA_0. Let $\alpha : \mathbb{N} \to \mathbb{N}$ be a one-to-one function. Let

$$R = \mathbb{Z}[x_i : i \in \mathbb{N}]/(\{x_i x_j : i, j \in \mathbb{N}\}),$$

$I = (\{(j+1)x_{\alpha(j)} : j \in \mathbb{N}\})$, and $J = (\{(j+2)x_{\alpha(j)} : j \in \mathbb{N}\})$. By 2, $I + J$ exists. It follows that $i \in \mathrm{Im}\alpha$ if and only if $x_i \in I + J$. Thus $\mathrm{Im}\alpha$ exists by Δ^0_1 comprehension. This completes the proof of $2 \to 1$.

(3→1). We reason within RCA_0. Let $\alpha : \mathbb{N} \to \mathbb{N}$ be a one-to-one function. Let $R = \mathbb{Z}[x_i, y : i \in \mathbb{N}]$. Let

$$I = (\{\prod_{k=0}^{j} p_{2k} x_{\alpha(j)}, y : j \in \mathbb{N}\}) \text{ and } J = (\{\prod_{k=0}^{j} p_{2k+1} x_{\alpha(j)}, y : j \in \mathbb{N}\})$$

where p_k is the k th prime. By 3, $I \cdot J$ exists. If $i \notin \mathrm{Im}\alpha$ then $x_i y \notin I \cdot J$. Suppose that $\alpha(j) = i$. Since $\prod_{k=0}^{j} p_{2k}$ and $\prod_{k=0}^{j} p_{2k+1}$ are relatively prime, there exists two integers l and m such that $l \prod_{k=0}^{j} p_{2k} + m \prod_{k=0}^{j} p_{2k+1} = 1$ by Bézout's lemma. Therefore $x_i y = l \prod_{k=0}^{j} p_{2k} x_i y + m \prod_{k=0}^{j} p_{2k+1} x_i y \in I \cdot J$. Thus $i \in \mathrm{Im}\alpha \leftrightarrow x_i y \in I \cdot J$ holds and hence by Δ^0_1 comprehension the image of α exists. This completes the proof of $3 \to 1$.

(4→1). Let $k \in \omega$. We reason within RCA_0. Let $\alpha : \mathbb{N} \to \mathbb{N}$ be a one-to-one function. Let

$$R = \mathbb{Z}[x_i, y_i : i \in \mathbb{N}]/(\{x_{\alpha(j)}^{k(j+1)} - y_{\alpha(j)} : j \in \mathbb{N}\})$$

and $I = (\{x_i, y_i : i \in \mathbb{N}\})$. By 4, I^k exists. It follows that $i \in \mathrm{Im}\alpha$ if and only if $y_i \in I^k$. Thus $\mathrm{Im}\alpha$ exists by Δ^0_1 comprehension. This completes the proof of $4 \to 1$.

(5→1). We reason within RCA_0. Let $\alpha : \mathbb{N} \to \mathbb{N}$ be a one-to-one function. Let

$$R = \mathbb{Z}[x_{i,k}, y_i : i \in \mathbb{N}, 2 \leq k \in \mathbb{N}]/(\{x_{\alpha(j),k}^{k(j+1)} - y_{\alpha(j)} : j \in \mathbb{N}\})$$

and $I = (\{x_{i,k}, y_i : i \in \mathbb{N}, 2 \leq k \in \mathbb{N}\})$. By 5, $\bigcap_{k=0}^{\infty} I^k$ exists. If $i \notin \mathrm{Im}\alpha$ then $y_i \notin I^2$ and hence $y_i \notin \bigcap_{k=0}^{\infty} I^k$. Suppose that $\alpha(j) = i$ and we have

$$y_i = x_{i,2}^{2(j+1)} = x_{i,3}^{3(j+1)} = \cdots \in \bigcap_{k=0}^{\infty} I^k.$$

Thus $i \in \mathrm{Im}\alpha \leftrightarrow y_i \in \bigcap_{k=0}^{\infty} I^k$ holds and hence by Δ_1^0 comprehension the image of α exists. This completes the proof of $5 \to 1$.

(6→1). Note that in the proof of 4→1 of Theorem 6.12, J is an ideal of R and $\mathrm{Ann}_R(J) = \{0_R\} : J$. Thus 6 implies 1.

(7→1). Note that $\mathrm{Nil}(R) = \sqrt{\{0_R\}}$. Thus by 2→1 of Theorem 6.12 7 implies 1. □

The proof that 3 implies 1 is redundant for 3 implies 4 with $k = 2$. Moreover, the same countable commutative ring as in the proof of $5 \to 1$ serves to prove $4 \to 1$. However the author leaves these proofs to express the idea.

6.3 Polynomial Rings

In this section we study the property of polynomial rings over countable fields. A part of the content is based on Friedman, Simpson and Smith [16]. Here we give detailed proofs. The following division algorithm is suggested in the proof of Lemma 2.3 of [16].

Proposition 6.24. RCA_0 proves the following. Let R be a countable commutative ring, $f \in R[x]$ be a nonzero polynomial, and $g \in R[x]$ be a monic polynomial. Then $(\exists q, r \in R[x])(f = qg + r \wedge \deg r < \deg g)$.

Proof. If $\deg f < \deg g$ then the desired statement holds trivially. Sot let $\deg f = n + i, \deg g = n$ $(n, i \in \mathbb{N})$. We show

$$(\forall l)(l \leq i + 1 \to (\exists q, r \in R[x])(f = qg + r \wedge \deg r \leq n + i - l))$$

via Σ_1^0 induction on l. If $l = 0$ then we have $f = 0_{R[x]} \cdot g + f \wedge \deg f = n + i - 0$, hence the statement holds. Assume that the statement holds for $l = k$ and let $k + 1 \leq i + 1$. By the induction hypothesis we have $q, r \in R[x]$ such that $f = qg + r \wedge \deg r \leq n + i - k$. If $\deg r < n + i - k$ then the statement holds for $l = k + 1$. So let $\deg r = n + i - k$. Let a $(0_R \neq a \in R)$ be the leading coefficient of r. We have $\deg(r - ax^{i-k} \cdot g) \leq n + i - (k + 1)$ and $f = qg + r = (q + ax^{i-k})g + (r - ax^{i-k} \cdot g)$. Thus the statement holds for $l = k + 1$. Finally let $l = i + 1$ and we have the desired statement. This completes the proof. □

A proof in some literature shows $(\forall m)(\forall f \in R[x])(\deg f = m \to (\exists q, r \in R[x])(f = qg + r \wedge \deg r < \deg g))$ by the induction on m. We can not take this way because we lack Π^0_2 induction.

