REVERSE MATHEMATICS AND ORDERED GROUPS

David Reed Solomon

August 28, 2003

Contents

Chapter 1

Computable and Reverse Mathematics

This chapter is an introduction to computable (or effective) mathematics and to reverse mathematics, both of which will later be used to study theorems of ordered groups. Computable mathematics involves applying ideas of computability theory to other areas of mathematics. By computable, we will always mean Turing computable. A typical question we might consider is whether the effective version of a particular theorem holds. That is, is the theorem true if all the objects in it are assumed to be computable? Precise definitions and concrete examples are given in Section 1.1.

Reverse mathematics is based more in proof theory, although as we shall see, it uses techniques from all areas of logic and has consequences in computable mathematics. The basic definitions and results are given in Section 1.2.

The last section of the chapter is a summary of the results contained later.

1.1 Computable Mathematics

We first give the general definition for a computable structure and then repeat it in the special case of groups. The languages involved are always assumed to be computable.

Definition 1.1. A model $\mathfrak{A}$ is **computable** if its domain $A \subseteq \omega$ is a computable set and its relations and functions are uniformly computable.

Definition 1.2. A **computable group** is a computable set $G \subseteq \omega$ together with a computable function $\cdot_G$ which satisfies the usual group axioms. We will let 1_G (or sometimes 0_G in the abelian case) stand for the identity element.

We are interested in studying the conditions under which effective versions of theorems hold. For example, consider the following theorem:

Theorem 1.3. *If H is a normal subgroup of a group G, then G/H is a group.*

The effective version of this theorem says:

Theorem 1.4. *If H is a computable normal subgroup of a computable group G, then G/H is a computable group.*

If we are careful defining what we mean by G/H, the effective version will be true. Define $G/H \subseteq \omega$ by choosing the ω–least representative for each coset:

$$\{ \, g \in G \mid \forall n < g(n \notin G \vee n^{-1}g \notin H) \, \}.$$

This definition picks out the least representative because $nH = gH$ if and only if $n^{-1}g \in H$. To define multiplication $\cdot_{G/H}$, use the formula:

$$a \cdot_{G/H} b = c \;\leftrightarrow\; a, b, c \in G/H \wedge c^{-1} \cdot_G a \cdot_G b \in H.$$

Thus the effective version of the theorem holds.

Contrast this situation with the following example.

Definition 1.5. A **binary branching tree** is a set $T \subseteq \{0,1\}^{<\omega}$ such that

$$\forall \sigma, \tau \in \{0,1\}^{<\omega} \left(\sigma \subseteq \tau \wedge \tau \in T \rightarrow \sigma \in T \right).$$

A **path** through T is a function $f : \omega \rightarrow \{0,1\}$ such that $f[n] \in T$ for all n, where $f[n]$ is the sequence $\langle f(0), \dots f(n) \rangle$.

Weak König's Lemma. *Every infinite binary branching tree has a path.*

The effective version of Weak König's Lemma says that every infinite computable binary branching tree has a computable path. Unfortunately, this statement is false. Jockusch Jr. and Soare (1972), however, modified the effective version to discover some computational content in Weak König's Lemma. Recall that a set $A \subseteq \omega$ is low if it has the lowest possible Turing jump, $A' = 0'$.

Low Basis Theorem (Jockusch Jr. and Soare (1972)). *Every infinite computable binary branching tree has a low path.*

One of our goals will be to give a similar analysis for theorems about ordered groups. Computably bounded Π^0_1 classes will play an important role in this analysis.

Definition 1.6. $C \in \{0,1\}^\omega$ is a **computably bounded (c.b.) $\mathbf{\Pi^0_1}$ class** if there is a computable binary branching tree T such that C is the set of paths through T.

Definition 1.7. Let $A, B \in \omega$ and $A \cap B = \emptyset$. S is a **separating set** for A and B if either $A \subseteq S \wedge S \cap B = \emptyset$ or $B \subseteq S \wedge S \cap A = \emptyset$.

Definition 1.8. $C \subseteq \{0,1\}^\omega$ is a **$\mathbf{\Pi^0_1}$ class of separating sets** if there are computably enumerable (c.e.) sets A and B such that C is the class of characteristic functions for the separating sets of A and B.

Notice that not all c.b. Π^0_1 classes are Π^0_1 classes of separating sets. In particular, a c.b. Π^0_1 class may have cardinality ω, but any Π^0_1 class of separating sets have either finite cardinality or cardinality 2^ω. The Low Basis Theorem was originally stated as every c.b. Π^0_1 class has a member of low degree. Jockusch Jr. and Soare (1972) proved a number of other results about c.b. Π^0_1 classes which we will have reason to refer to later.

Theorem 1.9 (Jockusch Jr. and Soare (1972)). *There is an infinite c.b. Π^0_1 class C such that for all $f, g \in C$, if $f \neq g$, then f and g are Turing incomparable.*

Theorem 1.10 (Jockusch Jr. and Soare (1972)). *There are c.e. sets A and B such that $A \cap B = \emptyset$, $A \cup B$ is coinfinite and if D, E are separating sets for A and B, then either D and E have the same Turing degree or they are Turing incomparable.*

To fix some notation before moving on, we will use $\leq_T$ for Turing reducibility, $\equiv_T$ for Turing equivalence, $\deg(A)$ for the Turing degree of A, $0'$ for the degree of the halting problem and $0^{(n)}$ for the n^{th} jump of $\emptyset$. This notation and others we will use follows Soare (1980).

1.2 Reverse Mathematics

Reverse mathematics is a branch of logic started by Harvey Friedman in the 1970's. It seeks to answer the question: *Which set existence axioms are required to prove the theorems of ordinary mathematics*? In addition to being interesting in their own right, answers to this question often have consequences in both effective mathematics and the foundations of mathematics. Before discussing these consequences, we need to be more specific about the motivating question.

Ordinary mathematics refers to the areas of mathematics that remained unchanged by the introduction of abstract set theory. These areas concern either countable or essentially countable mathematics. Essentially countable mathematics is another vague term that is best explained by an example. The study of complete separable metric spaces involves essentially countable mathematics because, although the spaces may be uncountable, they can be understood in terms of a countable basis. Simpson (1985) gives the following list of areas included in ordinary mathematics: number theory, geometry, calculus, differential equations, real and complex analysis, combinatorics, countable algebra, separable Banach spaces, computability theory, and the topology of complete separable metric spaces. Ordinary mathematics usually does not include abstract functional analysis, abstract set theory, universal algebra, or general topology.

The rest of this chapter is an introduction to reverse mathematics and to some of the definitions and notation used later. For more information and results, in particular for more examples of equivalences between theorems and subsystems of second order arithmetic, see Friedman et al. (1983), Hirst (1994), Simpson (1984), Simpson (1985) or Simpson (Unpublished). We will mostly follow the notation found in Friedman et al. (1983) and Simpson (Unpublished).

The setting for reverse mathematics is second order arithmetic. Second order arithmetic uses a two sorted first order language, $\mathcal{L}_2$. $\mathcal{L}_2$ has both number variables and set variables. The number variables are denoted by lower case letters and are intended to range over elements of ω. The set variables are denoted by capital letters and are intended to range over $\mathcal{P}(\omega)$. Because $\mathcal{L}_2$ has two types of variables it also has two types of quantifiers: $\exists X, \forall X$ and $\exists x, \forall x$. The terms of $\mathcal{L}_2$ are built from the number variables and the constants $0, 1$ using the function symbols $+, \cdot$. Atomic formulas have the form $t_1 = t_2$, $t_1 < t_2$ or $t_1 \in X$ where t_1, t_2 are terms. General formulas are built from the atomic formulas using the standard logical connectives and the two types of quantifiers.

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

$$\mathfrak{A} \;=\; \langle A, S_A, +_A, \cdot_A, 0_A, 1_A, <_A \rangle.$$

The number variables range over A, the set variables range over $S_A \subseteq \mathcal{P}(A)$, and the functions, constants, and relations are interpreted as indicated.

The axioms for second order arithmetic fall into three categories. The basic axioms specify the properties of $+, \cdot, 0, 1$ and $<$.

$$\begin{array}{rl} n+1 \neq 0 & m+1 = n+1 \rightarrow m = n \\ m+0 = m & m+(n+1) = (m+n)+1 \\ m \cdot 0 = 0 & m \cdot (n+1) = m \cdot n + m \\ \neg m < 0 & m < n+1 \leftrightarrow (m < n \vee m = n) \end{array}$$

There is an induction axiom for sets,

$$\big(\, 0 \in X \;\wedge\; \forall n\, (n \in X \rightarrow n+1 \in X)\,\big) \rightarrow \forall n\, (n \in X)$$

and a comprehension scheme for forming sets,

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

where φ is any formula of $\mathcal{L}_2$ in which X does not occur freely. φ may contain other free variables as parameters. The following formula induction scheme is derivable from the comprehension scheme and the induction axiom:

$$\big(\, \varphi(0) \;\wedge\; \forall n\, (\varphi(n) \rightarrow \varphi(n+1)\,)\,\big) \rightarrow \forall n\, \varphi(n).$$

The formal system of second order arithmetic is denoted by Z_2.

The intended model of Z_2 is

$$\langle \omega, \mathcal{P}(\omega), +, \cdot, 0, 1, < \rangle.$$

Models of Z_2 can be nonstandard in two different ways. The set over which the number variables range could be nonstandard or the nonstandard model could be of the form

$$\langle \omega, S, +, \cdot, 0, 1, < \rangle$$

where $S \subsetneq \mathcal{P}(\omega)$. Models in which the number variables range over ω are called ω–models.

The question of which set existence axioms are needed to prove a particular theorem is answered by examining which instances of the comprehension scheme are required. Hence, we examine subsystems of Z_2 which arise from restricting the formulas over which the comprehension scheme applies. One consequence of limiting comprehension is that the formula induction scheme is also limited. We may add some extra formula induction, but we will not add full formula induction because this scheme is a disguised set existence principle. For a complete discussion of this issue, see Friedman et al. (1983) and Simpson (Unpublished). A surprising observation is that the motivating question can be answered for a remarkable number of theorems by examining only five subsystems of Z_2. These subsystems are presented below in increasing order of strength.

The weakest subsystem considered here is RCA_0. RCA_0 stands for recursive comprehension axiom and is obtained by restricting the comprehension scheme to apply only to Δ^0_1 formulas. This restricted scheme is called Δ^0_1 comprehension. We also allow Σ^0_1 induction:

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

where φ is Σ^0_1. Friedman et al. (1983) show that RCA_0 proves the Π^0_1 formula induction scheme as well. Because RCA_0 contains Δ^0_1 comprehension and the comprehension scheme allows parameters, it follows that every model of RCA_0 is closed under Turing reduction. The minimum ω–model is

$$\langle \omega, REC, +, \cdot, 0, 1, < \rangle$$

where $REC \subseteq \mathcal{P}(\omega)$ is the set of computable sets.

Proving theorems in RCA_0 has consequences in computable mathematics. If a theorem is provable in RCA_0 then its effective or computable version is true. We will see the following example of this phenomenon in Chapter 6. Given suitable definitions, Friedman et al. (1983) showed that RCA_0 suffices to prove that every field has an algebraic closure. This result implies that every computable field has a computable algebraic closure, a result first proved earlier in Rabin (1960). Because of this connection to computable mathematics, we will be content once we have a proof in RCA_0 and will not seek a proof in a weaker subsystem. For results regarding weaker subsystems, see Hatzikiriakou (1989)

RCA_0 is strong enough to establish the basic facts about the number systems $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ and $\mathbb{R}$. This fact makes RCA_0 strong enough to be a reasonable base theory over which to do coding. The set of natural numbers, $\mathbb{N}$, is defined by $\forall n\,(n \in \mathbb{N})$ and the integers and rationals are defined with the help of the standard pairing function:

$$\langle x, y \rangle = \frac{1}{2}(i+j)(i+j+1) + i.$$

Associated with this pairing function are two projection functions:

$$\pi_1(\langle x, y \rangle) = x \qquad \text{and} \qquad \pi_2(\langle x, y \rangle) = y.$$

Notice that we will use ω to denote the standard natural numbers and $\mathbb{N}$ to denote the (possibly nonstandard) universe of a model of a subsystem of Z_2.

The real numbers do not form a set in Z_2; they must be represented by Cauchy sequences of rationals. Simpson (Unpublished) gives the following definitions.

Definition 1.11. (RCA_0) A **sequence of rational numbers** is a function $f : \mathbb{N} \to \mathbb{Q}$. Frequently we denote this sequence by $\langle q_k \,|\, k \in \mathbb{N}\rangle$.

Definition 1.12. (RCA_0) A **real number** is a sequence of rational numbers $\langle q_k \,|\, k \in \mathbb{N}\rangle$ such that

$$\forall k \, \forall i \, (\ |\, q_k - q_{k+i} \,| < 2^{-k}\ ).$$

We write $x \in \mathbb{R}$ to mean that x is a sequence of rationals satisfying this convergence rate. $0_{\mathbb{R}}$, or when it is not ambiguous just 0, denotes the sequence $\langle 0 \,|\, k \in \mathbb{N}\rangle$ and $1_{\mathbb{R}}$, or just 1, denotes $\langle 1 \,|\, k \in \mathbb{N}\rangle$.

Definition 1.13. (RCA_0) Let $x = \langle q_k \,|\, k \in \mathbb{N}\rangle$ and $y = \langle q'_k \,|\, k \in \mathbb{N}\rangle$ be two real numbers. We say $\mathbf{x} = \mathbf{y}$ if

$$\forall k \, (\ |\, q_k - q'_k \,| \leq 2^{-k+1}\ ).$$

The sum $\mathbf{x} + \mathbf{y}$ is the sequence

$$\langle q_{k+1} + q'_{k+1} \,|\, k \in \mathbb{N}\rangle.$$

The product $\mathbf{x} \cdot \mathbf{y}$ is the sequence

$$\langle q_{n+k} \cdot q'_{n+k} \,|\, k \in \mathbb{N}\rangle$$

where n is the least natural number such that $2^n \geq |\, q_0 \,| + |\, q_1 \,| + 2$.

With these definitions it can be shown in RCA_0 that the real number system obeys all the axioms of an Archimedean ordered field.

RCA_0 is strong enough to define sets of unique codes for finite sets and finite sequences. For the details of this coding, see Simpson (Unpublished). We will denote the set of finite sequences of elements of X by Fin_X. RCA_0 also suffices to define the length function $\mathrm{lh} : \mathrm{Fin}_X \to \mathbb{N}$. For $\sigma \in \mathrm{Fin}_X$, the i^{th} element in σ is denoted $\sigma(i)$, and σ is written

$$\langle \sigma(0), \ldots, \sigma(\mathrm{lh}(\sigma) - 1)\rangle.$$

If $\sigma, \tau \in \mathrm{Fin}_X$, then $\sigma \subseteq \tau$ if $\mathrm{lh}(\sigma) \leq \mathrm{lh}(\tau)$ and for all $i < \mathrm{lh}(\sigma)$, $\sigma(i) = \tau(i)$. The concatenation of σ and τ is written $\sigma^\frown\tau$. For any function $f : \mathbb{N} \to \mathbb{N}$, $f[n]$ is the sequence $\langle f(0), \ldots, f(n-1)\rangle$.

Definition 1.14. (RCA_0) A **tree** is a set $T \subseteq \mathrm{Fin}_{\mathbb{N}}$ such that T is closed under initial segments:

$$\forall \sigma, \tau \, \big((\sigma, \tau \in \mathrm{Fin}_{\mathbb{N}} \wedge \sigma \subseteq \tau \wedge \tau \in T) \to \sigma \in T \big).$$

T is **finitely branching** if each element of T has only finitely many successors:

$$\forall \sigma \, \exists n \, \forall m \, (\sigma^\frown\langle m\rangle \in T \rightarrow m < n).$$

T is **binary branching** if every element of T has at most two successors. T is **bounded** if there exists a function $f : \mathbb{N} \rightarrow \mathbb{N}$ such that for all $\tau \in T$ and all $m < \mathrm{lh}(\tau)$, $\tau(m) < f(m)$. A **path** through T is a function $g : \mathbb{N} \rightarrow \mathbb{N}$ such that $g[n] \in T$ for all n.

König's Lemma. *Every infinite finitely branching tree has a path.*

Weak König's Lemma. *Every infinite binary branching tree has a path.*

Bounded König's Lemma. *Every infinite bounded tree has a path.*

Each of these lemmas is really a set existence principle; they each assert the existence of certain functions. König's Lemma is strictly stronger than Weak König's Lemma, and Weak König's Lemma and Bounded König's Lemma are equivalent. As we saw in Section 1.1, the effective version of Weak König's Lemma fails.

The second subsystem of Z_2 is called WKL_0 or Weak König's Lemma. It contains the axioms of RCA_0 plus Weak König's Lemma. Because the effective version of Weak König's Lemma fails, WKL_0 is strictly stronger than RCA_0. The best intuition for WKL_0 is that Weak König's Lemma adds a compactness principle to RCA_0.