Next proposition is on factorization of polynomials.

Proposition 6.25. RCA_0 proves the following. Let K be a countable field which is algebraic closed.

1. Let $f \in K[x]$ be a polynomial with degree n. Then there exists elements $a_1, \ldots, a_n \in K$ such that $f = \prod_{i=1}^{n}(x - a_i)$. Moreover, the elements are unique up to orders.

2. There exists a function $\alpha : K[x] \to K^{<\mathbb{N}}$ such that $\alpha(f) = \langle a_1, \ldots, a_n \rangle$ satisfies the condition $f = \prod_{i=1}^{n}(x - a_i)$ for all $f \in K[x]$.

Proof. 1. First we prove the existence of $a_1, \ldots a_n$. Define Σ^0_1 formula by $\varphi(j) \equiv (j \leq \deg(f) \to (\exists a_1, \ldots, a_{j+1} \in K)(\exists g \in K[x])(f = g\prod_{i=1}^{j+1}(x - a_i))$. By Σ^0_1 induction we have $(\forall j)\varphi(j)$ in paticular $\varphi(n)$.

Next we show the uniqueness. Suppose that we have two factorization $f = \prod_{i=1}^{n}(x - a_i) = \prod_{i=1}^{n}(x - b_i)$. Let $\psi(j)$ say that if $j \leq n$ then there exists a permutation σ of $\{1, 2, 3, \ldots, j\}$ such that $a_i = b_{\sigma(i)}$ for all $i \leq j$. Observing that $\psi(j)$ is Σ^0_0, we have $(\forall j)\psi(j)$ in particular $\psi(n)$ by Σ^0_0 induction.

2. Notice that we have $(\forall f \in K[x])(\exists \langle a_1, \ldots, a_n \rangle \in K^{<\mathbb{N}})(f = \prod_{i=1}^{n}(x - a_i))$ and $f = \prod_{i=1}^{n}(x - a_i)$ is Σ^0_0.

□

Next we provide the notion of minimal polynomials.

Definition 6.26. Let F be a countable field and K be an algebraic closure of F. For each $a \in K$, a monic polynomial $f \in F[x]$ of the least degree such that $f(a) = 0_K$ is called the *minimal polynomial* of a.

Proposition 6.27. RCA_0 proves the following.

Let F be a countable field with its algebraic closure K. For each $a \in K$,

1. there exists the unique minimal polynomial $f \in F[x]$ of a.

2. the minimal polynomial of a is irreducible.

3. if $g \in F[x]$ satisfies these clauses

   - g is irreducible,
   - g is monic,
   - $g(a) = 0_K$,

   then g is the minimal polynomial of a.

Proof. 1. First we show the existence. Let $\varphi(k) \equiv (\exists f \in F[x])(\deg(f) = k \wedge f(a) = 0)$. By Σ^0_1 least number principle, there exists the least k satisfying $\varphi(k)$. If $\deg f = k$ and $f(a) = 0$, then, dividing by the first coefficient if necessary, f is a minimal polynomial of a.

Next we show the uniqueness. If a has two distinct minimal polynomials f and f', then we have $(f-f')(a) = f(a)-f'(a) = 0_K$ and $0 < \deg(f-f') < \deg f$, a contradiction.

2. $f = gh$ and $f(a) = 0_K$ implies $g(a) = 0_K$ or $h(a) = 0_K$. If f is the minimal polynomial of a, either g or h is constant by the minimality. This concludes that f is irreducible.

3. Let f be a minimal polynomial of a and g satisfy the condition above. Dividing f by g, we have $g = qf + r$ $(q, r \in F[x], \deg r < \deg f)$. $f(a) = g(a) = 0_K$ implies $r(a) = 0_K$ and we have $r = 0_{F[x]}$ by the minimality. Since g is irreducible and monic, it follows that $q = 1_{F[x]}$. This leads to $g = f$.

□

Note that RCA_0 does not prove the existence of a function which takes $a \in K$ to the minimal polynomial of a in general. The following theorem explains this situation.

Lemma 6.28. RCA_0 proves the following. Let F be a countable field and (K, h) be an algebraic closure of F. The following are equivalent.

1. The set of all irreducible elements $\mathrm{IRR}(F[x])$ of $F[x]$ exists.
2. The function which takes $a \in K$ to the minimal polynomial of a exists.
3. The image $h(F)$ of F under h exists.

Proof. The equivalence between 1 and 3 is Lemma 2.7 of [16]. Here we give a detailed proof for convenience.

$(1 \to 2)$. By the previous proposition we have $(\forall a \in K)(\exists f)(f \in \mathrm{IRR}(F[x]) \wedge f(a) = 0_K)$. By Σ^0_0 axiom choice of numbers we have a desired function.

$(2 \to 3)$. Notice that for given $a \in K$ $a \in h(F)$ if and only if the degree of the minimal polynomial of a is 1.

$(3 \to 1)$. For given $f \in F[x]$, by Proposition 6.25 let $hf = \prod_{i=0}^{n}(x - a_i)$ $(a_i \in K, n = \deg f)$. f is reducible if and only if there exists a proper subset $S \subset \{1, 2, 3, \ldots, n\}$ such that all coefficients of $\prod_{i \in S}(x - a_i)$ are in $h(F)$ (in this case $h^{-1}\prod_{i \in S}(x - a_i)$ is a divisor of f). Since the latter condition is Δ^0_1, $\mathrm{IRR}(F[x])$ exists by Δ^0_1 comprehension. □

Theorem 6.29. The following are equivalent over RCA_0.

1. ACA_0.
2. For any countable field F, there exists $\mathrm{IRR}(F[x])$, a set of all irreducible element of $F[x]$.

3. For any countable field F, a function which takes $f \in F[x]$ to an irreducible divisor of f exists.

4. For any countable field F,

$$(\forall \langle f_i : i \in \mathbb{N} \rangle \subset F[x])(\exists \langle g_i : i \in \mathbb{N} \rangle \subset F[x])(\forall i)(g_i \in \mathrm{IRR}(F[x]) \wedge g_i | f_i).$$

5. For any countable field F with its algebraic closure K, a function which takes $a \in K$ to the minimal polynomial $f \in F[x]$ of a exists.

6. For any field F with its algebraic closure K,

$$(\forall \langle a_i : i \in \mathbb{N} \rangle \subset K)(\exists \langle f_i : i \in \mathbb{N} \rangle \subset F[x])(\forall i)(f_i \text{ is the minimal polynomial of } a).$$

7. For any countable field F with its algebraic closure (K, h), the image $h(F)$ of F exists.

Note that 4 and 7 are the sequential version of Lemma 2.4 of [16] and Proposition 6.27.1 respectively.