We can now give a more formal explanation of the goals and methods of reverse mathematics. Consider a theorem Thm of ordinary mathematics which is stated in $\mathcal{L}_2$. If $RCA_0 \vdash Thm$ then from the viewpoint of reverse mathematics, we are satisfied. However, if $WKL_0 \vdash Thm$ and we cannot find a proof of Thm in RCA_0, then we want to show that WKL_0 is in some sense the weakest collection of set existence principles that proves Thm. To achieve this goal, we attempt to show for each axiom φ of WKL_0

$$RCA_0 + Thm \vdash \varphi.$$

We abbreviate this situation by $RCA_0 + Thm \vdash WKL_0$ or $RCA_0 \vdash Thm \leftrightarrow WKL_0$. If we prove $RCA_0 + Thm \vdash WKL_0$, then we have shown that Thm is equivalent to the subsystem WKL_0 and hence that no subsystem strictly weaker than WKL_0 can prove Thm. In particular, we can stop looking for a proof of Thm in RCA_0. The proof that $RCA_0 + Thm \vdash WKL_0$ is called the reversal of Thm and this process of proving axioms from theorems is the origin of the name reverse mathematics.

When trying to prove reversals, it is often helpful to use the following theorem.

Theorem 1.15. *(RCA_0) The following are equivalent:*

1. WKL_0
2. *For every pair of functions f, g such that for all m, n, $f(m) \neq g(n)$, there exists a set X such that for all m, $f(m) \in X$ and $g(m) \notin X$.*

One consequence of proving a theorem equivalent to WKL_0 is that the effective version of the theorem must fail. Although I have presented results in computable mathematics as consequences of results in reverse mathematics, usually the results in computable mathematics come first. If the effective version of a theorem is known to hold, then the proof that it holds can often be translated into RCA_0. Similarly, if the computable version fails, then why it fails often gives a hint as to how to use coding methods to prove a reversal. Provability in WKL_0 also has consequences for the foundations of mathematics. Because WKL_0 is Π^0_2 conservative over primitive recursive arithmetic, see Parsons (1970), it provides a modern rendering of Hilbert's Program. For a discussion of these consequences see Simpson (1988), Drake (1989) and Feferman (1988).

The third subsystem is ACA_0 or Arithmetic Comprehension Axiom. ACA_0 has the axioms of RCA_0 plus Σ^0_1 comprehension. It is strong enough to prove König's Lemma and hence is strictly stronger than WKL_0. Because ACA_0 contains Σ^0_1 comprehension, it can define the Turing jump of any set. Models of ACA_0 are closed under the Turing jump and the minimum ω–model is

$$\langle \omega, ARITH, +, \cdot, 0, 1, < \rangle$$

where $ARITH$ is the set of arithmetic sets.

The following theorem is helpful when proving reversals involving ACA_0.

Theorem 1.16. *(RCA_0) The following are equivalent:*

1. ACA_0
2. *The range of every one–to–one function exists.*

The fourth system is ATR_0 or Arithmetic Transfinite Recursion. The description of ATR_0 involves the notion of a well order.

Definition 1.17. (RCA_0) A **linear order** is a pair $(X, \leq_X)$ such that X is a set and $\leq_X$ is a binary relation on X such that:

$$\forall y \in X\,(y \leq_X y)$$
$$\forall y, z \in X\,(y \leq_X z \wedge z \leq_X y \rightarrow y = z)$$
$$\forall w, y, z \in X\,(w \leq_X y \wedge y \leq_X z \rightarrow w \leq_X z).$$

Definition 1.18. (RCA_0) A **well order** is a pair $(X, \leq_X)$ such that $(X, \leq_X)$ is a linear order and

$$\neg \exists x \in X\, \exists f : \mathbb{N} \rightarrow X\, \big(f(0) = x \wedge \forall i (f(i+1) <_X f(i))\big).$$

ATR_0 includes the axioms of ACA_0 plus axioms that allow arithmetic comprehension to be iterated along any well order. While ACA_0 is strong enough to prove that the n$^{\text{th}}$ Turing jump $0^{(n)}$ exists, ATR_0 is required to construct the uniform upper bound $0^{(\omega)}$. For a formal description of the axioms of ATR_0 see Friedman et al. (1983).

The last and most powerful subsystem is $\Pi_1^1 - CA_0$. $\Pi_1^1 - CA_0$ is ACA_0 plus the scheme of Π_1^1 comprehension. This system is strong enough to define Kleene's $\mathcal{O}$ and hence models of $\Pi_1^1 - CA_0$ are closed under the hyperjump. $\Pi_1^1 - CA_0$ is strictly stronger than ATR_0 and is useful for proving that certain recursions terminate. An example of this phenomenon is presented in Chapter 7. The following theorem is used to prove a reversal in that chapter.

Theorem 1.19. *(RCA_0) The following are equivalent:*

1. $\Pi_1^1 - CA_0$
2. *For any sequence of trees $\langle T_k \mid k \in \mathbb{N} \rangle$, there exists a set X such that $k \in X$ if and only if T_k has a path.*

1.3 Summary of Results

Now that we have the general definitions for reverse mathematics and computable mathematics, we can give a summary of the rusults to come.

In Chapter 2, we give the definitions and basic facts about partially and fully ordered groups. A partially ordered (p.o.) group is a group together with a partial order such that the order is preserved under multiplication on the left and the right. If the order is linear, the group is called fully ordered (f.o.).

A subgroup H of a p.o. group G is convex if for any $a, b \in H$ and $g \in G$,

$$a \leq g \leq b \Rightarrow g \in H.$$

For a convex normal subgroup H of a p.o. group G, there is not only a natural group structure on G/H, but also an induced partial order. If G is fully ordered, then this induced quotient order is a linear and its existence is provable in RCA_0. However, if G is only known to be partially ordered, then the existence of the induced order is equivalent to ACA_0.

Throughout this text, we will provide results in computable mathematics as corollaries to theorems in reverse mathematics. Since RCA_0 suffices to prove the existence of the induced order on the quotient of an f.o. group by a convex normal subgroup, it follows that if G is a computable fully ordered computable group and H is a computable convex normal subgroup, then the induced order on G/H is computable. By contrast, if G is a computably partially ordered computable group, then the induced order on G/H could be as complicated as $0'$.

One of the fundamental questions in ordered group theory is how to tell if a particular group admits a full order. In Chapter 3, we discuss three of the classical group conditions that insure full orderability. The fact that every torsion free abelian group is fully orderable was shown to be equivalent to WKL_0 by Hatzikiriakou and Simpson (1990). We extend this result to show the equivalence of WKL_0 and the theorem that every tosion free nilpotent group is fully orderable. RCA_0 suffices to show that the finite direct product of fully orderable groups is fully orderable, but WKL_0 is required for the case of infinite direct products.

Notice that we can again derive corollaries in computable mathematics. Downey and Kurtz (1986) were the first to give an example of a computable torsion free abelian group with no computable order. There is a uniform sequence of computably fully orderable computable groups such that the direct product, which is computable, has no computable order.

The center of a group G, denoted $C(G)$ or $\zeta_1(G)$, is defined by

$$C(G) \;=\; \{\, g \in G | \forall x (gx = xg) \,\}.$$

The existence of the center is equivalent to ACA_0, from which it follows that the center of a computable group (in fact a computable nilpotent group) can be as complicated as $0'$. In Chapter 8, this fact is used to explain why a particular method of construction for finitely generated nilpotent groups cannot be extended to infinitely generated nilpotent groups.

The last topic in Chapter 3 is the connection between computable bounded Π^0_1 classes and spaces of full orders of orderable computable groups. Once a group G is known to be fully orderable, it is natural to study the space of all full orders on G, denoted $\mathbb{X}(G)$. How many orders are there? What do they look like? How complicated can they be? We show that for any orderable computable group, there is a c.b. Π^0_1 class C and a Turing degree preserving bijection between C and $\mathbb{X}(G)$.

One alternative to looking for group conditions that imply full orderability is to look for semigroup conditions. In Chapter 4, we examine three classical semigroup conditions that imply full orderability and show that each is equivalent to WKL_0. The main trick here is to translate the conditions into the language of second order arithmetic is such a way that they can be studied inside RCA_0.

We next turn our attention to the analogue of the group theoretic result that every group can be represented as the quotient of a free group by a normal subgroup. In ordered group theory, every f.o. group is order isomorphic to the quotient of a f.o. free group by a convex normal subgroup. It turns out that RCA_0 is strong enough to prove this theorem, which answers an open question from Downey and Kurtz (1986) by showing that the effective version of the theorem holds. The proof is split between Chapter 5 and Appendix A. In Chapter 5, we develope the main argument assuming various technical facts, mostly explicit formulas for the embedding of free products into infinite matrix groups. These formulas, together with the definitions and basic facts about free groups and free products, are relegated to Appendix A.

In Chapter 6, we examine divisible closures and Hölder's Theorem. Hölder's Theorem is the main tool for classifying full orders of a particular fully orderable group. It states that every Archimedean fully ordered group is order isomorphic to a subgroup of the additive group of real numbers. Once we define what we mean by a subgroup of the reals in second order arithmetic, it turns out that RCA_0 suffices to prove Hölder's Theorem.

The motivation for studying divisible closures of abelian groups comes from similiar studies of algebraic closures of fields and real closures of ordered fields in Friedman et al. (1983), Smith (1981) and Metakides and Nerode (1979). The main questions about these notions of closure are those of existence, uniqueness and strong existence. In this context, strong existence means that the original algebraic object is isomorphic to a subspace of the closure. That is, the range of the embedding into the closure exists.

Friedman et al. (1983) answered the existence and uniqueness questions for the divisible closure of abelian groups and Downey and Kurtz (1986) answered the same questions for ordered abelian groups. In Chapter 6, we show that even for Archimedean f.o. groups, the existence of a strong divisible closure is equivalent to ACA_0.

Classifying the full orders on an orderable group can be an extremely difficult task. There is, however, a nice result classifying all possible order types for countable f.o. groups. In Chapter 7, we show this classification is equivalent to $\Pi^1_1 - CA_0$.

Chapter 8 is devoted to issues in computable mathematics. The first section returns to the connection between c.b. Π^0_1 classes and spaces of full orders on fully orderable computable groups. If G is a fully orderable computable group and $\mathbb{X}(G)$ is the space of full orders on G, then we have already mentioned that there is a Turing degree preserving bijection between some c.b. Π^0_1 class C and $\mathbb{X}(G)$. A question, asked in Downey and Kurtz (1986) and motivated by results in Metakides and Nerode (1979), is whether all c.b. Π^0_1 classes can be represented by computable torsion free abelian groups. That is, for an arbitrary c.b. Π^0_1 class C, is there a orderable computable abelian group G and a Turing degree preserving bijection from C to $\mathbb{X}(G)$. We show that the answer is no even if we weaken the notion of representation and restrict the class of c.b. Π^0_1 classes even further. We also extend the result to include computable torsion free nilpotent groups.

In the second section, we examine computable presentations of orderable computable abelian groups. Downey and Kurtz (1986) showed that there is an orderable computable abelian group with no computable order. However, their example is isomorphic to a computable group with a computable order. We show that this phenomena is true in general. Every orderable computable abelian group is classically isomorphic to a computably orderable computable group.

Chapter 2

Orders on Quotient Groups

2.1 Basic Definitions

This section lays out the basic definitions for partially and fully ordered groups. Fundamental notions such as convex subgroups, induced orders on quotient groups, and positive cones of partially ordered groups are defined. The main result is that RCA_0 suffices to prove the existence of the induced order on the quotient of an fully ordered group, but ACA_0 is required if the group is not known to be fully ordered. The notation and definitions below follow Kokorin and Kopytov (1974) and Fuchs (1963).

Definition 2.1. (RCA_0) A **group** is a set $G \subseteq \mathbb{N}$ together with a constant, 1_G (or sometimes 0_G), and an operation, $\cdot_G$, which obey the usual group axioms.

$$\forall a, b, c \in G\,(a \cdot_G (b \cdot_G c) = (a \cdot_G b) \cdot_G c)$$
$$\forall a \in G\,(1_G \cdot_G a = a \cdot_G 1_G = a)$$
$$\forall a \in G\,\exists a^{-1} \in G\,(a \cdot_G a^{-1} = a^{-1} \cdot_G a = 1_G).$$

Definition 2.2. (RCA_0) A **partial order** is a set X together with a binary relation $\leq_X$ which satisfies the following axioms.

$$\forall x \in X\,(x \leq_X x)$$
$$\forall x, y \in X\,(x \leq_X y \wedge y \leq_X x \rightarrow x = y)$$
$$\forall x, y, z \in X\,(x \leq_X y \wedge y \leq_X z \rightarrow x \leq_X z).$$

Definition 2.3. (RCA_0) A **partially ordered (p.o.) group** is a pair $(G, \leq_G)$ where G is a group, $\leq_G$ is a partial order on the set G, and for any $a, b, c \in G$, if $a \leq_G b$ then $a \cdot_G c \leq_G b \cdot_G c$ and $c \cdot_G a \leq_G c \cdot_G b$. If the order is a linear order, the pair $(G, \leq_G)$ is called a **fully ordered (f.o.) group**. A group for which there exists some full order is called an **O-group**

It should be clear from Definition 1.1 what the definitions of the corresponding computable objects are. For example, a computably partially ordered computable group G is a computable group G together with a computable binary relation $\leq_G$ on G such that $\leq_G$ satisfies the axioms for a partial order and the order is preserved under multiplication on both the left and the right. Except for cases when they are needed to avoid confusion, the subscripts on $\cdot_G$ and $\leq_G$ are dropped.

Example 2.4. The additive groups $(\mathbb{R}, +)$, $(\mathbb{Q}, +)$, and $(\mathbb{Z}, +)$ with the standard orders are all f.o. groups. Let $\mathbb{Q}^+$ and $\mathbb{R}^+$ be the strictly positive rational and real numbers. The multiplicative groups $(\mathbb{R}^+, \cdot)$ and $(\mathbb{Q}^+, \cdot)$ are f.o. groups under the standard orders.

Example 2.5. The most important example for our purposes is the free abelian group on ω generators. Let G be the free abelian group with generators $a_0, a_1, \ldots$. Elements of G have the form $\sum_{i\in I} r_i a_i$ where $I \subseteq \omega$ is a finite set, $r_i \in \mathbf{Z}$ and $r_i \neq 0$. To compare the element above with $\sum_{j\in J} q_j a_j$, let $K = I \cup J$. For each $k \in K$, define $r_k = 0$ if $k \in J \setminus I$ and $q_k = 0$ is $k \in I \setminus J$. Let k be the maximum element of K such that $r_k \neq q_k$. The order is given by: $\sum_{i\in I} r_i a_i \leq \sum_{j\in J} q_j a_j$ if and only if $r_k \leq q_k$. This order makes G into an f.o. group.

As expected, RCA_0 suffices to prove many basic facts about p.o. groups.

Lemma 2.6. *(RCA_0) If $(G, \leq)$ is a p.o. group and $a < b$, then for any $c \in G$, $ac < bc$ and $ca < cb$.*

Lemma 2.7. *(RCA_0) Let $(G, \leq)$ be a p.o. group.*

1. *If $a < b$ then $c^{-1}ac < c^{-1}bc$.*
2. *If $a < b$ then $b^{-1} < a^{-1}$.*
3. *If $a < b$ and $c < d$ then $ac < bd$.*

Defining a partial order can sometimes be notationally complicated. It is frequently easier to specify only the elements which are greater than the identity element. It turns out that specifying these positive elements uniquely determines the order.

Definition 2.8. (RCA_0) The **positive cone**, $P(G, \leq_G)$ of a p.o. group is the set of elements which are greater than or equal to the identity.

$$P(G, \leq_G) \;=\; \{\, g \in G \mid 1_G \leq_G g \,\}$$

Each element $x \in P(G, \leq_G)$ is called **positive**.

When the intended order $\leq_G$ is clear, $P(G)$ is used instead of $P(G, \leq_G)$. Because $P(G)$ has a Σ^0_0 definition, RCA_0 is strong enough to prove the existence of $P(G)$. Conversely, given the positive cone, $P(G)$, of some partial order on G, the relationship between any two elements can be calculated. Because $a \leq b$ if and only if $1_G \leq a^{-1}b$, determining if $a \leq b$ requires only knowing whether $a^{-1}b \in P(G)$. Thus, RCA_0 can recapture the order $\leq_G$ from $P(G)$. Notice that if G is a computable group, these conditions mean that $\deg(P(G)) = \deg(\leq_G)$ for any partial order $\leq_G$ and its associated positive cone.

Example 2.9. The complex numbers $(\mathbb{C}, +)$ with the order determined by

$$P(G) \;=\; \{\, x + yi \,|\, x > 0 \,\vee\, (\, x = 0 \wedge y \geq 0\,)\,\}$$

is an f.o. group. The group $(\mathbb{Q}^+, \cdot)$ with the order determined by $P(G) \;=\; \mathbb{N}^+$ is a p.o. group. Unraveling the definition of the positive cone show that if $a, b \in \mathbb{Q}^+$ then $a \leq b$ if and only if a divides b. This order is not a full order but does form a lattice.

There are algebraic conditions which determine if an arbitrary subset of a group is the positive cone for some full or partial order on that group.

Definition 2.10. (RCA_0) If G is a group and $X \subseteq G$, then

$$X^{-1} = \{\, g^{-1} \;|\; g \in X\,\}.$$

X is a **full subset of G** if $X \cup X^{-1} = G$ and X is a **pure subset of G** if $X \cap X^{-1} \subseteq \{1_G\}$.

Theorem 2.11. *(RCA_0) A subset P of a group G is the positive cone of some partial order on G if and only if P is a normal pure semigroup with identity. Furthermore, P is the positive cone of a full order if and only if in addition P is full.*

Proof. Any of the standard proofs of this theorem carry through in RCA_0. For the details, see Kokorin and Kopytov (1974) or Fuchs (1963). □

2.2 Quotient Groups

In the study of ordered groups, it is natural to ask which theorems of group theory hold for ordered groups and which theorems either fail completely or require extra conditions. For example, if H is a normal subgroup of G, then G/H inherits a group structure from G. However, if G is partially ordered, the normality of H is not strong enough for G to induce both a group structure and a partial order on G/H. H must also be convex for the partial order on G to induce a natural partial order on G/H. To formulate this statement in second order arithmetic, we first need a definition for the quotient group.

Let G be a group and H be a normal subgroup of G. As with computable groups in Chapter 1, unique representatives of each coset gH can be chosen by picking the $\leq_{\mathbb{N}}$–least element of gH. These choices can be made in RCA_0 because $mH = nH$ if and only if $m^{-1}n \in H$.

Definition 2.12. (RCA_0) If G is a group and H is a normal subgroup of G, then the **quotient group G/H** is defined by the set

$$\{\, n \;|\; n \in G \,\wedge\, \forall m < n\,(m \notin G \vee m^{-1} \cdot n \notin H)\,\}$$

and the operation

$$a \cdot_{G/H} b = c \;\leftrightarrow\; a, b, c \in G/H \;\wedge\; c^{-1} \cdot_G a \cdot_G b \in H.$$

Definition 2.13. (RCA_0) A subset X of a partial order Y is **convex** if

$$\forall a, b, x \in Y \big((a, b \in X \wedge a \leq x \leq b) \rightarrow x \in X \big).$$

A subgroup H of a p.o. group G is **convex** if it is convex as a subset of G.

Definition 2.14. Let $(G, \leq)$ be a p.o. group and H a convex normal subgroup. The **induced order**, $\leq_{G/H}$, on G/H is given by:

$$\{ \langle a, b \rangle \mid a, b \in G/H \wedge \exists h \in H (a \leq_G bh) \}.$$

That is, $a \leq_{G/H} b$ if and only if $\exists h \in H(a \leq_G bh)$

There are two useful variants of this definition, both of which are seen to be equivalent by unraveling the definitions. The first is to define $a \leq_{G/H} b$ if and only if $\exists h \in H$ $(a^{-1}bh \in P(G))$. The second is to define $P(G/H)$ as the image of $P(G)$ under the canonical map $G \rightarrow G/H$. This definition amounts to setting:

$$P(G/H) = \{ g \in G/H \mid \exists h \in H \, (gh \in P(G)) \}.$$

As above, the subscript G/H will be dropped as long as it is clear whether a and b are being compared as elements of G or G/H. When confusion may arise, we will denote elements of G/H by aH and bH.

From the viewpoint of reverse mathematics, there are two questions to ask concerning this definition. Which set existence axioms are required to form the induced order on G/H, and if orders on G/H and H are given, how hard is it to put them together to give an order on G that makes H convex and gives G/H the appropriate induced order? The answer to the first question points out an example in which having a full order on G gives extra computational power. The condition in Definition 2.14 is Σ^0_1, so Σ^0_1 comprehension suffices to define the induced order. In the next section, we will show that this is the best that can be done for p.o. groups. However, if the order is known to be total, then we can do better.

Theorem 2.15. *(RCA_0) Let $(G, \leq)$ be an f.o. group and H a convex normal subgroup. The induced order on G/H exists.*

Proof. Let $a, b \in G/H$ and $a \neq b$. Because a and b are representatives of different cosets, $ab^{-1} \notin H$.

Claim. $\exists h \in H \, (a \leq bh)$ if and only if $a \leq b$.

If $a \leq b$ then, because $1_G \in H$, it follows that $\exists h \in H \, (a \leq bh)$. For the other direction, suppose $\exists h \in H(a \leq bh)$ and $b < a$. Then $b < a \leq bh$ and so $1_G < b^{-1}a \leq h$. Since H is convex, $b^{-1}a \in H$ which gives a contradiction. The induced order can now be given by a Σ^0_0 condition: $aH \leq bH$ if and only if $aH = bH$ or $a < b$. □

Corollary 2.16. *If $(G, \leq_G)$ is a computably fully ordered computable group and H is a computable convex normal subgroup, then the induced order on G/H is computable.*

It is also worth noting that for a f.o. group, if $aH < bH$ then $\forall h \in H(ah < b)$. Indeed, if not, then $ah \geq b$ for some $h \in H$ and hence $bH \leq aH$. This fact is not true for general p.o. groups since it is possible that for some h, the elements a and bh are not comparable. The following example illustrates this point.

Example 2.17. Consider $(\mathbb{Q}^+, \cdot)$ with $P(\mathbb{Q}^+) = \mathbb{N}^+$. Under this partial order, $a \leq b$ if and only if a divides b. Let H be the subgroup generated by 2. Elements of H are of the form 2^n for some $n \in \mathbb{Z}$. The group is abelian, so H is normal. H is convex since if $2^n \leq x \leq 2^m$ then x must be of the form 2^p for some $n \leq p \leq m$. Let 3 represent the coset $\{ \ldots, 12, 6, 3, 3/2, 3/4, \ldots \}$ in $\mathbb{Q}^+/H$ and 9 represent the coset $\{ \ldots, 36, 18, 9, 9/2, 9/4, \ldots \}$. Since $3 \leq 9$ in this group and $1 \in H$, it is clear that $\exists h \in H(3 \leq 9h)$. However, $3 \not\leq 9/2$ and so it is not the case that $\forall h \in H(3 \leq 9h)$.

To answer the question about putting orders on G/H and H together, one additional condition is required. An order on H is not necessarily preserved under conjugation by arbitrary elements of G. However, any order on G must have this property. Thus for an order on H to extend to all of G, it must be that $a \leq_H b$ implies $gag^{-1} \leq_H gbg^{-1}$ for all $g \in G$. This condition turns out to be sufficient.

Definition 2.18. (RCA_0) Let H be a normal subgroup of G and $\leq$ a full order on H. $(H, \leq)$ is **fully G − ordered** if for any $a, b \in H$ and $g \in G$, $a \leq b$ implies $gag^{-1} \leq gbg^{-1}$.

Theorem 2.19. *(RCA_0) Let $(H, \leq_H)$ be a fully G-ordered normal subgroup and $(G/H, \leq_{G/H})$ an f.o. group. G admits a full order under which the induced orders on H and G/H correspond to those given and H is convex.*

Proof. Given $a, b \in G$, define $a \leq_G b$ if and only if either $aH \leq_{G/H} bH$ or $aH = bH$ and $a^{-1}b \in P(H)$. Verifying that this definition gives a full order on G is a straight forward matter of checking the axioms for a variety of cases. Notice that if $a, b \in H$ then $aH = bH$ and so they are compared in G using the order on H. Thus the restriction of $\leq_G$ to H is $\leq_H$. To show H is convex under this order, suppose that $a, b \in H$, $c \notin H$ and $a \leq_G c \leq_G b$. Then $aH \neq cH$, so $a \leq_G c$ implies $aH <_{G/H} cH$. Similarly, $cH <_{G/H} bH$ and so $aH <_{G/H} bH$ which is a contradiction. To show that the induced order on the quotient is $\leq_{G/H}$, suppose that $a, b \in G$ and $a \leq_G bh$ for some $h \in H$. Either $aH <_{G/H} bhH$ or $aH = bhH$ and $a^{-1}bh \in P(G)$. In either case $aH \leq_{G/H} bH$. Assuming $aH \leq_{G/H} bH$, either $aH <_{G/H} bH$, and hence $a < b$, or $aH = bH$ and $\exists h \in H(a = bh)$. In either case, $\exists h \in H(a \leq_G b)$. Thus the induced order on G/H is correct. □

2.3 Induced Orders

The goal of this section is to show that ACA_0 is equivalent to the existence of the induced order on the quotient of a p.o. group. By Theorem 1.16, ACA_0 is equivalent to the existent of the range of one-to-one functions. Given a one-to-one function, the strategy is to code the range into a group in such a way that it can be recovered from the order on the quotient group. The torsion free abelian group A on generators a_i, b_i for $i \in \mathbb{N}$ is used to do the coding. The first step is to present this group formally.

The elements of A are quadruples of finite sets (I, q, J, p) where I and J are finite subsets of $\mathbb{N}$ and p and q represent the functions

$$q : I \to \mathbb{Z} \setminus \{0\}$$
$$p : J \to \mathbb{Z} \setminus \{0\}.$$

The element represented by (I, q, J, p) is denoted

$$\sum_{i \in I} q_i a_i \ + \ \sum_{j \in J} p_j b_j.$$

The elements represented by (I, q, J, p) and (I', q', J', p') are equal if and only if $I = I'$, $J = J'$, $q = q'$ and $p = p'$. The sum

$$\Big(\sum_{i \in I} q_i a_i \ + \ \sum_{j \in J} p_j b_j \Big) \ + \ \Big(\sum_{k \in K} r_k a_k \ + \ \sum_{l \in L} s_l b_l \Big)$$

is defined to be

$$\sum_{m \in M} t_m a_m \ + \ \sum_{n \in N} u_n b_n$$

where

$$M = (I \cup K) \ \setminus \ \{x \in I \cap K \,|\, q_x + r_x = 0\}$$
$$N = (J \cup L) \ \setminus \ \{x \in J \cap L \,|\, p_x + s_x = 0\}$$

and t_m is defined to be q_m if $m \in I \setminus K$, r_m if $m \in K \setminus I$ and $q_m + r_m$ if $m \in I \cap K$. u_n is defined similarly. The identity element, 0_A, is the element represented by $(\emptyset, \emptyset, \emptyset, \emptyset)$ and if g is represented by (I, q, J, p), then g^{-1} is the sum

$$\sum_{i \in I} -q_i a_i \ + \ \sum_{j \in J} -p_j b_j.$$

Theorem 2.20. *(RCA_0) The following are equivalent:*

1. *ACA_0*
2. *For every p.o. group $(G, \leq_G)$ and every convex normal subgroup H, the induced order $\leq_{G/H}$ on G/H exists.*

Proof.

Case. (1) $\Rightarrow$ (2) :

For $x, y \in G/H$, use Σ^0_1 comprehension in ACA_0 to define the relation:

$$x \leq_{G/H} y \ \leftrightarrow \ \exists h \in H \ (x \leq_G yh).$$

Case. (2) $\Rightarrow$ (1) :

Let $f : \mathbb{N} \to \mathbb{N}$ be a one-to-one function. By Theorem 1.16, it suffices to show that the range of f exists. Use Σ^0_0 comprehension to define the partial order $\leq_A$ by:

$$P(A) \ = \ \left\{ \sum_{i \in I} q_i a_i \ + \ \sum_{j \in J} p_j b_j \ \middle| \ J = \emptyset \wedge \forall i \in I(q_i > 0) \right\}.$$

The idea here is that $P(A)$ is the semigroup generated by the elements a_i for $i \in \mathbb{N}$. The definition is Σ^0_0 because $\forall i \in I$ is a bounded quantifier.

Claim. $P(A)$ is the positive cone for a partial order on A.

It suffices to show that $P(A)$ is a pure normal semigroup with identity. By definition, $0_A \in P(A)$. $P(A)$ is normal because it is a subset of an abelian group. $P(A)$ is a semigroup since it is closed under componentwise addition. Finally, since $P^{-1}(A)$ is defined by

$$P^{-1}(A) \ = \ \left\{ \sum_{i \in I} q_i a_i \ + \ \sum_{j \in J} p_j b_j \ \middle| \ J = \emptyset \wedge \forall i \in I(q_i < 0) \right\},$$

it is clear that $P(A)$ is pure.

Let H be the subgroup generated by elements of the form $-a_n + b_m$ where $f(n) = m$. Formally, $\sum_{i \in I} q_i a_i \ + \ \sum_{j \in J} p_j b_j$ is in H if and only if either $I = J = \emptyset$ or $I \neq \emptyset$ and

$$\forall i \in I(f(i) \in J \wedge q_i = -p_{f(i)}) \ \wedge \ \forall j \in J \ \exists i \in I(f(i) = j \wedge q_i = -p_j).$$

This condition is Σ^0_0 since all the quantification is bounded. H is normal because the group is abelian.

Claim. H is convex.

To prove this claim, it suffices to show that there are no nontrivial intervals in H. That is, for any $c, d \in H$, $c \leq d$ implies $c = d$. Notice that any $c, d \in H$ can be expressed as

$$c = \sum_{i \in I} -q_i a_i \ + \ \sum_{i \in I} q_i b_{f(i)} \qquad d = \sum_{j \in J} -p_j a_j \ + \ \sum_{j \in J} p_j b_{f(j)}.$$

If $c \leq d$, then $-c + d \in P(A)$. Since $P(A)$ is generated by the a_i's, the b_i part of the sums must cancel out. Hence

$$\sum_{i \in I} -q_i b_{f(i)} \ + \ \sum_{j \in J} p_j b_{f(j)} \ = \ 0.$$

Since 0 is represented by the quadruple $(\emptyset, \emptyset, \emptyset, \emptyset)$, we have $I = J$ and $q = p$. Hence $c = d$ as required.

Now that A, $P(A)$, and H are defined, all that remains to show is how the range of f can be defined from the induced order $\leq_{A/H}$ on A/H. This definition follows from the final two claims.

Claim. The existence of $\leq_{A/H}$ implies the existence of the set $P(A) + H$.

Given $x \in A$, we need to decide if $x \in P(A)+H$. Let $n \in G/H$ be such that $n+H = x+H$. Since x and n differ by a element of H, $x \in P(A) + H$ if and only if $n \in P(A) + H$. However,

$$\begin{aligned} 0_{A/H} \leq_{A/H} n \;&\leftrightarrow\; \exists h \in H\ (n + h \in P(A)) \\ &\leftrightarrow\; n \in P(A) + H. \end{aligned}$$

Thus, the set $P(A) + H$ is definable from $\leq_{A/H}$ in RCA_0.

Claim. $b_m \in P(A) + H \;\leftrightarrow\; m \in range(f)$

First assume that $b_m = p + h$ for some $p \in P(A)$ and $h \in H$. Then b_m can be written as:

$$b_m \;=\; \sum_{i\in I} q_i a_i \;+\; \left(\sum_{j\in J} -p_j a_j \;+\; \sum_{j\in J} p_j b_{f(j)}\right).$$

The parts of the equation with a_i's must cancel out, leaving $I = J$. Furthermore, because only b_m appears on the left of the equation, $J = \{n\}$ where $f(n) = m$ and $p_n = 1$. Hence m is in the range of f.

For the other direction, assume that m is in the range of f. For some n, $f(n) = m$, and hence $-a_n + b_m \in H$ and $a_n \in P(A)$. Adding these equations shows that $b_m \in P(A)+H$. □

Corollary 2.21. *There is a computably partially ordered computable group $(G, \leq_G)$ and a computable convex normal subgroup H such that the degree of the induced order on G/H is $0'$.*

Proof. Let f be a computable one-to-one function that enumerates $0'$. Since f is computable, the p.o. group in the proof of Theorem 2.20 is a computably partially ordered computable group. The range of f is computable from the induced order on G/H, so $\deg(\leq_{G/H}) = 0'$. □

Chapter 3

Group Conditions

Now that we have the basic definitions for ordered groups, we would like to know which groups can be ordered. Notice that any group can be partially ordered: take the trivial partial order under which no two distinct elements are comparable. The question of when a group admits a full order is more complicated. Being torsion free is a necessary condition, but unfortunately not a sufficient one. Let G be the group presented by the letters a and b with the relation $aba^{-1} = b^{-1}$. G is torsion free but not orderable. Indeed, if $b > 1_G$ then $aba^{-1} = b^{-1}$ forces $b^{-1} > 1_G$ and if $b < 1_G$ then $aba^{-1} = b^{-1}$ forces $b^{-1} < 1_G$. In Sections 3.1 and 3.2, three stronger conditions are presented that suffice to guarantee full orderability. In Section 3.3, we show that the existence of the center of a group is equivalent to ACA_0.

If G is an O-group, it is natural to study the space of all full orders on G. In Section 3.4, we present one connection between spaces of orders and c.b. Π^0_1 classes. We will return to this theme in the last chapter once we have more tools from ordered group theory.

3.1 Torsion Free Abelian and Nilpotent Groups

Being torsion free and abelian is the simplest group condition that implies full orderability. A proof of this fact can be found in Fuchs (1963) or Kokorin and Kopytov (1974).