Proof. The equivalence between 1 and 2 is Theorem 4.1 of [16]. The equivalences between 2, 3, and 4 is trivial. The equivalence between 5 and 6 is also trivial. The equivalence between 2, 5, and 7 follows from the previous lemma. □

We end this section by giving a detailed proof of Lemma 2.8.(1) of [16].

Definition 6.30. Let R be a countable commutative ring. A polynomial $f = \sum_{i=0}^{n} a_i x^i \in R[x]$ is *primitive* if the greatest common divisor of $\langle a_i : i \leq n \rangle$ equals 1_R.

Proposition 6.31. RCA_0 proves the following.

1. There exists a function α which take a polynomial $f \in \mathbb{Q}[x]$ to a primitive polynomial $f_0 \in \mathbb{Z}[x]$ such that $(\exists c \in \mathbb{Q})(f = cf_0)$.

2. Let α be the function in the clause 1. f is irreducible in $\mathbb{Q}[x]$ if and only if $\alpha(f)$ is irreducible in $\mathbb{Z}[x]$ for all $f \in \mathbb{Q}[x]$.

3. $\mathrm{IRR}(\mathbb{Z}[x])$ exists, so $\mathrm{IRR}(\mathbb{Q}[x])$ does.

Proof. We show the existence of $\mathrm{IRR}(\mathbb{Z}[x])$. It is enough to show that the number of divisors of a given polynomial $f \in \mathbb{Z}[x]$ is finite. If g divides f (in $\mathbb{Z}[x]$) then $g(i)$ divides $f(i)$ (in $\mathbb{Z}$) for all $1 \leq i \leq n$ where n is the degree of f. □

6.4 Euclidean Domains and Principal Ideal Domains (PIDs)

Definition 6.32 (Euclidean domains)**.** The following definition is made in RCA_0. Let R be a countable commutative domain. A function $|*| : R \to \mathbb{N}$ is said to be *norm function* if

1. $(\forall a \in R)(a \neq 0_R \to |a| > |0_R|)$,
2. $(\forall a, b \in R)(b \neq 0_R \to (\exists q, r \in R)(a = qb + r \wedge |r| < |b|)$.

A countable commutative domain together with a norm function is said to be *Euclidean domain*. The range of a norm function can be replaced by any well-ordered set X. However, we require the Σ^0_1 least number principle along the order of X for technical reasons.

$\mathbb{Z}$ with the ordinary absolute value function $|*| : \mathbb{Z} \to \mathbb{N}$ is one of the simplest example of an Euclidean domain. By Proposition 6.24, the ring of polynomials $F[x]$ for any countable field F with the degree function $\deg : F[x] \to \mathbb{N} \cup \{-\infty\}$ forms an Euclidean domain.

Definition 6.33 (relatively prime)**.** The following definitions are made in RCA_0. Let R be a countable commutative ring. Recall that we write $(\exists c \in R)(a = bc)$ as $b|a$ for $a, b \in R$. Elements $a_0, \dots, a_n \in R$ are said to be *relatively prime* if $(\forall b \in R)((\forall i \leq n)(b|a_i \to b \text{ is a unit})$.

Now we prove Bézout's lemma for Euclidean domains within RCA_0.

Theorem 6.34 (Bézout's lemma)**.** RCA_0 proves the following. Let R be an Euclidean domain and $a_1, a_2, \dots, a_n \in R$ be a finite sequence of nonzero elements. Then the following are equivalent.

1. $a_1, a_2, \dots, a_n$ are relatively prime.
2. $(\exists t_1, t_2, \dots, t_n \in R)(\sum_{i=1}^n t_i a_i = 1_R)$.

Proof. The implication $2 \to 1$ is trivial. (This is true for a general countable commutative ring R.) We show the converse. Let

$$\varphi(x) \equiv (\exists s_1, \dots, s_n \in R)(\sum_{i=1}^n s_i a_i \neq 0_R \wedge |\sum_{i=1}^n s_i a_i| = x).$$

By Σ^0_1 least number principle, take the least x and such $s_1, \dots, s_n \in R$. Let $u = \sum_{i=1}^n s_i a_i$ and $a_k = qu + r, |r| < |u|$ for $1 \leq k \leq n$. It follows that $r = \sum_{i=1}^n s'_i a_i$ where $s'_i = -qs_i$ $(i \neq k), 1_R - qs_i$ $(i = k)$ and $\varphi(|r|)$. By the minimality of x, we have $r = 0_R$. Therefore, by our assumption 1, u is a unit. Thus $\sum_{i=1}^n (u^{-1}s_i)a_i = 1_R$. This completes the proof. □

The rest of this section discusses Σ^0_1 PIDs.

Definition 6.35 (Σ^0_1 PIDs)**.** The following definitions are made in RCA_0. Let R be a countable commutative ring. A sequence $\mathcal{I} = \langle r_i : i \in \mathbb{N} \rangle$ of elements of R is said to be a Σ^0_1 ideal if $(\forall i, j)(\exists k)(r_i + r_j = r_k)$ and $(\forall i)(\forall s \in R)(\exists j)(r_i s = r_j)$, cf. Remark 2.2 of Simpson [60]. A sequence of Σ^0_1 ideals is defined similarly. A countable commutative domain R is said to be Σ^0_1 PID if $(\exists i)(\forall j)(\exists s \in R)(r_j = r_i s)$ for any Σ^0_1 ideal $\mathcal{I} = \langle r_i : i \in \mathbb{N} \rangle$ of R. r_i is said to be a *generator* of the Σ^0_1 ideal.

$\mathbb{Z}$ is a Σ^0_1 PID. $\mathbb{Z}[x]$ is not a Σ^0_1 PID for the Σ^0_1 ideal generated by $\{x, 2\}$ does not have a single generator. If F is a countable field then $F[x]$ is a Σ^0_1 PID. This fact follows from the following proposition.

Proposition 6.36. RCA_0 proves that every Euclidean domain is a Σ^0_1 PID.

Proof. We reason within RCA_0. Let R be an Euclidean domain and $\langle r_i : i \in \mathbb{N} \rangle$ be a Σ^0_1 ideal of R. We may assume that $(\exists k)(r_k \neq 0_R)$. Let $\varphi(x) \equiv (\exists k)(r_k \neq 0_R \wedge |r_k| = x)$ and take the least x and k by Σ^0_1 least number principle. For any j we have $r_j = q r_k + r$ $(q, r \in R, |r| < |r_k|)$. If $r \neq 0_R$ then we have $\varphi(|r|)$, a contradiction to the minimality of x. Therefore we have $r = 0_R$ and hence r_k is a generator of $\langle r_i : i \in \mathbb{N} \rangle$. This completes the proof. □

A kind of sequential version of Proposition 6.36 is not provable in RCA_0. In fact, we have

Theorem 6.37. The following are equivalent over RCA_0.