Theorem 3.1. *Every torsion free abelian group is an O-group.*

The effective content of Theorem 3.1 was first explored in Downey and Kurtz (1986). They constructed a computable group isomorphic to $\bigoplus_\omega \mathbb{Z}$ which has no computable full order.

Theorem 3.2 (Downey and Kurtz (1986)). *There is a computable torsion free abelian group with no computable full order.*

Hatzikiriakou and Simpson (1990) used a similar proof in the context of reverse mathematics to show that Theorem 3.1 is equivalent to WKL_0. By the Low Basis Theorem, this fact implies that every computable torsion free abelian group must have a full order of low degree.

Theorem 3.3 (Hatzikiriakou and Simpson (1990)). *(RCA_0) The following are equivalent:*

1. *WKL_0*
2. *Every torsion free abelian group is an O-group.*

Theorem 3.1 is generalized in Kokorin and Kopytov (1974) to torsion free nilpotent groups.

Theorem 3.4. *Every torsion free nilpotent group is an O-group.*

The goal of this section is to use arguments similar to those in Hatzikiriakou and Simpson (1990), to show that Theorem 3.4 is equivalent to WKL_0. Notice that as long as RCA_0 suffices to prove that every abelian group is nilpotent, Theorem 3.3 already shows that Theorem 3.4 implies WKL_0. To state the result precisely, we need a formal definition of nilpotent groups in second order arithmetic.

In keeping with standard mathematical notation, if H is a normal subgroup of G, we will let $\pi : G \to G/H$ denote the projection function. That is, π picks out the $<_{\mathbb{N}}$-least representative of gH. Frequently, we will write gH instead of $\pi(g)$.

Definition 3.5. The **center** of G, $C(G)$, is the set

$$\{ g \in G \mid \forall x \in G\, (gx = xg) \}.$$

In general, the existence of the center is equivalent to ACA_0, as we shall see in Section 3.3. However if $C(G)$ is given, several properties of it can be proved in RCA_0.

Lemma 3.6. *(RCA_0) If $C(G)$ exists then $C(G)$ is a normal subgroup of G.*

Lemma 3.7. *(RCA_0) If H is a normal subgroup of G, $\pi : G \to G/H$ and $C(G/H)$ exists, then*

$$K = \{g \in G \mid \pi(g) \in C(G/H)\} = \pi^{-1}(C(G/H))$$

is a normal subgroup of G.

Proof. It is straight forward to check that K is a subgroup. To show that K is normal, let $k \in K$ and $g \in G$. Because $\pi(k) \in C(G/H)$, it follows that k commutes modulo H with all elements of G. In particular, $g^{-1}kH = kg^{-1}H$ or in the notation of π, $\pi(g^{-1}k) = \pi(kg^{-1})$. From here it follows that $\pi(k) = \pi(gkg^{-1})$. Thus $\pi(gkg^{-1}) \in C(G/H)$ and $gkg^{-1} \in K$. □

Definition 3.8. Let G be a group. The **upper central series** of G is the series of subgroups

$$\zeta_0 G \leq \zeta_1 G \leq \zeta_2 G \leq \cdots$$

defined by

$$\zeta_0 G = \langle 1_G \rangle$$
$$\zeta_1 G = C(G)$$
$$\zeta_{i+1} G = \pi^{-1}\big(C(G/\zeta_i G)\big)$$

where $\pi : G \to G/\zeta_i G$. G is **nilpotent** if $\zeta_n G = G$ for some $n \in \omega$.

Notice that $\zeta_{i+1}G/\zeta_i G = C(G/\zeta_i G)$. In order to use nilpotent groups in reverse mathematics, we need to define a code for them that explicitly gives the information contained in the upper central series.

Definition 3.9. The i^{th} column of a set X is denote by X_i and is defined by:

$$X_i = \{ n \mid \langle n, i \rangle \in X \}.$$

Definition 3.10. (RCA_0) The pair $N \subseteq \mathbb{N}$ and $n \in \mathbb{N}$ is a **code for a nilpotent group** G if the first $n+1$ columns of N satisfy

1. $N_0 = \langle 1_G \rangle$
2. $N_1 = C(G)$
3. $N_n = G$
4. For $0 \leq i \leq n$, N_i is a normal subgroup of G.
5. For $0 \leq i < n$, if $\pi : G \to G/N_i$, then $N_{i+1} = \pi^{-1}(C(G/N_i))$.

A group G is **nilpotent** is there is such a code (N, n) for G.

Lemma 3.11. *(RCA_0) Every abelian group is nilpotent.*

Proof. If G is abelian then we can define a code for G as a nilpotent group by setting $n = 1$ and $N \subseteq \mathbb{N}$ with $N_0 = \langle 1_G \rangle$ and $N_1 = G$. □

Lemma 3.12. *(RCA_0) If (N, n) is the code for a nilpotent group G then for all $0 \leq i < n$, N_{i+1}/N_i is abelian.*

Proof. By definition, $N_{i+1} = \pi^{-1}(C(G/N_i))$ with $\pi : G \to G/N_i$. Therefore, $N_{i+1}/N_i \cong C(G/N_i)$. □

Theorem 3.13. *(RCA_0) The following are equivalent.*

1. *WKL_0*
2. *Every torsion free nilpotent group is an O-group.*

The goal of the rest of this section is to prove this theorem. The idea is that a nilpotent group is formed from a finite number of abelian quotients N_{i+1}/N_i. If these quotients are torsion free then each is fully orderable by Theorem 3.3 and so we only need to put these orders together in a nice way. The first step is to show that that if G is a torsion free nilpotent group then each N_{i+1}/N_i is also torsion free. Notice that if (N, n) is the code for a torsion free nilpotent group G and $n \geq 1$, then N_1 must also be torsion free since it is a subgroup of G.

Definition 3.14. The **commutator** of x and y, denoted $[x, y]$, is the element $x^{-1}y^{-1}xy$.

Lemma 3.15. *(RCA_0) Let (N, n) be a code for a nilpotent group G. If $0 \leq i < n$ and $x \in N_{i+1}$, then $[x, g] \in N_i$ for all g.*

Proof. Notice that for $i = 0$, the lemma follows trivially because N_1 is the center of G. Assume $i \geq 1$. By definition, $x \in N_{i+1}$ means $xgN_i = gxN_i$ for all g. For any particular g, there is a $c \in N_i$ such that $xg = gxc$ and hence also $cg^{-1}x^{-1} = x^{-1}g^{-1}$. Let h be any element of G.

$$\begin{aligned} [x, g] \cdot h &= x^{-1}g^{-1}xg \cdot h \\ &= x^{-1}g^{-1}gxch \\ &= ch \end{aligned}$$

Since $c \in N_i$, we know that $ch = hc\tilde{c}$ for some $\tilde{c} \in N_{i-1}$. We now have:

$$\begin{aligned} ch &= hc\tilde{c} \\ &= hcg^{-1}x^{-1}xg\tilde{c} \\ &= hx^{-1}g^{-1}xg\tilde{c}. \end{aligned}$$

Thus, we have $[x, g] \cdot h = h \cdot [x, g] \cdot \tilde{c}$ for some $\tilde{c} \in N_{i-1}$. Another way to write this equality is

$$[x, g] \cdot hN_{i-1} = h \cdot [x, g]N_{i-1}.$$

This equality means that $[x, g]N_{i-1}$ is in the center of G/N_{i-1} and hence that $[x, g] \in N_i$. $\square$

Lemma 3.16. *(RCA_0) Let (N, n) be a code for a nilpotent group G. If $1 \leq i < n$ and $x \in N_{i+1}$, then for all $m > 0$*

$$[x, g]^m N_{i-1} = [x^m, g]N_{i-1}.$$

Proof. Because $[x, g]^m N_{i-1} = [x^m, g]N_{i-1}$ is a Σ^0_0 statement, we can prove this lemma in RCA_0 by induction on m. The case for $m = 1$ is trivial, so assume the equality holds for m and we prove it for $m + 1$. Since $[x, g]^{m+1} = [x, g]^m \cdot [x, g]$, we can apply the induction hypothesis in the form $[x, g]^m = [x^m, g] \cdot c$ for some $c \in N_{i-1}$. We now have:

$$\begin{aligned} [x, g]^{m+1} &= [x^m, g] \cdot c \cdot [x, g] \\ &= x^{-m}g^{-1}x^m gc \cdot [x, g]. \end{aligned}$$

By Lemma 3.15, $x \in N_{i+1}$ implies $[x, g] \in N_i$ and so $[x, g]$ commutes with elements of G modulo N_{i-1}. Therefore, for some $\tilde{c} \in N_{i-1}$ we have

$$\begin{aligned} x^{-m} \cdot g^{-1}x^m gc \cdot [x, g] &= x^{-m} \cdot [x, g] \cdot g^{-1}x^m gc\tilde{c} \\ &= x^{-m-1}g^{-1}xgg^{-1}x^m gc\tilde{c} \\ &= [x^{m+1}, g] \cdot c\tilde{c}. \end{aligned}$$

Because $c\tilde{c} \in N_{i-1}$, this calculation establishes the induction case. $\square$

Lemma 3.17 (Mal'cev). *(RCA_0) Let (N, n) be a code for a torsion free nilpotent group G. For every $0 \leq i < n$, N_{i+1}/N_i is torsion free.*

Proof. We prove this theorem by bounded induction on i. Because $N_0 = \langle 1_G \rangle$ we have $N_1/N_0 = N_1$, which establishes the theorem for $i = 0$. Assume $i \geq 1$ and the theorem holds for $i - 1$. The induction hypothesis tells us that N_i/N_{i-1} is torsion free. Let $x \in N_{i+1}$ and suppose that $x^m \in N_i$ for some $m > 0$. We need to show that $x \in N_i$. By Lemma 3.16, $[x, g]^m N_{i-1} = [x^m, g]N_{i-1}$ for any g. By Lemma 3.15, $x^m \in N_i$ implies that $[x^m, g] \in N_{i-1}$. Therefore, $[x, g]^m \in N_{i-1}$. Applying Lemma 3.15 to $x \in N_{i+1}$ tells us that $[x, g] \in N_i$. Putting these facts together, we have:

$$[x, g]N_{i-1} \in N_i/N_{i-1}$$
$$[x, g]^m N_{i-1} = 1_G N_{i-1}.$$

Since N_i/N_{i-1} is torsion free, it must be that $[x, g] \in N_{i-1}$. However, this fact implies that $xgN_{i-1} = gxN_{i-1}$ for all g and so $x \in N_i$ as required. □

Lemma 3.18. *(WKL_0) Let (N, n) be a code for a torsion free nilpotent group. For every $0 \leq i < n$, N_{i+1}/N_i is a fully G/N_i-orderable group.*

Proof. We need to show that there is a full order on N_{i+1}/N_i such that for all $a, b \in N_{i+1}/N_i$ and $g \in G/N_i$, if $aN_i < bN_i$ then $gag^{-1}N_i < gbg^{-1}N_i$. By Lemmas 3.12 and 3.17, N_{i+1}/N_i is a torsion free abelian group and hence by Theorem 3.3, WKL_0 proves that it is fully orderable.

Let $\leq$ be any full order on N_{i+1}/N_i, let $a < b$ be elements of N_{i+1}/N_i and let $g \in G/N_i$. Since $N_{i+1}/N_i \cong C(G/N_i)$, we have $gag^{-1}N_i = aN_i$ and $gbg^{-1}N_i = bN_i$. Hence, $aN_i < bN_i$ implies $gag^{-1}N_i < gbg^{-1}N_i$. □

We are now ready to prove Theorem 3.13

Proof.

Case. (2) ⇒ (1)

Assume every torsion free nilpotent group is an O-group. By Lemma 3.11, this assumption implies that every torsion free abelian group is an O-group. From here, Theorem 3.3 implies (1).

Case. (1) ⇒ (2)

For each $1 \leq i \leq n$, let $\bar{P}_i$ be the strict positive cone of a full G/N_{i-1}-order on N_i/N_{i-1}. Define P_i and P by:

$$P_i = \{x \in N_i \mid xN_{i-1} \in \bar{P}_i\}$$
$$P = (\cup_{i=1}^n P_i) \ \cup \ \{1_G\}.$$

We prove that P is the positive cone for a full order on G in the following series of claims.

Claim. P is a semigroup with identity.

It suffices to show P is closed under multiplication. Let $x, y \in P$ with $x, y \neq 1_G$. There are i, j such that $x \in P_i$ and $y \in P_j$. If $i = j$ then $xN_{i-1}, yN_{i-1} \in \bar{P}_i$ and so $xyN_{i-1} \in \bar{P}_i$ and $xy \in P_i$. If $i \neq j$ then, without loss of generality, assume that $i < j$. Since $x \in P_i$, it follows that $x \in N_i$ and hence $x \in N_{j-1}$. But then, $xyN_{j-1} = yN_{j-1}$ and so $xy \in P_j$.

Claim. P is normal.

Let $x \in P$, $x \neq 1_G$ and $g \in G$. There is an i such that $x \in P_i$. Since $\bar{P}_i$ is the strict positive cone of a full G/N_{i-1}–order on N_i/N_{i-1}, we have that $xN_{i-1} \in \bar{P}_i$ implies that $gxg^{-1}N_{i-1} \in \bar{P}_i$. Hence $gxg^{-1} \in P_i$.

Claim. P is pure.

Let $x \in P$ and $x \neq 1_G$. We need to show that $x^{-1} \notin P$. There is an i such that $x \in P_i$. Because $\bar{P}_i$ is the strict positive cone on N_i/N_{i-1}, we know that $x \in N_i$, $x \notin N_{i-1}$. Hence $x^{-1} \in N_i$ and $x^{-1} \notin N_{i-1}$. However, because $xN_{i-1} \in \bar{P}_i$, it follows that $x^{-1}N_{i-1} \notin \bar{P}_i$ and so $x^{-1} \notin P_i$. To show $x^{-1} \notin P_j$ for $j > i$, notice that since $x^{-1} \in N_i$, we also have $x^{-1} \in N_{j-1}$. Therefore $x^{-1}N_{j-1} = 1_G N_{j-1}$ and hence $x^{-1} \notin P_j$. Finally, assume for a contradiction that $j < i$ and $x^{-1} \in P_j$. It follows that $x^{-1} \in N_{i-1}$. However, above we showed that $x^{-1} \notin N_{i-1}$. Thus, $x^{-1} \notin P_j$ for any j.

Claim. P is full.

Let $x \in P$ and $x \neq 1_G$. We need to show that either $x \in P$ or $x^{-1} \in P$. There is an i such that $x \in N_i$ and $x \notin N_{i-1}$. Since $\bar{P}_i$ is a full order on N_i/N_{i-1}, either $xN_{i-1} \in \bar{P}_i$ or $x^{-1}N_{i-1} \in \bar{P}_i$. Thus, either $x \in P_i$ or $x^{-1} \in P_i$. □

3.2 Direct Products

Groups are frequently constructed by means of a direct product. These constructions preserve full orderability. A proof of the following theorem can be found in either Fuchs (1963) or Kokorin and Kopytov (1974).

Theorem 3.19. *Any direct product of O-groups is an O-group.*

To examine this theorem in reverse mathematics, we need to distinguish between finite and restricted countable direct products. The finite direct product $A_0 \times A_1 \times \ldots \times A_{n-1}$ consists of sequences of length n such that the i^{th} element of each sequence is in A_i. Multiplication is componentwise. The elements of the restricted direct product of A_i for $i \in \mathbb{N}$ are finite sequences σ such that for all $i < \text{lh}(\sigma)$, $\sigma(i) \in A_i$. The idea is that the element represented by σ has 1_{A_j} as its j^{th} component for all $j \geq \text{lh}(\sigma)$. In order to make each sequence represent a distinct element, we add the requirement that the last element in the sequence not be an identity element. The formal definitions are given below.

Definition 3.20. (RCA_0) If $n \in \mathbb{N}$ and for all $i < n$, A_i is a group, then the **finite direct product** $G = \prod_{i=0}^{n-1} A_i$ is defined by:

$$G = \{\sigma \in \mathrm{Fin}_{\mathbb{N}} \mid \mathrm{lh}(\sigma) = n \wedge \forall i < n\,(\sigma(i) \in A_i)\}$$
$$1_G = \langle 1_{A_0}, 1_{A_1}, \dots, 1_{A_{n-1}} \rangle$$
$$\sigma \cdot_G \tau = \langle \sigma(0) \cdot_{A_0} \tau(0), \dots, \sigma(n-1) \cdot_{A_{n-1}} \tau(n-1) \rangle.$$

Theorem 3.21. *(RCA_0) If $n \in \mathbb{N}$ and for all $i < n$, A_i is an O–group, then $G = \prod_{i=0}^{n-1} A_i$ is an O–group.*

Proof. Let $P^+(A_i)$ be the strict positive cone of a full order on A_i. Order G lexicographically:

$$P^+(G) = \{\sigma \in G \mid \exists i < n\ (\sigma(i) \in P^+(A_i) \wedge \forall j < i(\sigma(j) = 1_{A_j}))\}$$
$$P(G) = P^+(G) \cup \{\ \langle 1_{A_0}, \dots, 1_{A_{n-1}} \rangle\ \}.$$

From this definition, $P(G)$ is clearly full, pure, and contains the identity. It remains to check that it is a normal semigroup. Since $P(G)$ is closed under multiplication, it is a semigroup. To see that it is normal, let $\sigma \in P(G)$ have its first non-identity element at $\sigma(i)$. If $\tau = \langle g_0, \dots, g_{n-1} \rangle \in G$ then $\tau\sigma\tau^{-1}$ is

$$\langle g_0, \dots, g_{n-1} \rangle \cdot_G \langle 1_{A_0}, \dots, 1_{A_{i-1}}, a_i, \dots, a_{n-1} \rangle \cdot_G \langle g_0^{-1}, \dots, g_{n-1}^{-1} \rangle.$$

The first non-identity element in this product is $g_i a_i g_i^{-1}$. Because $a_i \in P^+(A_i)$, we have $g_i a_i g_i^{-1} \in P^+(A_i)$ and hence $\tau\sigma\tau^{-1} \in P^+(G)$. □

Definition 3.22. (RCA_0) Let A be a set such that for each i, the i^{th} column A_i is a group. The **restricted direct product** $G = \prod_{n \in \mathbb{N}} A_n$ is defined by:

$$G = \{\sigma \in \mathrm{Fin}_{\mathbb{N}} \mid \forall i < \mathrm{lh}(\sigma)\ (\sigma(i) \in A_i) \wedge \sigma(\mathrm{lh}(\sigma) - 1) \neq 1_{A_{\mathrm{lh}(\sigma)-1}}\}$$
$$1_G = \langle\rangle$$

where $\langle\rangle$ is the empty sequence. Multiplication is componentwise, removing any trailing identity elements.

Theorem 3.23. *(RCA_0) The following are equivalent:*

1. *WKL_0*
2. *If $\forall i$ (A_i is an O-group) then $G = \prod_{i \in \mathbb{N}} A_i$ is an O-group.*

Proof.

Case. (1) $\Rightarrow$ (2):
We know $\forall i \, \exists Y$ (Y is a positive cone on A_i). From the Theorem 3.21, if $n \in \mathbb{N}$ then

$$RCA_0 \vdash \exists Y (Y \text{ is positive cone on } \prod_{i=0}^{n-1} A_i).$$

A uniform (strict) order on the $A_i's$ is a set P such that P_i is the (strict) positive cone of a full order on A_i. To prove that G is an O-group, it suffices to prove the existence of a uniform order on the A_i. From a uniform order, we can define the lexicographic order on G as in Theorem 3.21. To show the existence of a uniform order, we build a tree T such that any path on the tree codes such an order. T is built in stages such that at the end of stage s, all nodes of length s are defined. Each node on T keeps a guess at an approximation to a uniform strict order. Suppose σ is a node on T at level s, $s+1 = \langle e, i \rangle$, $e \neq 1_{A_i}$, and P_σ is σ's approximation. At stage $s+1$ we check if $1_{A_j} \in P_\sigma$ for any j. Since P_σ is a finite set, this can be done computably. If $1_{A_j} \in P_\sigma$, then P_σ cannot be a subset of a uniform strict order, so we terminate this branch. Otherwise, we define two extensions of P_σ: one by adding $e \in A_i$ to P_σ and the other by adding $e^{-1} \in A_i$ to P_σ. These sets are each closed under one step multiplication and conjugation by elements less than s. One extension becomes $P_{\sigma^\frown 0}$ and the other becomes $P_{\sigma^\frown 1}$. This construction is presented formally below. T_s will be the set of nodes of T of length s.

Construction

Stage 0: Set $T = \{\langle\rangle\}$ and $P_{\langle\rangle} = \emptyset$.

Stage $\mathbf{s+1}$: Assume $s = \langle e, i \rangle$. For each $\sigma \in T_s$ do the following:

1. Check if 1_{A_j} appears in P_σ for any j. If so, σ has no extensions on T, so move on to the next node in T_s. If not, add $\sigma^\frown 0$ and $\sigma^\frown 1$ to T_{s+1} and move on to step 2.

2. If $e = 1_{A_i}$ or e does not represent an element of A_i, then set $P_{\sigma^\frown 0} = P_{\sigma^\frown 1} = P_\sigma$ and move on to the next node in T_s.

3. If $e \in A_i$ and $e \neq 1_{A_i}$ define

$$\tilde{P}_{\sigma^\frown 0} = P_\sigma \cup \{\langle e^{-1}, i \rangle\}$$
$$\tilde{P}_{\sigma^\frown 1} = P_\sigma \cup \{\langle e, i \rangle\}$$

   Extend these by:

$$\begin{aligned}
\langle k, j \rangle \in P_{\sigma^\frown 0} \quad \leftrightarrow \quad & \langle k, j \rangle \in \tilde{P}_{\sigma^\frown 0} \ \vee \\
& \exists \langle m, j \rangle, \langle n, j \rangle \in \tilde{P}_{\sigma^\frown 0} \ (m \cdot_{A_j} n = k) \ \vee \\
& \exists n \leq s \ \exists \langle m, j \rangle \in \tilde{P}_{\sigma^\frown 0} \ (n \in A_j \wedge n \cdot_{A_j} m \cdot_{A_j} n^{-1} = k) \\
\langle k, j \rangle \in P_{\sigma^\frown 1} \quad \leftrightarrow \quad & \langle k, j \rangle \in \tilde{P}_{\sigma^\frown 1} \ \vee \\
& \exists \langle m, j \rangle, \langle n, j \rangle \in \tilde{P}_{\sigma^\frown 1} \ (m \cdot_{A_j} n = k) \ \vee \\
& \exists n \leq s \ \exists \langle m, j \rangle \in \tilde{P}_{\sigma^\frown 1} \ (n \in A_j \wedge n \cdot_{A_j} m \cdot_{A_j} n^{-1} = k).
\end{aligned}$$

End of Construction

Claim. T is infinite.

For a contradiction, suppose that T is not infinite and hence there is some level n at which T has no nodes. Notice that our coding for pairs satisfies the inequality $\langle x, y\rangle \geq y$. Therefore, if $\langle x, y\rangle$ occurs in the construction before stage n, we know that $y \leq n$. That is, at stage n, T has only considered elements from A_0 through A_n. By Theorem 3.21,

$$RCA_0 \vdash \prod_{i=0}^{n} A_i \text{ is an O-group.}$$

Let X be the strict positive cone for a full order on this finite product and $P^+(A_i)$ be defined by

$$x \in P^+(A_i) \;\leftrightarrow\; \langle 1_{A_0}, \ldots, 1_{A_{i-1}}, x, 1_{A_{i+1}}, \ldots, 1_{A_n}\rangle \in X.$$

For each $k \leq n$, $k = \langle x, i\rangle$ for some $i \leq n$. Define $\sigma \in \mathrm{Fin}_{\mathbb{N}}$ with $\mathrm{lh}(\sigma) = n$ by

$$\sigma(k) = \begin{cases} 1 & \text{if } k = \langle x, i\rangle \wedge x \in P^+(A_i) \\ 0 & \text{otherwise} \end{cases}$$

From the definition it is clear that

$$\sigma(k) = 0 \leftrightarrow x = 1_{A_i} \vee x^{-1} \in P^+(A_i) \vee x \notin A_i. \tag{3.1}$$

To prove the claim, it suffices to show that $\sigma \in T$. We show by induction that for all $k \leq n$, $\sigma|_k \in T$ and $P_{\sigma|_k} \subseteq X$. Clearly, $\sigma|_0 = \langle\rangle \in T$ and $P_{\sigma|_0} = \emptyset \subseteq X$. Assume that $\sigma|_k \in T$ and $P_{\sigma|_k} \subseteq X$. Because $1_{A_j} \notin P_{\sigma|_k}$ we know that $\sigma|_{k+1} \in T$. From the definition of σ and Equation 3.1, it is clear that $\tilde{P}_{\sigma|_{k+1}} \subseteq X$. Because $P_{\sigma|_{k+1}}$ is obtained by multiplying and conjugating elements of $\tilde{P}_{\sigma|_{k+1}}$, it follows that $P_{\sigma|_{k+1}} \subseteq X$. Thus, $\sigma|_n = \sigma \in T$.

Since T is infinite, WKL_0 provides a path S through T. Define:

$$\tilde{Z} = \bigcup_{\sigma \in S} P_\sigma$$

$$Z = \tilde{Z} \;\cup\; \{\langle 1_{A_i}, i\rangle \mid i \in \mathbb{N}\}.$$

$\tilde{Z}$ has a Σ^0_1 definition, but for $x \neq 1_{A_i}$

$$\langle x, i\rangle \in \tilde{Z} \leftrightarrow \langle x^{-1}, i\rangle \notin \tilde{Z}.$$

Thus, $\tilde{Z}$ has a Δ^0_1 definition and so both $\tilde{Z}$ and Z exist. It remains to show that Z_i is the positive cone for a full order on A_i.

To show Z_i is full, consider any $x \in A_i$, $x \neq 1_{A_i}$. Let $\sigma \in S$ with $\mathrm{lh}(\sigma) = \langle x, i\rangle$. Since S is a path, either $\sigma^\frown 0 \in S$ or $\sigma^\frown 1 \in S$.

$$\sigma^\frown 0 \in S \Rightarrow \langle x, i\rangle \in P_{\sigma^\frown 0} \Rightarrow x \in Z_i$$

$$\sigma^\frown 1 \in S \Rightarrow \langle x^{-1}, i\rangle \in P_{\sigma^\frown 1} \Rightarrow x^{-1} \in Z_i$$

To show Z_i is pure, suppose $x \neq 1_{A_i}$ and $x, x^{-1} \in Z_i$. For some $\sigma \in S$, $\langle x, i\rangle, \langle x^{-1}, i\rangle \in P_\sigma$. From the construction, 1_{A_i} appears in both $P_{\sigma^\frown 0}$ and $P_{\sigma^\frown 1}$ so neither $\sigma^\frown 0$ nor $\sigma^\frown 1$ has an extension. This condition means σ cannot be on a path which contradicts $\sigma \in S$.

Z_i is a semigroup since if $x, y \in Z_i$ then there is a $\sigma \in S$ such that $\langle x, i\rangle, \langle y, i\rangle \in P_\sigma$. S is a path so P_σ has an extension τ in the tree. By the one step multiplicative closure, $\langle x \cdot_{A_i} y, i\rangle \in P_\tau$ and hence $x \cdot_{A_i} y \in Z_i$. Showing Z_i is normal is similar but uses the one step closure under conjugates. Thus Z_i is a full order on A_i and we have constructed the desired uniform order.

Case. (2) $\Rightarrow$ (1):

Assume the restricted direct product of O-groups is an O-group. To prove WKL_0, it suffices by Theorem 1.15 to prove that a separating set exists for any two functions with disjoint ranges. Let f, g be functions such that for all n, m, $f(n) \neq g(m)$. We need to form a set S such that

$$\text{range}(f) \subseteq S \ \wedge \ \text{range}(g) \subseteq \mathbb{N} \setminus S.$$

Recall from the first half of this proof, that an order on the direct product is equivalent over RCA_0 to a uniform order on the components A_i. The idea of this proof is to give abelian groups A_n each of which has two generators, a_n and b_n. If n is in the range of f, we force a_n and b_n to have the same sign in any order on A_n. That is, either both are positive or both are negative. If n is in the range of g, we force a_n and b_n to have different signs in any order. If neither of these holds, then we let A_n be a torsion free abelian group on two generators. Since the groups are abelian, we use additive notation. The groups look like:

$$A_{f(n)} = \langle a_{f(n)}, b_{f(n)} \mid a_{f(n)} = p_n b_{f(n)}\rangle$$
$$A_{g(n)} = \langle a_{g(n)}, b_{g(n)} \mid a_{g(n)} = -p_n b_{g(n)}\rangle$$

where p_n is the n$^{\text{th}}$ prime starting with 3. If n is not in the range of f or g then

$$A_n = \langle a_n, b_n \mid - \rangle.$$

Formally, A_n is given by the elements $ca_n + db_n$ where $c, d \in \mathbb{Z}$ and

$$\neg\exists i(p_i < 2|d| \wedge f(i) = n)$$
$$\neg\exists i(p_i < 2|d| \wedge g(i) = n).$$

To add $ca_n + db_n$ and $c'a_n + d'b_n$ we check whether $(c + c')\, a_n + (d + d')\, b_n$ violates either of these conditions. If there is an i such that $p_i < 2|d+d'|$ and $f(i) = n$, then we use the relation $a_n = p_i b_n$ to rewrite $(d + d')\, b_n$ as $c''a_n + d''b_n$ where $|d''| < p_i/2$. If the second condition is violated, we do the same thing except we use the relation $a_n = -p_i b_n$. We start the numbering of the primes with 3 because if we started with 2 and $f(2) = n$ then the elements $a_n + b_n$ and $2a_n - b_n$ would be the same. Using only odd p_i makes the coding more convenient.

Because the definition of A_n is uniform in n, the sequence A_n exists. It remains to show that each A_n is orderable and that the separating set is given by a uniform order of the A_n.

Claim. Each A_n is an O-group.

The proof of this claim splits into three cases. In RCA_0, we cannot tell which case holds, but we know that one of them must hold.

1. If $f(i) = n$ then
$$P(A_n) = \{ca_n + db_n \mid c > 0 \vee (c = 0 \wedge d \geq 0)\}.$$
2. If $g(i) = n$ then
$$P(A_n) = \{ca_n + db_n \mid c > 0 \vee (c = 0 \wedge d \leq 0)\}.$$
3. If $n \notin \text{range}(g) \cup \text{range}(f)$ then
$$P(A_n) = \{ca_n + db_n \mid c > 0 \vee (c = 0 \wedge d \geq 0)\}.$$

In each case it is easy to verify that the set given is the positive cone of a full order. This shows
$$RCA_0 \vdash \forall n(A_n \text{ is an O-group}).$$
By assumption, there is a uniform order on the A_n. Let P be the uniform positive cone. That is, P_n is the positive cone of a full order on A_n. Define S by
$$S = \{n \mid a_n \in P_n \leftrightarrow b_n \in P_n\}.$$
S is the desired separating set since if n is in the range of f then $a_n \in P_n \leftrightarrow b_n \in P_n$ while if n is in the range of g then $a_n \in P_n \leftrightarrow -b_n \in P_n$. □

From the perspective of computable mathematics, uniformity is also the key issue in ordering direct products. If we are given computable f.o. groups uniformly, then the direct product can be computably fully ordered using the lexicographic order. However, if we have a sequence of computably fully orderable computable groups, it is not necessarily possible to compute a uniform sequence of computable full orders. We have the following corollaries to Theorems 3.21 and 3.23.

Corollary 3.24. *The direct product of a finite number of computably fully orderable computable groups is computably fully orderable.*

Corollary 3.25. *There is a uniform sequence of computably fully orderable computable groups G_i, $i \in \omega$, such that $\Pi_{i \in \omega} G_i$ is a computable group with no computable full order. $\Pi_{i \in \omega} G_i$ does have a full order of low degree.*

3.3 The Center

The results in this section concern how complicated the center of a group can be. In terms of reverse mathematics, the existence of the center is equivalent to ACA_0. As a consequence, there is a computable group whose center is as complicated as $0'$. However, this result can be refined to show that even for 2 step nilpotent groups, which are intuitively the simplest nonabelian groups, the center can still be as complicated as $0'$. In order to prove these results, we need an introduction to 2 step nilpotent groups.

Definition 3.26. G is **n step nilpotent**, for $n > 1$, if $\zeta_n G = G$. G is **properly n step nilpotent** if G is n step nilpotent and $\zeta_{n-1} G \neq G$.

According to the definition, G is properly 2 step nilpotent if $C(G) \neq G$ and $G/C(G)$ is abelian. These groups can also be defined in terms of the lower central series. The following lemma states the essential property of this alternate definition.

Lemma 3.27. *G is 2 step nilpotent if and only if each commutator $[x, y]$ commutes with all the elements of the group.*

Lemma 3.27 can be used to establish the following identity for 2 step nilpotent groups.

$$\begin{aligned} [x^{-1}, y] &= xy^{-1}x^{-1}y \\ &= xy^{-1}x^{-1}yxx^{-1} \\ &= x \cdot [y, x] \cdot x^{-1} \\ &= [y, x] \end{aligned}$$

Similarly, we have:

$$[x, y^{-1}] = [y, x]$$
$$[x^{-1}, y^{-1}] = [x, y]$$
$$[x, y]^{-1} = [y, x].$$

Let G be a free group on the generators a_i, $i \in \omega$, subject to the relations $[[g, h], k] = 1_G$ for all $g, h, k \in G$. This group is called the free 2 step nilpotent group on a_i. We have the following identity:

$$a_i a_j = a_j a_i a_i^{-1} a_j^{-1} a_i a_j = a_j a_i \cdot [a_i, a_j].$$

Using the identities above and performing similar calculations, we get

$$a_i^{-1} a_j = a_j a_i^{-1} \cdot [a_j, a_i]$$
$$a_i a_j^{-1} = a_j^{-1} a_i \cdot [a_j, a_i]$$
$$a_i^{-1} a_j^{-1} = a_j^{-1} a_i^{-1} \cdot [a_i, a_j].$$

Because these identities allow us to commute any pair of generators modulo a commutator of generators, we can write any element of G as

$$a_{j_0}^{k_0} a_{j_1}^{k_1} \cdots a_{j_l}^{k_l} \cdot c$$

where $j_0 < j_1 < \cdots < j_l$, $k_i \in \mathbb{Z} \setminus \{0\}$ and c is a product of commutators. Furthermore, we can write c as a product of powers of commutators of the form $[a_i, a_j]$ or $[a_i, a_j]^{-1}$ with $i < j$. To get a unique normal form for each element, we arrange these commutators so that a power of $[a_i, a_j]$ occurs to the left of a power of $[a_k, a_l]$ if and only if $i < k$ or $i = k$ and $j < l$.