1. ACA_0**.**
2. Let R be an Euclidean domain and $\langle \langle r_{ij} : j \in \mathbb{N} \rangle : i \in \mathbb{N} \rangle$ be a sequence of Σ^0_1 ideals of R. Then there exists a sequence $\langle k_i : i \in \mathbb{N} \rangle$ such that r_{ik_i} is a generator of $\langle r_{ij} : j \in \mathbb{N} \rangle$ for all i.
3. Let R be an Euclidean domain and $\langle I_i : i \in \mathbb{N} \rangle$ be a sequence of ideals of R. Then there exists a sequence $\langle r_i : i \in \mathbb{N} \rangle$ of elements of R such that r_i is a generator of I_i for all i.

Proof. Reasoning in ACA_0, we show the implication $1 \to 2$. By the proof of the previous proposition, we have $(\forall i)(\exists k)(r_k$ generates $\langle r_{ij} : j \in \mathbb{N} \rangle)$. Thus there exists a desired sequence by axiom choice of numbers for arithmetical formulae. The implication $2 \to 3$ is trivial. Reasoning in RCA_0, we show the implication $3 \to 1$ via Lemma 1.9. Let α be a one-to-one function. Define a sequence $\langle I_i : i \in \mathbb{N} \rangle$ of ideals of $\mathbb{Z}$ by letting

$$k \in I_i \leftrightarrow k = 0_{\mathbb{Z}} \vee (\exists j \leq |k|)(\alpha(j) = i \wedge (\exists l \leq |k|)((j+1)l = |k|)).$$

By our assumption 3, let $\langle r_i : i \in \mathbb{N} \rangle$ a sequence of generators of $\langle I_i : i \in \mathbb{N} \rangle$. It follows that $i \in \mathrm{Im}\alpha$ if and only if $r_i \neq 0_{\mathbb{Z}}$. Thus the image of α exists by Δ^0_1 comprehension. This completes the proof. □

Proposition 6.38. RCA_0 proves that every irreducible element of a Σ^0_1 PID is a prime element.

Proof. A standard proof can be carried out in RCA_0. In this proof, $(a_0, a_1, \ldots, a_n)$ denotes the Σ^0_1 ideal generated by $a_0, a_1, \ldots, a_n \in R$. Let R be a Σ^0_1 PID and $a \in R$ be an irreducible element. Let $a|b_0b_1$ $(b_0, b_1 \in R)$. Let c_i be a generator of (a, b_i) and $a = r_ic_i$ $(r_i \in R)$ for $i = 0, 1$. It follows that r_i or c_i is a unit. If both c_0 and c_1 are units, we have $1_R = s_0a +_R t_0b_0 = s_1a +_R t_1b_1$ $(s_0, s_1, t_0, t_1 \in R)$ and $a|(s_0a+_Rt_0b_0)(s_1a+_Rt_1b_1) = 1_R$. It follows that a is a unit, a contradiction. Therefore either r_0 or r_1 is a unit. If r_i is a unit then $b_i = uc_i = ur_i^{-1}a$ $(u \in R)$ and hence $a|b_i$. Thus a is a prime element. This completes the proof. □

Proposition 6.39. RCA_0 proves the following. Let R be a Σ^0_1 PID and $a \in R$ be an irreducible element. Then the ideal generated by a exists. Moreover, the ideal is a maximal ideal.

Proof. Reasoning within RCA_0, we show that $a|b \leftrightarrow \neg(\exists r, s \in R)(ra + sb = 1_R)$ for any $b \in R$. First we show the implication $\rightarrow$. (This is true for a general countable commutative ring R.) Let $a|b$ and $b = ta$ $(t \in R)$. If $ra + sb = 1_R$ then $a(r + st) = 1_R$. Therefore a is a unit, a contradiction to the assumption that a is irreducible. Thus $\neg(\exists r, s \in R)(ra + sb = 1_R)$. Second we show the implication $\leftarrow$. Let c be a generator of the Σ^0_1 ideal generated by a and b. Let $a = rc, b = sc, c = ta + ub$ $(r, s, t, u \in R)$. By our assumption that a is irreducible, either r or c is a unit. If c is a unit then $1_R = c^{-1}ta + c^{-1}ub$, a contradiction. Therefore r is a unit and we have $r^{-1}a = c, b = sr^{-1}a$, and hence $a|b$. Thus we have the desired equivalence. By Δ^0_1 comprehension the ideal generated by a exists. It is easily verified that the ideal is maximal. This completes the proof. □

Corollary 6.40. WKL_0 proves that every Σ^0_1 PID which is not a field have a maximal ideal.

Proof. Reasoning within WKL_0, let P be a prime ideal of a Σ^0_1 PID, cf. Theorem 6.10. A generator of P is prime and hence irreducible. Thus by Proposition 6.39 P is maximal. □

It is not known that whether the previous corollary implies WKL_0 over RCA_0 or not.

6.5 Noetherian Rings

It is a worrisome question to define Noetherian rings within a weak base theory. Letting R be a countable commutative ring, we consider the following conditions.

1. There exists a non finitely generated ideal I of R.
2. There exists an irredundant ascending chain of ideals $I_0 \subsetneq I_1 \subsetneq \cdots$ of R.
3. There exists an ascending chain of ideals $I_0 \subset I_1 \subset \cdots$ of R such that $(\forall i)(\exists j \geq i)(I_j \subsetneq I_{j+1})$.

4. There exists a sequence $\langle a_i : i \in \mathbb{N} \rangle$ of elements of R such that $(\forall i)(a_{i+1} \notin (a_0, \dots a_i))$.

5. There exists a sequence $\langle a_i : i \in \mathbb{N} \rangle$ of elements of R such that $(\forall i)(\exists j \geq i)(a_{j+1} \notin (a_0, \dots, a_j))$.

6. There exists an irredundant ascending chain of Σ^0_1 ideals $\mathcal{I}_0 \subsetneq \mathcal{I}_1 \subsetneq \cdots$ of R.

7. There exists an ascending chain of Σ^0_1 ideals $\mathcal{I}_0 \subset \mathcal{I}_1 \subset \cdots$ of R such that $(\forall i)(\exists j \geq i)(\mathcal{I}_j \subsetneq \mathcal{I}_{j+1})$.

8. There exists a non finitely generated Σ^0_1 ideal $\mathcal{I}$ of R.

9. There exists a sequence $\langle a_i : i \in \mathbb{N} \rangle$ of elements of R such that $(a_0) \subsetneq (a_1) \subsetneq \cdots$.