These normal forms give us a computable presentation of the free 2 step nilpotent group. Furthermore, since we can write down a description of the normal form using only bounded quantifiers, we can define the free 2 step nilpotent group on generators a_i, $i \in \omega$, in RCA_0. Because an element is in the center if and only if it is a product of commutators, RCA_0 suffices to prove that there is a nilpotent code for this group.

Theorem 3.28. *(RCA_0) The following are equivalent:*

1. *ACA_0*
2. *For every group G the center of G, $C(G)$, exists.*

Proof.
Case. (1) $\Rightarrow$ (2)

The center of G is defined by a Π_1^0 formula, so ACA_0 suffices to prove its existence.

Case. (2) $\Rightarrow$ (1)

By Theorem 1.16, it suffices to prove the existence of the range of an arbitrary one-one function f. Let G be the free 2 step nilpotent group on generators a_i and b_i for $i \in \mathbb{N}$ with the following extra relations:

$$a_i a_j = a_j a_i \text{ for all } i, j \in \omega$$
$$b_i b_j = b_j b_i \text{ for all } i, j \in \omega$$
$$a_i b_j = b_j a_i \iff \forall k \leq i\, (f(k) \neq j).$$

Elements of G have unique normal forms:

$$a_{i_1}^{n_1} \cdots a_{i_k}^{n_k} b_{j_1}^{m_1} \cdots b_{j_l}^{m_l} \cdot c$$

where $i_1 < \cdots < i_k$, $j_1 < \cdots < j_l$, $n_p \neq 0$ and $m_q \neq 0$ for $1 \leq p \leq k$ and $1 \leq q \leq l$, and c is a product of commutators with those which match the added relations removed. By the comments above, G exists as a group in RCA_0. However, as we are about to see, RCA_0 is not strong enough to prove that there is a code for G as a nilpotent group.

Let $C(G)$ be the center of G. To define the range of f we use the following equivalences:

$$\begin{aligned} b_j \in C(G) &\Leftrightarrow \forall i\,(a_i b_j = b_j a_i) \\ &\Leftrightarrow \forall i\,\forall k \leq i\,(f(k) \neq j) \\ &\Leftrightarrow \forall k\,(f(k) \neq j). \end{aligned}$$

Therefore, $b_j \in C(G)$ if and only if j is not in the range of f. This equivalence allows us to give a Σ^0_0 definition of the range of f.

$$\text{range}(f) \;=\; \{\, j \mid b_j \notin C(G)\,\}$$

□

Corollary 3.29. *There is a computable 2 step nilpotent group G such that $C(G) \equiv_T 0'$.*

Proof. Consider the group G constructed in the theorem when f is a computable one-one function enumerating the halting problem. G satisfies the conditions of the corollary. Since we can define the range of f from $C(G)$, we have $0' \leq_T C(G)$. However, because $C(G)$ has a Π^0_1 definition from G and G is computable, we know that $C(G) \leq_T 0'$. □

In addition, the group G in Corollary 3.29 is computably fully orderable. Let H be the subgroup generated by the commutators. H is normal because G is 2 step nilpotent and H is computable because we can tell if an element is the product of commutators by looking at the normal form. H is generated by commutators of the form $[a_i, b_j]$ for which $\exists k \leq i\,(f(k) = j)$. There are no relations between these generators, so H is a torsion free abelian group which can be computably fully ordered using the generators. Since G is 2 step nilpotent, the elements of H commute with all elements of G. Therefore, any full order on H is a full G-order. G/H is the abelianization of G, which is the torsion free abelian group generated by a_i and b_j for $i, j \in \omega$. Again, there are no extra relations between these elements in G/H, so G/H can be computably fully ordered using these generators. Using Theorem 2.19, the orders on H and G/H can be combined into a computable full order on G.

Finitely generated nilpotent groups have been extensively studied from the viewpoint of computational algebra. These groups have very nice computational properties. For example, the word problem, the conjugacy problem and the isomorphism problem are all solvable. The key algebraic facts to establish these results are that finitely generated nilpotent groups are also finitely presented, that finitely generated nilpotent groups are residually finite and that every subgroup is finitely generated.

Theorem 3.30 (Baumslag et al. (1991)). *The center of a finitely generated nilpotent group is computable.*

Corollary 3.31 (Baumslag et al. (1991)). *All the terms in the upper central series for a finitely generated nilpotent group are computable.*

3.4 Spaces of Full Orders

Once a group G is known to be fully orderable, there are many natural questions to ask about the space of all full orders on G. For example, algebraists have tried to say explicitly what the full orders look like. This project turns out to be extremely difficult. An easier question is how computationally complicated can the orders be. Downey and Kurtz (1986) phrased this question in terms of the connection between c.b. Π^0_1 classes and full orders on torsion free abelian groups. In Chapter 8, we will formulate their question explicitly and answer it.

A first step towards answering this question comes from looking at the proof of Theorem 3.23. In the proof of this theorem, we used nodes on a tree to guess at full orders and terminate branches when they violate certain algebraic conditions. We used the property that finite direct products are orderable to show, in WKL_0, that the tree is infinite and therefore has a path. This path codes a full order on the countable direct product.

In this section, we give a similar argument, only not in the context of reverse mathematics. Starting with a fully orderable computable group G, we build a computable binary branching tree, the paths of which code all the full orders on G. Since we are not restricted to a weak axiom system, the property that G is fully orderable is enough to guarantee that the tree is infinite. The paths of the tree correspond, up to Turing degree, exactly to the full orders of G. In this way, we show that up to Turing degree, the space of full orders on a computable group is a c.b. Π^0_1 class.

Definition 3.32. Let G be a fully orderable computable group. The **space of orders** of G, denoted $\mathbb{X}(G)$, is

$$\{\, P \subseteq G \,|\, P \text{ is the positive cone of a full order on } G \,\}.$$

Metakides and Nerode performed a similar analysis for orderable computable fields. Their work on the connection between spaces of orders for such fields and c.b. Π^0_1 classes was the motivation for Downey and Kurtz (1986) to ask about these connections for ordered groups.

Theorem 3.33 (Metakides and Nerode (1979)). *Let F be an orderable computable field. There is a c.b. Π^0_1 class C and a Turing degree preserving bijection $\varphi : \mathbb{X}(F) \to C$.*

Theorem 3.34. *Let G be a fully orderable computable group. There is a c.b. Π^0_1 class C and a Turing degree preserving bijection $\varphi : \mathbb{X}(G) \to C$.*

Proof. Let G be a fully orderable computable group enumerated by $g_0, g_1, \ldots$ with $g_0 = 1_G$. We build a computable binary branching tree T in stages. T_n denotes the part of T built at the end of stage n and includes all the nodes of T of length $\leq n$. To each node $\sigma \in T$ there is an associated finite set S_σ, which contains σ's guess at a subset of a strict positive cone.

Construction

Stage 0: $\langle\rangle \in T_0$ and $S_{\langle\rangle} = \emptyset$.

Stage 1: $\langle 1\rangle \in T_1$ and $S_{\langle 1\rangle} = \emptyset$. The purpose of this stage is to put a code for 1_G into every path but not to include 1_G in the strict positive cone.

Stage n+1: Assume T_n is given and define T_{n+1} to include T_n. For each $\sigma \in T_n$ with $\text{lh}(\sigma) = n$ do the following:

1. If $1_G \in S_\sigma$, then σ has no extensions in T_{n+1}.
2. Otherwise, both $\sigma^\frown 0$ and $\sigma^\frown 1$ are put into T_{n+1}.

We define the associated sets by:

$$S_{\sigma^\frown 0} = S_\sigma \cup \{g_{n+1}^{-1}\} \cup \{gh | g, h \in S_\sigma\} \cup \{g_i^{-1} h g_i | i \leq n+1 \wedge h \in S_\sigma\}$$
$$S_{\sigma^\frown 1} = S_\sigma \cup \{g_{n+1}\} \cup \{gh | g, h \in S_\sigma\} \cup \{g_i^{-1} h g_i | i \leq n+1 \wedge h \in S_\sigma\}.$$

End of Construction

Let C be the c.b. Π_1^0 class of paths through T. For each $P \in \mathbb{X}(G)$, let $f_P : \omega \to \{0,1\}$ be the map that sends n to 0 if $g_n \notin P$ and sends n to 1 if $g_n \in P$. For each $f \in C$, let P_f be the set

$$P_f = \{\, g \in G \,|\, f(g) = 1 \,\} \cup \{\, g^{-1} \,|\, f(g) = 0 \,\}.$$

We can now define the map $\varphi : \mathbb{X} \to C$ as the map that takes P to f_P. We need to verify that φ is a degree preserving bijection.

Claim. For each $f \in C$, $P_f \in \mathbb{X}(G)$.

To prove this claim, we check the required algebraic properties of P_f. To see that P_f is full, notice that $f(0) = 1$, so $1_G \in P_f$. For $n > 0$, either $f(n) = 1$, in which case $n \in P_f$, or $f(n) = 0$, in which case $n^{-1} \in P_f$. Therefore, $P_f \cup P_f^{-1} = G$.

To show that P_f is a semigroup, we only need to show it is closed under multiplication. Assume $g, h \in P_f$ and $gh \notin P_f$. Since P_f is full, we know that $h^{-1}g^{-1} \in P_f$. Let n be the maximum of the indices for g, h and $h^{-1}g^{-1}$. By the construction we have the following:

$$g, h, h^{-1}g^{-1} \in S_{f|_n}$$
$$g, g^{-1} \in S_{f|_{n+1}}$$
$$1_G \in S_{f|_{n+2}}.$$

Therefore, $f|_{n+2}$ has no extensions in T which contradicts the fact that f is a path through T. The proofs for normality and purity are similar.

Claim. For each $P \in \mathbb{X}(G)$, $f_P \in C$.

We prove by induction that $f_P|_n$ is on T for all n. The case for $n = 0$ follows from stage 1 of the construction because $1_G \in P$, $g_0 = 1_G$ and $\langle 1 \rangle \in T$. Also, notice that

$$S_{\langle 1 \rangle} = \emptyset \subseteq P^+ = P \setminus \{1_G\}.$$

For the inductive step, assume that $f_P|_n \in T$ and $S_{f_P|_n} \subseteq P^+$. Thus $1_G \notin S_{f_P|_n}$ and so both $f_P|_n{}^\frown 0$ and $f_P|_n{}^\frown 1$ are in T. Without loss of generality, assume that $f_P(n+1) = 1$ and so $f_P|_{n+1} = f_P|_n{}^\frown 1$. Since $g_{n+1} \neq 1_G$ and $f_P(n+1) = 1$, we know that $g_{n+1} \in P^+$. Also, since $S_{f_P|_n} \subseteq P^+$ and P^+ is closed under one multiplication and conjugation, we have $S_{f_P|_{n+1}} \subseteq P^+$ as required.

To finish the proof, we make the following trivial observations:

1. If $g \in C$, then $g = f_{P_g}$.
2. If $Q \in \mathbb{X}(G)$, then $Q = P_{f_Q}$.
3. If $P \neq Q$ in $\mathbb{X}(G)$, then $f_P \neq f_Q$.
4. If $f \neq g$ in C, then $P_f \neq P_g$.

These observations show that φ is a bijection and that φ^{-1} takes $f \in C$ to $P_f \in \mathbb{X}(G)$. Finally, from the definitions it is clear that $f_P \leq_T P$ for any $P \in \mathbb{X}(G)$ and $P_f \leq_T f$ for any $f \in C$. Therefore, $\deg(P) = \deg(f_P)$, so φ preserves Turing degrees. □

Chapter 4

Semigroup Conditions

4.1 Definition of the Conditions

In Chapter 3, we examined group conditions that imply full orderability. Semigroup conditions can also be analyzed to determine if a group is orderable. In this chapter, we study three theorems giving semigroup conditions. The versions stated in Kokorin and Kopytov (1974) are given below. In these theorems, $S(a_1, \ldots, a_n)$ denotes the normal semigroup generated by $a_1, \ldots, a_n$.

Theorem 4.1 (Fuchs (1958)). *A partial order on G with positive cone P can be extended to a full order if and only if for any finite sequence of non-identity elements, $a_1, \ldots, a_n \in G$, there is a sequence $\epsilon_1, \ldots, \epsilon_n$ with $\epsilon_i = \pm 1$ such that*

$$P \cap S(a_1^{\epsilon_1}, \ldots a_n^{\epsilon_n}) = \emptyset.$$

Theorem 4.2 (Łos (1954), Ohnishi (1952)). *G is an O-group if and only if for any finite sequence of non-identity elements $a_1, \ldots, a_n$ there exists a sequence $\epsilon_1, \ldots, \epsilon_n$ such that*

$$1_G \notin S(a_1^{\epsilon_1}, \ldots a_n^{\epsilon_n}).$$

Theorem 4.3 (Lorenzen (1949)). *G is an O-group if and only if for any finite sequence of non-identity elements $a_1, \ldots, a_n$*

$$\bigcap S(a_1^{\epsilon_1}, \ldots a_n^{\epsilon_n}) = \emptyset$$

where the intersection extends over all sequences $\epsilon_1, \ldots, \epsilon_n$ with $\epsilon_i = \pm 1$.

The first step in studying these theorems in reverse mathematics is to translate the semigroup conditions into the language of second order arithmetic. To do this, we need a definition for the normal semigroup generated by a finite number of elements. If A is the code of a finite sequence of elements of G, let $S(A)$ be the normal semigroup generated by A. $S(A)$ is built in stages with $S(A) = \bigcup_n S_n(A)$. The idea is to start with $S_0(A) = A$ and at step $n+1$, add the elements that can be formed by conjugating a member of $S_n(A)$ or by multiplying two members of $S_n(A)$.

$$\begin{array}{rcl} S_0(A) & = & A \\ & \vdots & \\ S_{n+1}(A) & = & S_n(A) \ \cup \ \{gag^{-1} \mid a \in S_n(A), g \in G\} \ \cup \ \{ab \mid a, b \in S_n(A)\} \\ & \vdots & \end{array}$$

It is clear that $S(A) = \bigcup_n S_n(A)$ is the desired semigroup. Formally, we define a function s such that:

$$x \in S_n(A) \leftrightarrow \exists m \, (s(A, n, m, x) = 1)$$

and for all n, m, x either $s(A, n, m, x) = 0$ or $s(A, n, m, x) = 1$. Define s by recursion on n with A and m as parameters.

$$s(A, 0, m, x) = \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{otherwise} \end{cases}$$

$$s(A, n+1, m, x) = \begin{cases} 1 & \text{if } s(A, n, m, x) = 1 \text{ or} \\ & \exists a, g \leq m \, (s(A, n, m, a) = 1 \wedge x = gag^{-1}) \text{ or} \\ & \exists a, b \leq m \, (s(A, n, m, a) = s(A, n, m, b) = 1 \wedge \\ & \qquad \wedge \ x = ab) \\ 0 & \text{otherwise} \end{cases}$$

Before proceeding with the main results of this chapter, we need to establish two preliminary facts.

Definition 4.4. (RCA_0) If A is a code for a finite sequence of elements of G, let A^{-1} be the code for the finite sequence defined by $A^{-1}(k) = A(k)^{-1}$ for $0 \leq k \leq \mathrm{lh}(A)$.

Lemma 4.5. *(RCA_0) If A is a code for a finite sequence of elements of G and $s(A, n, m, x) = 1$, then $\exists p \, (s(A^{-1}, n, p, x^{-1}) = 1)$.*

Proof. The proof is by Σ^0_1 induction on n.
Base case: Assume $s(A, 0, m, x) = 1$ and so $x \in A$. By definition, $x^{-1} \in A^{-1}$ and $s(A^{-1}, 0, m, x^{-1}) = 1$.
Induction case: Assume $s(A, n+1, m, x) = 1$ and split into three subcases.

1. If $s(A, n, m, x) = 1$ then the induction hypothesis implies there is a p such that $s(A^{-1}, n, p, x^{-1}) = 1$ and hence $s(A^{-1}, n+1, p, x^{-1}) = 1$.

2. There are $g, a \leq m$ with $s(A, n, m, a) = 1$ and $x = gag^{-1}$. By the induction hypothesis there is a p with $s(A^{-1}, n, p, a^{-1}) = 1$. Since $x^{-1} = ga^{-1}g^{-1}$, taking $\tilde{p} = \max\{p, g\}$ gives $s(A^{-1}, n+1, \tilde{p}, x^{-1}) = 1$.

3. There are $a, b \leq m$ with $s(A, n, m, a) = s(A, n, m, b) = 1$ and $x = ab$. By the induction hypothesis there are p_1, p_2 such that $s(A^{-1}, n, p_1, a^{-1}) = 1$ and $s(A^{-1}, n, p_2, b^{-1}) = 1$. Let $p = \max\{p_1, p_2\}$. Since $x^{-1} = b^{-1}a^{-1}$, if follows that $s(A^{-1}, n+1, p, x^{-1}) = 1$.

□

Lemma 4.6. *(RCA_0) Let P be the positive cone of a full order on G and A be a code for a finite sequence of nonidentity elements of P. If $s(A, n, m, x) = 1$ then $x > 1_G$.*

Proof. The proof is by Σ^0_1 induction on n.
For the base case, assume $s(A, 0, m, x) = 1$. Since $A \subset P$ and $1_G \notin P$, $x > 1_G$. For the induction case, use the same three subcases as in Lemma 4.5. □

The next step is to write the semigroup conditions using $s(A, n, m, x)$. Let $\mathrm{Fin}_{\pm 1}$ be the set of codes for finite sequences of ± 1. If $A \in \mathrm{Fin}_G$, $\sigma \in \mathrm{Fin}_{\pm 1}$, and $\mathrm{lh}(A) = \mathrm{lh}(\sigma)$, then let A_σ be the sequence of elements of G defined by:

$$\mathrm{lh}(A_\sigma) = \mathrm{lh}(A)$$
$$\forall k < \mathrm{lh}(A_\sigma)\ (A_\sigma(k) = A(k)^{\sigma(k)}).$$

For example, if $A = \langle 1_G, a\rangle$ and $\sigma = \langle +1, -1\rangle$ then $A_\sigma = \langle 1_G, a^{-1}\rangle$.

In the remaining equations in this section, it is assumed that A ranges over $\mathrm{Fin}_{G\setminus 1_G}$ and σ ranges over $\mathrm{Fin}_{\pm 1}$. The semigroup condition in Theorem 4.1 can be translated into the notation of $s(A, n, m, x)$ by the following steps:

$$\forall A\, \exists \sigma\ \big(\mathrm{lh}(A) = \mathrm{lh}(\sigma) \wedge P \cap S(A_\sigma) = \emptyset\big)$$
$$\forall A\, \exists \sigma\, \forall x\ \big(\mathrm{lh}(A) = \mathrm{lh}(\sigma) \wedge (x \in S(A_\sigma) \rightarrow x \notin P)\big)$$
$$\forall A\, \exists \sigma\, \forall x\ \big(\mathrm{lh}(A) = \mathrm{lh}(\sigma) \wedge (\exists n, m\ s(A_\sigma, n, m, x) = 1 \rightarrow x \notin P)\big)$$
$$\forall A\, \exists \sigma\, \forall x\ \big(\mathrm{lh}(A) = \mathrm{lh}(\sigma) \wedge (\forall n, m\ s(A_\sigma, n, m, x) = 0 \vee x \notin P)\big).$$

Since $\exists \sigma \in \mathrm{Fin}_{\pm 1}(\mathrm{lh}(\sigma) = \mathrm{lh}(A))$ is really a bounded quantifier, this condition is Π^0_1.

The semigroup condition in Theorem 4.2 can be translated as follows:

$$\forall A\, \exists \sigma\ \big(\mathrm{lh}(A) = \mathrm{lh}(\sigma) \wedge 1_G \notin S(A_\sigma)\big)$$
$$\forall A\, \exists \sigma\ \big(\mathrm{lh}(A) = \mathrm{lh}(\sigma) \wedge \forall n, m\, s(A_\sigma, n, m, 1_G) = 0\big).$$

Again, because $\exists \sigma \in \mathrm{Fin}_{\pm 1}(\mathrm{lh}(\sigma) = \mathrm{lh}(A))$ is a bounded quantifier, this condition is Π^0_1.

The semigroup condition in Theorem 4.3 can be written as follows:

$$\forall A\, \forall x\, \exists \sigma\ \big(\mathrm{lh}(A) = \mathrm{lh}(\sigma) \wedge x \notin S(A_\sigma)\big)$$
$$\forall A\, \forall x\, \exists \sigma\ \big(\mathrm{lh}(A) = \mathrm{lh}(\sigma) \wedge \forall m, n\, s(A_\sigma, n, m, x) = 0\big).$$

This sentence is also Π^0_1.

Theorems 4.1, 4.2 and 4.3 can now be stated in the language of second order arithmetic.

Theorem 4.7. *(WKL_0) A partial order on G with positive cone P can be extended to a full order if and only if*

$$\forall A\, \exists \sigma\, \forall x, n, m\ \big(lh(A) = lh(\sigma) \wedge (s(A_\sigma, n, m, x) = 0 \vee x \notin P)\big). \tag{4.1}$$

Theorem 4.8. *(WKL_0) G is an O-group if and only if*

$$\forall A\, \exists \sigma\, \forall n, m\ \big(lh(A) = lh(\sigma) \wedge s(A_\sigma, n, m, 1_G) = 0\big). \tag{4.2}$$

Theorem 4.9. *(WKL_0) G is an O-group if and only if*

$$\forall A\, \forall x\, \exists \sigma\, \forall m, n\ \big(lh(A) = lh(\sigma) \wedge s(A_\sigma, n, m, x) = 0\big). \tag{4.3}$$

There are several connections between these theorems. G is an O-group if and only if the trivial order with positive cone $P = \{1_G\}$ can be extended to a full order. By Theorem 4.7, this condition is equivalent to:

$$\forall A \exists \sigma \forall x, n, m\ \big(\mathrm{lh}(A) = \mathrm{lh}(\sigma) \wedge (s(A_\sigma, n, m, x) = 0 \vee x \neq 1_G)\big)$$

which in turn is equivalent to Equation (4.2). Hence, RCA_0 proves that Theorem 4.8 is a special case of Theorem 4.7. Setting $x = 1_G$ shows that (4.3) implies (4.2).

Showing that Equation (4.2) implies Equation (4.3) requires more work. For $\sigma \in \mathrm{Fin}_{\pm 1}$, let σ^{-1} have the same length as σ with $\sigma^{-1}(k) = -\sigma(k)$. Notice that $A_{\sigma^{-1}} = A_\sigma^{-1}$ and $(A_{\sigma^{-1}})^{-1} = A_\sigma$. For a contradiction, suppose that (4.2) holds and (4.3) does not. Because (4.3) fails, there are A and x such that

$$\forall \sigma \in \mathrm{Fin}_{\pm 1} \exists m, n\ \big(\mathrm{lh}(\sigma) = \mathrm{lh}(A) \rightarrow s(A_\sigma, n, m, x) = 1\big). \tag{4.4}$$

Fix A and x. Because (4.2) holds, there is a σ such that

$$\forall n, m\ \big(s(A_\sigma, n, m, 1_G) = 0\big). \tag{4.5}$$

Fix σ. Applying (4.4) with σ^{-1}, we have $s(A_{\sigma^{-1}}, n, m, x) = 1$ for some m, n and hence by Lemma 4.5, $s(A_\sigma, n, p, x^{-1}) = 1$. Applying (4.4) with σ we have $s(A_\sigma, \tilde{n}, \tilde{m}, x) = 1$ for some $\tilde{m}, \tilde{n}$. Without loss of generality, assume $n \geq \tilde{n}$. By definition, $s(A_\sigma, n, \tilde{m}, x) = 1$ and so if $k > n, \tilde{m}$ then $s(A_\sigma, n, k, 1_G) = 1$. This fact contradicts (4.5).

4.2 Equivalence with WKL_0

The goal for the rest of this chapter is to prove the following theorem.

Theorem 4.10. *(RCA_0) The following are equivalent:*

1. *WKL_0*

2. *Theorem 4.7*

3. *Theorem 4.8*

4. *Theorem 4.9*

By the comments at the end of the last section, we know that (2) implies (3) and that (3) and (4) are equivalent. In this section, we will show that (1) implies (2) and that (3) implies (1).

Proposition 4.11. *(RCA_0) If a partial order on G with positive cone P can be extended to a full order, then Equation* (4.1) *holds for P.*

Proof. Assume Q is the positive cone of a full order extending P. Given any $A \in \mathrm{Fin}_{G\setminus 1_G}$, let $\sigma \in \mathrm{Fin}_{\pm 1}$ be such that $\mathrm{lh}(\sigma) = \mathrm{lh}(A)$ and for every $k < \mathrm{lh}(\sigma)$, $A(k)^{-\sigma(k)} \in Q$. For a contradiction, assume for some x, n, m we have

$$s(A_\sigma, n, m, x) = 1 \wedge x \in P.$$

Because $P \subseteq Q$, we have that $x \in Q$. Applying Lemma 4.5 to $s(A_\sigma, n, m, x) = 1$, we have $s(A_{\sigma^{-1}}, n, p, x^{-1}) = 1$ for some p. However by our choice of σ, $A_{\sigma^{-1}}$ must be contained in $Q \setminus 1_G$ and hence $x^{-1} > 1_G$ by Lemma 4.6. Thus $x, x^{-1} \in Q$ and so $x = 1_G$. This conclusion contradicts $x^{-1} > 1_G$. $\square$

Proposition 4.12. *(WKL_0) If $P \subset G$ and Equation* (4.1) *holds for P then P can be extended to the positive cone of a full order on G.*

Proof. This proof is similar to the proof of Theorem 3.23. Suppose G is enumerated as $g_0, g_1, \ldots$. We build a binary branching tree T which codes the positive cone of a full order along every path. Equation (4.1) will imply that T is infinite and so WKL_0 guarantees that it has a path. To simplify the notation we construct $T \subseteq \mathrm{Fin}_{\pm 1}$ instead of $T \subseteq \mathrm{Fin}_{\{0,1\}}$. For each $\sigma \in T$ with $\mathrm{lh}(\sigma) = k$, let $Q_\sigma \in \mathrm{Fin}_{G\setminus 1_G}$ be

$$Q_\sigma \;=\; \langle g_1^{\sigma(1)}, \ldots, g_{k-1}^{\sigma(k-1)} \rangle.$$

For example, if $\sigma = \langle +1, -1, -1 \rangle$ then $Q_\sigma = \langle g_1^{-1}, g_2^{-1} \rangle$. The reason for not including g_0 in Q_σ is so that $1_G \notin Q_\sigma$. Q_σ represents σ's guess as a subset of a strict positive cone extending P.

As in the earlier constructions, T is built in stages and after stage k, no new nodes of length k enter T. T_k denotes the nodes of T after stage k.

Construction

Stage 0: Set $T_0 = \{\langle\rangle\}$ and $Q_{\langle\rangle} = \langle\rangle$.

Stage 1: Set $T_1 = \{\langle\rangle, \langle -1 \rangle\}$ and $Q_{\langle -1 \rangle} = \langle\rangle$. The purpose of this stage is to code 1_G into every path.

Stage s = k+1: For each $\sigma \in T_k$ check if Equation (4.1) has been violated by a number below k:

$$\exists x, n, m \leq k \ \big(s(Q_\sigma, n, m, x) = 1 \wedge x \in P\big)$$

There are two possible answers to this question.

1. If YES: Equation (4.1) has been violated, so neither $\sigma^\frown\langle -1\rangle$ nor $\sigma^\frown\langle +1\rangle$ enters T_{k+1}.
2. If NO: Extend σ by putting both $\sigma^\frown\langle -1\rangle$ and $\sigma^\frown\langle +1\rangle$ in T_{k+1}.

End of Construction

We need to verify various properties of the construction. Let $[k] = \langle g_1, \dots, g_{k-1}\rangle$ and $[k]_\sigma = \langle g_1^{\sigma(1)}, \dots, g_{k-1}^{\sigma(k-1)}\rangle$.

Lemma 4.13. *(RCA_0) T is infinite.*

Proof. It suffices to show that for each k there is an element of T of length k. Fix $k > 0$. Since P satisfies Equation (4.1), there is a $\sigma \in \mathrm{Fin}_{\pm 1}$ with $\mathrm{lh}(\sigma) = k$ and

$$\forall x, n, m \ \big(s([k]_\sigma, n, m, x) = 0 \vee x \notin P\big).$$

In particular, this condition holds if we bound the quantifiers by k. From the definition of T, it follows that for all $i \leq k$, $\sigma|_i \in T$ and hence $\sigma \in T$. □

By Weak König's Lemma there is a path h through T. Let

$$h[n] = \langle h(0), \dots, h(n-1)\rangle \ \in \mathrm{Fin}_{\pm 1}$$
$$\tilde{h}[n] = [n]_{h[n]} = \langle g_1^{h(1)}, \dots, g_{n-1}^{h(n-1)}\rangle.$$

Lemma 4.14. *(RCA_0) For any $x \in G \setminus 1_G$, $h(x) = 1 \leftrightarrow h(x^{-1}) = -1$.*

Proof. If $h(x) = h(x^{-1}) = 1$ and k is the maximum of the indices for x and x^{-1} and the values of x and x^{-1} as natural numbers, then $x, x^{-1} \in \tilde{h}[k+1]$. Since $s(\tilde{h}[k+1], 0, 0, x) = 1$ and $s(\tilde{h}[k+1], 0, 0, x^{-1}) = 1$, it follows that $s(\tilde{h}[k+1], 1, k, 1_G) = 1$. But, $1_G \in P$ and so by the construction of T, $h[k+1]$ has no extensions. This statement contradicts the choice of h as a path. The case for $h(x) = h(x^{-1}) = -1$ is similar. □

We are now in a position to define Q and verify that it is a full order extending P.

$$x \in Q \leftrightarrow h(x) = -1$$

Q exists by Δ_1^0 comprehension. It contains 1_G since the only node of length 1 in T is $\langle -1\rangle$ and it is both full and pure by Lemma 4.14.

Claim. $P \subset Q$

Suppose $g_i \in P \setminus 1_G$ and $h(g_i) = 1$. By definition, $g_i \in \tilde{h}[i+1]$ and so $s(\tilde{h}[i+1], 0, 0, g_i) = 1$. As in Lemma 4.14, $s(\tilde{h}[i+1], 0, 0, g_i) = 1$ and $g_i \in P$ contradicts the fact that h is a path.

Claim. Q is closed under multiplication.

Suppose that $a, b \in Q$ and $ab \notin Q$. From Lemma 4.14 and the definition of Q, it follows that $h(a^{-1}) = 1$, $h(b^{-1}) = 1$ and $h(ab) = 1$. For a large enough k, we have $a^{-1}, b^{-1}, ab \in \tilde{h}[k]$ and hence if m is the maximum of the values of $a^{-1}, b^{-1}, ab, b^{-1}$ and a^{-1} as natural numbers and their indices as elements of G, then $s(\tilde{h}[k], 2, m, 1_G) = 1$. Since $1_G \in P$, this statement contradicts the fact that h is a path.

Claim. Q is normal.

Suppose $q \in Q$, $g \in G$ and $gqg^{-1} \notin Q$. As above, $h(q^{-1}) = 1$, $h(gqg^{-1}) = 1$ and there is a k with $q^{-1}, gqg^{-1} \in \tilde{h}[k]$. There is an m such that $s(\tilde{h}[k], 2, m, 1_G)$ since the definition of s yields the normal semigroup. As above, $h[k]$ cannot be on a path. This claim completes the proof that Q is a full order extending P. □

Together Propositions 4.11 and 4.12 show (1) implies (2) in Theorem 4.10. The next step is to show that (3) implies (1) in the theorem.

Proposition 4.15. *(RCA_0) For an abelian group G the following are equivalent:*

1. *Equation* (4.2) *holds.*
2. *G is torsion free.*

Proof.

Case. (1) $\Rightarrow$ (2) :

For a contradiction assume that Equation (4.2) holds and $a \neq 1_G$ is a torsion element of G.

Claim. For all $k \geq 1$, $\exists p[s(\langle a \rangle, k-1, p, a^k) = 1]$.

The claim is proved by Σ^0_1 induction on k. If $k = 1$, then $a \in \langle a \rangle$ implies $s(\langle a \rangle, 0, 0, a) = 1$. For $k+1$, the induction hypothesis states that there are p, p' such that $s(\langle a \rangle, k-1, p, a^k) = 1$ and $s(\langle a \rangle, k-1, p', a) = 1$. If $p'' = \max\{p, p'\}$ then $s(\langle a \rangle, k, p'', a^{k+1}) = 1$, which proves the claim.