10. There exists a sequence $\langle a_i : i \in \mathbb{N} \rangle$ of elements of R such that $(a_0) \subset (a_1) \subset \cdots$ and $(\forall i)(\exists j \geq i)((a_j) \subsetneq (a_{j+1}))$.

Clearly ACA_0 proves that all the conditions except 9 and 10 are equivalent, that the conditions 9 and 10 are equivalent, and that one of conditions 9 or 10 implies one of conditions from 1 to 8. More precisely, RCA_0 proves $2 \to 3$, $3 \to 2$, $2 \to 4$, $4 \to 5$, $4 \to 6$, $6 \to 7$, $7 \to 8$, $8 \to 7$, $9 \to 10$, $9 \to 4$, and $10 \to 5$. WKL_0 proves $4 \to 2$ and $5 \to 3$. We give proofs for nontrivial implications.

Proof. $(1 \to 4)$. By arithmetical comprehension, define a sequence $\langle a_i : i \in \mathbb{N} \rangle$ of elements of I by $a_{i+1} = \mu y \{ y \in I : y \notin (a_0, a_1, \dots, a_i) \wedge (a_0, a_1, \dots a_i, y) \neq I \}$.

$(3 \to 1)$. Reasoning within ACA_0, we show the contraposition. Assume $\neg 1$. Let $\langle I_i : i \in \mathbb{N} \rangle$ be an ascending chain of ideals of R such that $I_i \subset I_{i+1}$ for all $i \in \mathbb{N}$. By arithmetical comprehension let $I = \bigcup_{i \in \mathbb{N}} I_i = \{ a \in R : \exists i (a \in I_i) \}$. By our assumption, let $a_0, a_1, \dots, a_n \in I$ be a generators of I. Since $I \subset \bigcup_{i \in \mathbb{N}} I_i$ we have $(\forall i \leq n)(\exists m)(a_i \in I_m)$ and this imply $(\exists m_0)(\forall i \leq n)(a_i \in I_{m_0})$ by Σ^0_0 bounding. Then it follows that $I \subset I_{m_0}$. On the other hand, since $\bigcup_{i \in \mathbb{N}} I_i \subset I$ we have $I_{m_0} \subset I_l \subset I \subset I_{m_0}$ i.e., $I_l = I_{m_0}$ for all $l \geq m_0$. Thus we have $\neg 3$.

$(2 \to 4)$. We reason within RCA_0. Since $(\forall i)(\exists a)(a \in I_{i+1} \setminus I_i)$ holds, so does $(\exists f)(\forall i)(f(i) \in I_{i+1} \setminus I_i)$ by Σ^0_0 axiom choice of numbers. Put $a_i = f(i)$ and we have a desired sequence $\langle a_i : i \in \mathbb{N} \rangle$ of elements of R.

$(4 \to 2)$. Via weak König's lemma, we can construct a sequence $\langle I_i : i \in \mathbb{N} \rangle$ of ideals with following Π^0_1 properties.

- I_i is an ideal of R for all $i \in \mathbb{N}$,
- $a_0, a_1, \dots a_i \in I_i$ for all $i \in \mathbb{N}$,
- $a_{i+1} \notin I_i$ for all $i \in \mathbb{N}$.

$(8 \to 7)$. Let $\mathcal{I} = \langle a_i : i \in \mathbb{N} \rangle$. Let $\varphi(\langle n, r \rangle)$ say that $r \in R$ is generated by $a_0, \dots, a_n$. Observing that φ is Σ^0_1, by Lemma 1.3, let $\langle \mathcal{I}_n : n \in \mathbb{N} \rangle$ be an enumeration of elements that satisfies φ. Clearly $\langle \mathcal{I}_n \rangle$ is a desired ascending chain of Σ^0_1 ideals. $\square$

The idea of proof of $3 \to 1$ requires that I must include $\bigcup_{i\in\mathbb{N}} I_i$ and be included by $\bigcup_{i\in\mathbb{N}} I_i$, i.e., I must equal $\bigcup_{i\in\mathbb{N}} I_i$. On the other hand, the assertion that $\bigcup_{i\in\mathbb{N}} I_i$ exists for any ascending chain of ideals $\langle I_i : i \in \mathbb{N}\rangle$ is equivalent to ACA_0 over RCA_0.

Proposition 6.41. The following is equivalent over RCA_0.

1. ACA_0.
2. Let $\langle I_n : n \in \mathbb{N}\rangle$ be an ascending chain of ideals of a countable commutative ring. Then the ideal $\bigcup_{n\in\mathbb{N}} I_n = \{a \in R : (\exists n)(a \in I_n)\}$ exists.

Proof. The implication $1 \to 2$ is trivial. Reasoning within RCA_0 we show $2 \to 1$ via Lemma 1.9. Let $\alpha : \mathbb{N} \to \mathbb{N}$ be a one-to-one function. Let $R = \mathbb{Q}[x_0, x_1, \dots]$ be the polynomial ring over the rational field $\mathbb{Q}$ with countably infinitely many indeterminates. Define an ascending chain of ideals $\langle I_i : i \in \mathbb{N}\rangle$ as $p \in I_n$ if and only if every monomial $qx_{m_0}^{e_0}x_{m_1}^{e_1}\dots x_{m_l}^{e_l}$ of p contains at least one $i \le l$ such that $(\exists j < n)(\alpha(j) = m_i)$. By our assumption 2, $\bigcup_{n\in\mathbb{N}} I_n$ exists. It follows that $(\exists j)(\alpha(j) = i) \leftrightarrow x_i \in \bigcup_{n\in\mathbb{N}} I_n$ for all $i \in \mathbb{N}$. Thus by Δ^0_1 comprehension the image of α exists. This completes the proof. □

Definition 6.42. The following definitions are made in RCA_0. Let R be a countable commutative ring.

1. R is said to satisfy the *ascending chain condition on ideals* if every ascending chain $I_0 \subset I_1 \subset \cdots$ of ideals of R is stationary i.e., $(\exists n)(I_n = I_{n+1} = \cdots)$.
2. R is said to satisfy the *ascending chain condition on principal ideals* if every sequence $\langle a_i : i \in \mathbb{N}\rangle$ such that $(a_0) \subset (a_1) \subset \cdots$ of elements of R is stationary i.e., $(\exists n)((a_n) = (a_{n+1}) = \cdots)$.

In the rest of this section we prove the decomposition theorems for countable Noetherian rings within ACA_0.

Proposition 6.43. The following is provable in ACA_0. Let R be a countable commutative ring with the ascending chain condition on principal ideals. If an element $a \in R$ is not 0_R nor a unit then there exists a sequence of irreducible elements $\langle b_i : i < n\rangle$ of finite length such that $a = \prod_{i<n} b_i$.

Proof. We reason within ACA_0. Let the arithmetical formula $\varphi(x, y)$ say that if $x \in R$ and x is not a product of any finite sequence of irreducible elements then $y \in R$, $y|x$, $x \not| y$, and y is not a product of any finite sequence of irreducible elements. It follows that $(\forall x)(\exists y)\varphi(x, y)$ and by arithmetical comprehension we have $(\exists f)(\forall x)\varphi(x, f(x))$. We show the contraposition of the statement. Let $a \in R$ not be 0_R nor a unit and suppose that a is not a product of any finite sequence of irreducible elements. Then we have an ascending chain

$$(a_0) \subsetneq (a_1) \subsetneq \cdots$$

of principal ideals by primitive recursion by putting $a_0 = a$ and $a_{i+1} = f(a_i)$. This complete the proof. □

Moreover, RCA_0 proves that if R is a Σ^0_1 PID then the decomposition is unique up to order and units. Thus RCA_0 proves that every Σ^0_1 PID is a UFD.

Proposition 6.44. The following is provable in ACA_0. Let R be a countable commutative ring with the ascending chain condition on ideals. If $I \subset R$ is an ideal then there exists a sequence of irreducible ideals $\langle J_i : i < n\rangle$ of finite length such that $I = \bigcap_{i<n} J_i$.

Proof. We reason within ACA_0. Assume for a contradiction that there does not exist a sequence of irreducible ideals $\langle J_i : i < n\rangle$ of finite length such that $I = \bigcap_{i<n} J_i$. Let the formula $\varphi(x, y)$ say that if x is finite sequence of elements of R and the ideal generated by $I \cup \{x_0, \ldots, x_{\mathrm{lh(x)}-1}\}$ is not expressive as an intersection of finite number of irreducible ideals then y is an extension of x of the form $x^\frown\langle r\rangle$ $(r \in R)$ such that $r \notin (I \cup \{x_0, \ldots, x_{\mathrm{lh(x)}-1}\})$ and the ideal generated by $I \cup \{x_0, \ldots, x_{\mathrm{lh(x)}-1}, r\}$ is not also expressive as an intersection of finite number of irreducible ideals. Since every ideal of R is finitely generated, φ can be taken as an arithmetical formula. We have $(\forall x)(\exists y)\varphi(x, y)$ and by arithmetical comprehension $(\exists f)(\forall x)\varphi(x, f(x))$. Define $\langle s_i : i \in \mathbb{N}\rangle$ by primitive recursion by putting $s_0 =$ the empty sequence and $s_{i+1} = f(s_i)$. Define $\langle a_i : i \in \mathbb{N}\rangle$ by putting $a_i =$ the last component of s_{i+1}. It follows that $(a_0) \subsetneq (a_0, a_1) \subsetneq \cdots$ is a strict ascending chain of ideals, a contradiction with the ascending chain condition. This completes the proof. □

Proposition 6.45. RCA_0 proves that every irreducible ideal of a countable commutative ring with the ascending chain condition on ideals is a primary ideal.

Proof. We reason within RCA_0. Let I be an irreducible ideal of a countable commutative ring R with the ascending chain condition. Let $a, b \in R$ be such that $ab \in I$ and $(\forall i \geq 1)(b^i \notin I)$. It is enough to show that $a \in I$. By Δ^0_1 comprehension let $\langle J_i : i \in \mathbb{N}\rangle$ be an ascending chain of ideals such that $J_i = I : (b^i)$. By the assumption let n be such that $(\forall i \geq n)(J_i = J_n)$. We shall show that $I = (I \cup \{a\}) \cap (I \cup \{b^n\})$. Let $r = s + tb^n \in (I \cup \{a\}) \cap (I \cup \{b^n\})$ $(s \in I, t \in R)$. Since $r \in (I \cup \{a\})$ and $ab \in I$ we have $rb \in I$. Therefore we have $tb^{n+1} = rb - sb \in I$ and hence $t \in I : (b^{n+1}) = J_{n+1} = J_n = I : (b^n)$. Therefore $tb^n \in I$ and hence $r = s + tb^n \in I$. Thus $I = (I \cup \{a\}) \cap (I \cup \{b^n\})$ and since I is irreducible we have $a \in I$. This completes the proof. □

By the previous two proposition it follows that ACA_0 proves the Lasker-Noether primary decomposition theorem for a countable commutative rings. Moreover, RCA_0 proves the uniqueness of the primary decomposition. The exploration for reversals will be quite interesting work.

6.6 Other Topics

Simpson [60] showed that Hilbert basis theorem is equivalent over RCA_0 to the assertion $\mathrm{WO}(\omega^\omega)$ that the ordinal number ω^ω is well ordered. Here Hilbert basis theorem is formalized as for any countable field K and any $m \in \mathbb{N}$, every Σ^0_1

ideal of $K[x_0, \ldots, x_m]$ is finitely generated. It is known that $\mathsf{I}\Sigma^0_1$ does not imply $\mathrm{WO}(\omega^\omega)$, that $\mathrm{WO}(\omega^\omega)$ is implied by $\mathsf{I}\Sigma^0_2$, that $\mathrm{WO}(\omega^\omega)$ does not imply $\mathsf{B}\Sigma^0_2$, and that $\mathrm{WO}(\omega^\omega) + \mathsf{B}\Sigma^0_2$ does not imply $\mathsf{I}\Sigma^0_2$ over RCA_0 [62]. This is an example of Reverse Mathematics which is not classified into "big five" systems. The theorem remains valid if we replace K by any countable commutative Noetherian ring. The logical strength of the replaced version is not known.

Hatzikiriakou [27] showed that ACA_0 is equivalent over RCA_0 to the existence of the integral closure of a countable commutative ring. He also developed the theory of prime ideals including Lying Over, Going Down, and Going Up theorem within WKL_0. The reversals remain open.

Conidis [8, 9] developed the theory of Artinian rings within WKL_0 with Reverse Mathematics results. One possible reason why WKL_0 suffices is that every prime ideal of an Artinian ring is maximal. Especially he showed that WKL_0 is equivalent over $\mathsf{RCA}_0 + \mathsf{I}\Sigma^0_2$ to the Akizuki-Hopkins theorem which asserts that every countable commutative Artinian ring is Noetherian. He also showed that WKL_0 is equivalent over RCA_0 to the structural theorem which asserts that every countable commutative Artinian ring is isomorphic to a finite direct product of local Artinian rings. In connection with this result, we can consider the Artin-Wedderburn theorem for (not necessarily commutative) rings.

Definition 6.46. The following definitions are made within RCA_0. Note that a countable ring in this definition is not necessarily commutative. A countable ring R is said to be *simple* if

$$(\forall a \in R)(\forall b \in R \setminus \{0_R\})(\exists x, y \in R)(a = xby).$$

Note that if a countable ring R is simple then R does not have any nontrivial proper ideal. A countable ring R is said to be *semisimple* if R is isomorphic to the finite product of simple rings. A ring R is said to be *left Artinian* if there does not exists an infinite strictly descending chain of left ideals

$$I_0 \supsetneq I_1 \supsetneq \cdots \supsetneq I_n \supsetneq \cdots .$$

The Artin-Wedderburn theorem for countable rings is formalized within RCA_0 as follows. The following are equivalent for any countable ring R.

1. R is left Artinian and $\mathrm{Jac}(R) = \{0_R\}$.
2. R is semisimple, i.e., there exists simple rings $R_0, R_1, \ldots, R_n$ such that
$$R \cong R_0 \oplus R_1 \oplus \cdots \oplus R_n.$$
3. R is isomorphic to the finite product of matrix rings over division rings, i.e., there exists division rings $D_0, D_1, \ldots, D_n$ and positive integers $m_0, m_1, \ldots, m_n$ such that
$$R \cong M_{m_0}(D_0) \oplus M_{m_1}(D_1) \oplus \cdots \oplus M_{m_n}(D_n).$$

Wedderburn's part is $2 \leftrightarrow 3$ and Artin's part is $1 \leftrightarrow 2$. By routine inspection, we see that Wedderburn's part is provable within RCA_0. On the other hand, Artin's part implies the structural theorem above and hence WKL_0 over RCA_0. It is expected that WKL_0 proves Artin's part extending Conidis' method to the noncommutative case.

References

[1] Abian, S. and Brown, A. A theorem on partially ordered sets, with applications to fixed point theorems. *Canadian Journal of Mathematics, 13, 78-82*, 1961.

[2] Arslanov, M. M. Some generalizations of a fixed-point theorem. *Izv. Vyssh. Uchebn. Zaved. Mat. 25, number 5, 9-16, translated in: Soviet Math. (Iz. VUZ) 25, number 5, 1-10*, 1981.

[3] Bernays, P. and Hilbert, D. *Grundlagen der Mathematik volume I.* Springer, 1934.

[4] Birkhoff, G. *Lattice Theory.* American Mathematical Society Colloquium Publications, 1940.

[5] Bourbaki, N. Sur le théorème de Zorns. *Archiv der Mathematik 2:6, 434-437*, 1949.

[6] Chandler, B. and Magnus, W. *The History of Combinatorial Group Theory: A Case Study in the History of Ideas.* Springer-Verlag, New York, 1982.

[7] Chubb, J., Hirst, J. L., and McNicholl, T. H. Reverse mathematics, computability, and partitions of trees. *The Journal of Symbolic Logic, volume 74, number 1, March*, 2009.

[8] Conidis, C. J. Chain conditions in computable rings. *Transactions of the American Mathematical Society, volume 362(12) 6523-6550*, 2010.

[9] Conidis, C. J. A new proof that Artinian implies Noetherian via weak König's lemma. *Preprint*, 2012.

[10] Cook, S. and Nguyen, P. *Logical Foundations of Proof Complexity.* Cambridge University Press, 2010.

[11] Davey, B. A. and Priestley, H. A. *Introduction to Lattices and Order (second edition).* Cambridge University Press, 2002.

[12] Davis, A. A characterization of complete lattices. *Pacific Journal of Mathematics, 5, 311-319*, 1955.

[13] Downey, R. , Hirschfeldt, D. R. , Kach, A. M. , Lempp, S. , Mileti, J. R. , and Montálban, A. Subspaces of computable vector spaces. *Journal of Algebra 314, 888-894*, 2007.

[14] Downey, R. , Lempp, S. , and Mileti, J. R. Ideals in computable rings. *Journal of Algebra 314, 872-887*, 2007.

[15] Friedman, H. Some systems of second order arithmetic and their use, in Proceedings of the International Congress of Mathematicians (Vancouver, 1974), volume 1. *Canadian Math. Congress, 235-242*, 1975.

[16] Friedman, H., Simpson, S. G., and Smith, R. Countable algebra and set existence axioms. *Annals of Pure and Applied Logic 25, 141-181*, 1983.

[17] Friedman, H., Simpson, S. G., and Smith, R. Addendum to: "Countable algebra and set existence axioms". *Annals of Pure and Applied Logic 28, 319-320*, 1985.

[18] Frittaion, E. and Marcone, A. Linear extensions of partial orders and reverse mathematics. *Mathematical Logic Quarterly 58, 417-423*, 2012.

[19] Fuchs, L. *Abelian Groups.* Publishing House of the Hungarian Academy of Science, Budapest Mathematics , 1958.

[20] Fuchs, L. *Infinite Abelian Groups: volume 1.* Academic Press, New York, 1970.

[21] Fujiwara, M. and Sato, T. Note on total and partial functions in second order arithmetic. *Kyoto University RIMS Kokyuroku 1950*, 2015.

[22] Gödel, K. *The Incompleteness Theorem (Japanese translation by Hayashi, S. and Yasugi, M.).* Iwanami Shoten, 2006.

[23] Granas, A. and Dugundji, J. *Fixed Point Theory.* PWN-Polish Scientific Publishers, 1982.

[24] Granas, A. and Dugundji, J. *Fixed Point Theory.* Springer, 2003.

[25] Hájek, P. and Pudlák, P. *Metamathematics of First-Order Arithmetic.* Springer-Verlag, Berlin, Heidelberg, New York, 1993.

[26] Hatzikiriakou, K. Algebraic disguises of Σ^0_1 induction. *Archives of Mathematical Logic 29, 47-51*, 1989.

[27] Hatzikiriakou, K. Extensions of commutative rings in subsystems of second order arithmetic. *5th Panhellenic Logic Symposium*, 2005.

[28] Higgins, P. M. *Techniques of Semigroup Theory.* Oxford University Press, 1992.

[29] Hirschfeldt, D. R. Slicing the Truth: On the Computability Theoretic and Reverse Mathematical Analysis of Combinatorial Principles. *to appear*, 2010.

[30] Hirst, J. L. *Combinatorics in subsystems of second order arithmetic.* PhD thesis, Pennsylvania State University, 1987.

[31] Hirst, J. L. Connected components of graphs and reverse mathematics. *Archives of Mathematical Logic 31, 183-192*, 1992.

[32] Hoffman, P. A proof of Isbell's zigzag theorem. *Journal of the Australian Mathematical Society volume 84, issue 02, April, 229-232*, 2008.

[33] Honda, K. Realism in the theory of abelian groups I. *Commentarii Mathematici Universitatis Sancti Pauli 5, 37-75*, 1956.

[34] Honda, K. and Nagata, M. *Abelian Groups and Algebraic Groups (in Japanese)*. Kyoritsu Shuppan, 1969.

[35] Hotta, R. *Introduction to Algebra Groups, Rings and Modules (in Japanese)*. Syokabo, 1987.

[36] Howie, J. M. *Fundamentals of Semigroup Theory*. Oxford University Press, 1996.

[37] Ishihara, H. Constructive reverse mathematics: compactness properties (in Crosilla, L. and Schuster, P., editors, From Sets and Types to Analysis and Topology, Oxford Logic Guides 48, pages 245?267). *Oxford University Press*, 2005.

[38] Jockusch, Jr., C. G. Ramsey's theorem and recursion theory. *The Journal of Symbolic Logic volume 37, 268-280*, 1972.

[39] Kantorovitch, L. The method of successive approximations for functional equations. *Acta Mathematica 71, 63-97*, 1939.

[40] Kirby, L. A. S. and Paris, J. B. Σ_n-collection schemas in arithmetic. *Logic Colloquium '77, Stud, Logic Foundations Math. 96, North-Holland, Amsterdam-New York, 199-209*, 1975.

[41] Knaster, B. Un théorème sur les fonctions d'ensembles. *Ann. Soc. Polon. Math. 6, 133-134*, 1927.

[42] Kohlenbach, U. *Applied Proof Theory: Proof Interpretations and Their Use in Mathematics*. Springer-Verlag Berlin Heidelberg, 2008.

[43] Lerman, M., Solomon, R., and Towsner, H. Separating principles below Ramsey's theorem for pairs. *Preprint*, 2013.

[44] Liu, J. RT^2_2 does not imply WKL_0. *The Journal of Symbolic Logic volume 77 number 2, 609-620*, 2012.

[45] Magnus, W., Karrass, A., and Solitar, D. *Combinatorial Group Theory: Presentations of Groups in Terms of Generators and Relations (second revised edition)*. Dover Publications, 1976.

[46] Markowsky, G. Chain-complete posets and directed sets with applications. *Algebra Universalis 6, 53-68*, 1976.

[47] Miller, C. F. Decision problems for groups: survey and reflections. *Algorithms and Classification in Combinatorial Group Theory (eds. Baumslag, G. and Miller III, C. F.), MSRI Publications number 23, Springer-Verlag, 1-59*, 1992.

[48] Morita, Y. *Introduction to Algebra (in Japanese).* Shokabo, 1987.

[49] Nagao, H. *Algebra (in Japanese).* Asakura Shoten, 1983.

[50] Nielsen, J. Om regning med ikke kommutative faktorer og dens anvendelse i gruppeteorien. *Matematisk Tidsskrift B, 77-94. English translation: Math. Scientist 6, 73-85 (1981). I. 6. D. II. 2,5,7*, 1921.

[51] Rangaswamy, K. M. Characterization of intersections of neat subgroups of abelian groups. *Journal of Indian Mathematical Society 29, 31-36*, 1965.

[52] Reid, M. *Undergraduate Commutative Algebra.* Cambridge University Press, 1995.

[53] Roman, S. *Lattices and Ordered Sets.* Springer, 2008.

[54] Sato, T. Reverse mathematics and Isbell's zig-zag theorem. *Mathematical Logic Quarterly, volume 60, issue 4-5, August 2014, 348-353*, 2014.

[55] Schröder, B. *Ordered Sets An Introduction.* Birkhäuser, 2002.

[56] Seetapum, D. and Slaman, T. A. On the strength of Ramsey's theorem. *Notre Dame Journal for Formal Logic 36, 570-582*, 1995.

[57] Shinoda, J. *Recursive Functions and Predicates (in Japanese).* Kawai bunka kyouiku kenkyujo, 1997.

[58] Shioji, N. and Tanaka, K. Fixed point theory in weak second-order arithmetic. *Annals of Pure and Applied Logic, 47, 167-188.*, 1990.

[59] Shore, R. A. and Hirschfeldt, D. R. Combinatorial principles weaker than Ramsey's theorem for pairs. *The Journal of Symbolic Logic volume 72, issue 1, 171-206*, 2007.

[60] Simpson, S. G. Ordinal numbers and the Hilbert basis theorem. *The Journal of Symbolic Logic volume 53 number 3, September*, 1988.

[61] Simpson, S. G. *Subsystems of Second Order Arithmetic (second edition).* Cambridge University Press, 2009.

[62] Simpson, S. G. Comparing WO(ω^ω) with Σ^0_2 induction. *arXiv*, 2015.

[63] Simpson, S. G. and Smith, R. L. Factorization of polynomials and Σ^0_1 induction. *Annals of Pure and Applied Logic 31, 289-306*, 1986.

[64] Soare, R. I. *Recursively Enumerable Sets and Degrees: A Study of Computable Functions and Computably Generated Sets.* Springer-Verlag, Berlin, Heidelberg, 1987.

[65] Solomon, R. *Reverse mathematics and ordered groups.* PhD thesis, Cornell University, 1998.

[66] Solomon, R. Ordered groups: a case study in reverse mathematics. *The Bulletin of Symbolic Logic volume 5, number 1, March*, 1999.

[67] Specker, E. Ramsey's theorem does not hold in recursive set theory. *Logic Colloauium '69, Stud. Logic Found. Math., North-Holloand, Amsterdam*, 1971.

[68] Tamura, T. *Semigroup Theory (in Japanese).* Kyoritsu Shuppan, 1972.

[69] Tanaka, K. *Reverse Mathematics and Second Order Arithmetic (in Japanese).* Kawai bunka kyouiku kenkyujo, 1997.

[70] Tarski, A. A lattice-theoretical fixpoint theorem and its applications. *Pacific Journal of Mathematics, 5, 285-309*, 1955.

[71] Taskovic, M. R. New equivalents of the axiom of choice and consequences. *Mathematica Moravica volume 13-1, 77-94*, 2009.

[72] van der Waerden, B. L. *Modern Algebra volume I.* Frederick Ungar Publishing Company, 1949.

[73] Weyl, H. *Das Kontinuum.* Leipzig, Verlag von Veit and Comp., 1918.

[74] Witt, E. Beweisstudien zum satz von M. Zorns. *Mathematische Nachrichten 4, 434-438*, 1951.