If a is a torsion element then for some k, $a^k = (a^{-1})^k = 1_G$. Equation (4.2) for the sequence $\langle a \rangle$ says that either

$$\begin{aligned} &\forall n, m \ \big(s(\langle a \rangle, n, m, 1_G) = 0\big) \\ \text{or} \qquad &\forall n, m \ \big(s(\langle a^{-1} \rangle, n, m, 1_G) = 0\big). \end{aligned}$$

But the claim implies that

$$\begin{aligned} &\exists p \ \big(s(\langle a \rangle, k-1, p, 1_G) = s(\langle a \rangle, k-1, p, a^k) = 1\big) \\ &\exists p \ \big(s(\langle a^{-1} \rangle, k-1, p, 1_G) = s(\langle a^{-1} \rangle, k-1, p, (a^{-1})^k) = 1\big). \end{aligned}$$

Case. (2) $\Rightarrow$ (1)

The first step of this direction is to show that for an abelian group G the normal semigroup generated by $A \in \mathrm{Fin}_G$ is the same as the semigroup generated by A. That is, if $A = \langle a_1, \dots a_n \rangle$ then any element of $S(A)$ can be written as $a_1^{k_1} \cdots a_n^{k_n}$ for some choice of $k_1, \dots k_n \in \mathbb{N}$ with at least one $k_i > 0$. Informally this statement is clear because any subset of an abelian group is normal. However, we need the formal fact that every element can be written in this form. We define a function $\mathrm{prod}(A, \sigma)$ that takes $A = \langle a_1, \dots, a_n \rangle$ and $\sigma = \langle \sigma_1, \dots, \sigma_n \rangle$ to $a_1^{\sigma_1} \cdots a_n^{\sigma_n}$. For $A \in \mathrm{Fin}_A$ and $\sigma \in \mathrm{Fin}_\mathbb{N}$ with $\mathrm{lh}(A) = \mathrm{lh}(\sigma)$, define $\mathrm{prod}(A, \sigma)$ by recursion on $\mathrm{lh}(A)$: $\mathrm{prod}(A, \sigma) = 0$ if $\mathrm{lh}(A) = 0$, $\mathrm{prod}(A, \sigma) = A(0)^{\sigma(0)}$ if $\mathrm{lh}(A) = 1$ and if $\mathrm{lh}(A) > 1$ then

$$\mathrm{prod}(A, \sigma) = \begin{cases} \mathrm{prod}(A', \sigma') \cdot \mathrm{prod}(A'', \sigma'') & \text{if } \mathrm{lh}(\sigma) = \mathrm{lh}(A) \\ 0 & \text{if } \mathrm{lh}(\sigma) \neq \mathrm{lh}(A) \end{cases}$$

where

$$\begin{gathered} \mathrm{lh}(A') = \mathrm{lh}(\sigma') = \mathrm{lh}(A) - 1 \\ \mathrm{lh}(A'') = \mathrm{lh}(\sigma'') = 1 \\ \forall k < \mathrm{lh}(A')[A'(k) = A(k) \wedge \sigma'(k) = \sigma(k)] \\ [A''(0) = A(\mathrm{lh}(A) - 1)] \wedge [\sigma''(0) = \sigma(\mathrm{lh}(\sigma) - 1)]. \end{gathered}$$

There are two lemmas to prove about this formal notation.

Lemma 4.16. *(RCA_0) If $A \in Fin_G$, $\sigma, \tau \in Fin_\mathbb{N}$ and $lh(A) = lh(\sigma) = lh(\tau)$ then*

$$prod(A, \sigma) \cdot prod(A, \tau) = prod(A, \sigma + \tau)$$

where $\sigma + \tau \in Fin_\mathbb{N}$ is defined by $(\sigma + \tau)(k) = \sigma(k) + \tau(k)$.

Proof. This lemma is proved by induction on $\mathrm{lh}(A)$. If $\mathrm{lh}(A) = 1$:

$$\begin{aligned} \mathrm{prod}(A, \sigma) \cdot \mathrm{prod}(A, \tau) &= A(0)^{\sigma(0)} A(0)^{\tau(0)} \\ &= A(0)^{\sigma(0) + \tau(0)} \\ &= \mathrm{prod}(A, \sigma + \tau). \end{aligned}$$

If $\mathrm{lh}(A) > 1$ then we rewrite $\mathrm{prod}(A, \sigma) \cdot \mathrm{prod}(A, \tau)$ as:

$$\begin{aligned} & \mathrm{prod}(A', \sigma') \cdot \mathrm{prod}(A'', \sigma'') \cdot \mathrm{prod}(A', \tau') \cdot \mathrm{prod}(A'', \tau'') \\ = \ & \mathrm{prod}(A', \sigma') \cdot \mathrm{prod}(A', \tau') \cdot \mathrm{prod}(A'', \sigma'') \cdot \mathrm{prod}(A'', \tau'') \\ = \ & \mathrm{prod}(A', \sigma' + \tau') \cdot \mathrm{prod}(A'', \sigma'' + \tau'') \\ = \ & \mathrm{prod}(A, \sigma + \tau). \end{aligned}$$

The second line uses the fact that G is abelian and the third line uses the induction hypothesis. □

Lemma 4.17. *If $A \in Fin_G$, $n \in \mathbb{N}$, $x \in G$ and $\exists m\, [s(A, n, m, x) = 1]$ then there is a $\sigma \in Fin_\mathbb{N}$ with $lh(\sigma) = lh(A)$ and at least one $k < lh(\sigma)$ with $\sigma(k) > 0$ such that $x = prod(A, \sigma)$.*

Proof. This claim is proved by induction on n. For the base case, assume $s(A, 0, m, x) = 1$. Then $x = A(j)$ for some j. Define σ by $\sigma(j) = 1$ and $\sigma(i) = 0$ for $i \neq j$. For the induction case, assume $s(A, n+1, m, x) = 1$ and split into three subcases.

1. If $s(A, n, m, x) = 1$, then we are done by the induction hypothesis.

2. If $x = ab$ with $s(A, n, m, a) = s(A, n, m, b) = 1$, then by the induction hypothesis, $a = \text{prod}(A, \sigma)$ and $b = \text{prod}(A, \tau)$. By Lemma 4.16, $x = \text{prod}(A, \sigma + \tau)$.

3. If $x = gag^{-1}$ with $s(A, n, m, a) = 1$ and $g \leq m$, then since G is abelian, $x = a$. Hence $s(A, n, m, x) = 1$ and the induction hypothesis applies.

□

We can now prove that if G is torsion free abelian then Equation (4.2) holds by Π^0_1 induction on $\text{lh}(A)$.
Base case: We need to show that for each $a \in G \setminus 1_G$ either

$$\begin{aligned} &\forall n, m \; \big(s(\langle a \rangle, n, m, 1_G) = 0\big) \\ \text{or} \qquad &\forall n, m \; \big(s(\langle a^{-1} \rangle, n, m, 1_G) = 0\big). \end{aligned}$$

Suppose that neither equation holds and that $s(\langle a \rangle, n, m, 1_G) = 1$. By Lemma 4.17, $1_G = \text{prod}(\langle a \rangle, \sigma)$ for some σ and $1_G = a^{\sigma(0)}$ by the definition of prod. Therefore a is a torsion element which contradicts the fact that G is torsion free.
Induction step: This case will be presented less formally to avoid an undue amount of notational baggage. Assume Equation (4.2) holds for $\langle a_1, \ldots, a_n \rangle$ and fails for $\langle a_1, \ldots, a_n, b \rangle$. Let $\langle \epsilon_1, \ldots, \epsilon_n \rangle$ be the exponents in Equation (4.2) for $\langle a_1, \ldots, a_n \rangle$. By assumption, there are n_1, m_1, n_2, m_2 such that

$$\begin{aligned} s(\langle a_1^{\epsilon_1}, \ldots, a_n^{\epsilon_n}, b \rangle, n_1, m_1, 1_G) = 1 \\ s(\langle a_1^{\epsilon_1}, \ldots, a_n^{\epsilon_n}, b^{-1} \rangle, n_2, m_2, 1_G) = 1. \end{aligned}$$

By Lemma 4.17, there are $k_1, \ldots, k_{n+1}$ and $l_1, \ldots, l_{n+1}$ such that

$$\begin{aligned} a_1^{\epsilon_1 k_1} \cdots a_n^{\epsilon_n k_n} b^{k_{n+1}} &= 1_G \\ a_1^{\epsilon_1 l_1} \cdots a_n^{\epsilon_n l_n} b^{-l_{n+1}} &= 1_G \end{aligned}$$

which gives

$$a_1^{\epsilon_1 (k_1 l_{n+1} + k_{n+1} l_1)} \cdots a_n^{\epsilon_n (k_n l_{n+1} + k_{n+1} l_n)} = 1_G.$$

This equation contradicts Equation (4.2) for $\langle a_1, \ldots, a_n \rangle$. □

Proposition 4.15 shows that statement (3) in Theorem 4.10 implies that every torsion free abelian group is an O–group. By Theorem 3.3, this statement implies WKL_0. We have now completed the proof of Theorem 4.10.

Chapter 5

Free Groups

There is a well known result in group theory that every group can be written as a quotient of a free group. A similar result holds for ordered groups. For every f.o. group G, there is an f.o. free group F and a convex normal subgroup $N \subseteq F$ such that $G \cong F/N$ by an order preserving isomorphism. It is assumed that F/N has the induced quotient order. Surprisingly, this theorem is provable in RCA_0 and that proof is the main result of this chapter. This result answers an open question from Downey and Kurtz (1986) by showing that the effective version of the theorem holds. There is one technical lemma required to prove the main theorem. We need to know that RCA_0 suffices to show that the free group on two generators is an O-group. In the first section, we assume this fact and show that RCA_0 proves the main theorem. The last two sections are devoted to proving the technical lemma. In Section 2, we introduce ordered rings and a special class of matrices. In Section 3, we use this class of matrices to order the free product of O-groups. As a corollary, we prove that the free group on two generators is an O-group.

5.1 Main Result

The formal definitions and properties of free groups and free products are given in Appendix A. There we show that RCA_0 is strong enough to prove the existence of the set of reduced words and define a group structure on them. In this chapter, we will use the standard mathematical notation for free groups. In general, if $X = \{x_0, x_1, \ldots\}$ is the set of generators of a free group, then Word_X denotes the set of words in X and the elements of the group are written as $x_{i_1}^{n_1} \cdots x_{i_k}^{n_k}$ with $n_i \in \mathbb{Z} \setminus 0$. Here, if $n_i > 0$, then $x_i^{n_i}$ refers to x_i^1 repeated n_i times. If $n_i < 0$, then $x_i^{n_i}$ refers to x_i^{-1} repeated $|n_i|$ times. Using this notation, we prove that every group is isomorphic to the quotient of a free group by a normal subgroup.

Theorem 5.1. *(RCA_0) Every group is the epimorphic image of a free group.*

Proof. Let F be the free group on the generators $X = \{x_0, x_1, \ldots\}$ and suppose G is enumerated as $g_0, g_1, \ldots$. Define a map $\psi : X \to G$ by $x_n \mapsto g_n$ and extend ψ to a map from

$\text{Word}_X \to G$ by sending $x_{i_1}^{n_1} \cdots x_{i_k}^{n_k} \mapsto g_{i_1}^{n_1} \cdots g_{i_k}^{n_k}$. This map respects the equivalence of words and hence restricts to an epimorphism $\tilde{\psi} : F \to G$. This argument can be made formal by using notions similar to the Prod notation from Chapter 4. $\square$

If N is the kernel of $\tilde{\psi}$ then $G \cong F/N$. The main technical facts needed to prove the version of this theorem for f.o. groups are stated as Theorem 5.2 and Corollary 5.3. The proofs of these results will be given in Section 3 of this chapter. Using these tools, we can prove that the free group on a countable number of generators is an O-group. $\mathbb{N}^+$ denotes the set of strictly positive natural numbers.

Theorem 5.2. *(RCA_0) The free product of two O-groups is an O-group.*

Corollary 5.3. *(RCA_0) The free group on two generators is an O-group.*

Lemma 5.4. *(RCA_0) Let F be the free group on the two generators x, y. For each $i \in \mathbb{N}^+$ let $\alpha_i = x^i y^i$.*

1. *The word $\alpha_{i_1}^{n_1} \cdots \alpha_{i_k}^{n_k}$ with $i_{j+1} \neq i_j$, $n_j \in \mathbb{Z} \setminus \{0\}$, and $k > 0$ freely reduces to a word ending in $x^\epsilon y^{i_k}$ if $n_k > 0$ and $y^\epsilon x^{-i_k}$ if $n_k < 0$.*
2. *No product $\alpha_{i_1}^{n_1} \cdots \alpha_{i_k}^{n_k}$ with the above restrictions is the identity element.*

Proof. Assuming the first property holds, there is either an x or a y with a nonzero exponent in the reduced form of $\alpha_{i_1}^{n_1} \cdots \alpha_{i_k}^{n_k}$. Therefore, the second property follows immediately from the first.

The first property is proved by induction on k. If $k = 1$ then

$$\alpha_{i_1}^{n_1} = (x^{i_1} y^{i_1})^{n_1}$$

which satisfies the first property. If $k > 1$, then split into four cases depending on the signs of n_k and n_{k-1}.

Case. $n_k > 0$ and $n_{k-1} > 0$

By the induction hypothesis, $\alpha_{i_1}^{n_1} \cdots \alpha_{i_{k-1}}^{n_{k-1}}$ reduces to a word ending in $x^\epsilon y^{i_{k-1}}$. Thus $\alpha_{i_1}^{n_1} \cdots \alpha_{i_k}^{n_k}$ reduces to a word ending in $x^\epsilon y^{i_{k-1}} (x^{i_k} y^{i_k})^{n_k}$. Since $n_k > 0$, this word ends in $x^{i_k} y^{i_k}$.

Case. $n_k > 0$ and $n_{k-1} < 0$

By the induction hypothesis, $\alpha_{i_1}^{n_1} \cdots \alpha_{i_{k-1}}^{n_{k-1}}$ reduces to a word ending in $y^\epsilon x^{-i_{k-1}}$. Hence $\alpha_{i_1}^{n_1} \cdots \alpha_{i_k}^{n_k}$ reduces to a word ending in $y^\epsilon x^{-i_{k-1}} (x^{i_k} y^{i_k})^{n_k}$. If $n_k = 1$ then we have a word ending in $y^\epsilon x^{i_k - i_{k-1}} y^{i_k}$. By assumption, $i_k - i_{k-1} \neq 0$ so we have satisfied the first property. If $n_k > 1$, then this word ends in $x^{i_k} y^{i_k}$.

Case. $n_k < 0$ and $n_{k-1} < 0$

This case is similar to the first case.

Case. $n_k < 0$ and $n_{k-1} > 0$

This case is similar to the second case. $\square$

Proposition 5.5. *(RCA_0) The free group on a countable number of generators is an O-group.*

Proof. Let F and α_i be as in Lemma 5.4 and let $P(F)$ be the positive cone for some full order on F. Let G be the free group on the generators $x_0, x_1, \ldots$. Define the homomorphism:

$$\psi : G \to F$$
$$x_{i_1}^{n_1} \cdots x_{i_k}^{n_k} \mapsto \alpha_{i_1}^{n_1} \cdots \alpha_{i_k}^{n_k}.$$

If $x_{i_1}^{n_1} \cdots x_{i_k}^{n_k}$ is fully reduced and $x_{i_1}^{n_1} \cdots x_{i_k}^{n_k} \neq 1_G$, then $\alpha_{i_1}^{n_1} \cdots \alpha_{i_k}^{n_k}$ satisfies the hypotheses of the previous lemma. Hence $\alpha_{i_1}^{n_1} \cdots \alpha_{i_k}^{n_k} \neq 1_F$ and so ψ is a monomorphism. The order on G is defined from $P(F)$.

$$P(G) = \{ \ x_{i_1}^{n_1} \cdots x_{i_k}^{n_k} \mid \alpha_{i_1}^{n_1} \cdots \alpha_{i_k}^{n_k} \in P(F) \ \}$$

It is straightforward to verify that $P(G)$ is the positive cone for a full order on G. $\square$

Definition 5.6. (RCA_0) If G_1 and G_2 are p.o. groups, then a map $\psi : G_1 \to G_2$ is called an **o-homomorphism** if ψ is an order preserving homomorphism. If ψ is onto, then ψ is called an **o-epimorphism**.

We can now prove the main result of the chapter. Standard proofs of this result can be found in Fuchs (1963) or Kokorin and Kopytov (1974). These proofs cannot be done in RCA_0. The proof used here comes from Revesz (1986).

Theorem 5.7. *(RCA_0) Any fully ordered group is the o-epimorphic image of a fully ordered free group.*

Proof. Let G be an f.o. group, $P(G)$ be the positive cone of a full order on G, and $g_0, g_1, \ldots$ be an enumeration of G. Let F be the free group on the generators $x_0, x_1, \ldots$ and $P(F)$ be the positive cone of some full order on F. As in Theorem 5.1, define the epimorphism:

$$\varphi : F \to G$$
$$x_{i_1}^{n_1} \cdots x_{i_k}^{n_k} \mapsto g_{i_1}^{n_1} \cdots g_{i_k}^{n_k}.$$

We need to produce a new order $\tilde{P}(F)$ on F under which φ is order preserving. Define the embedding:

$$\psi : F \to G \times F$$
$$a \mapsto \langle \varphi(a), a \rangle.$$

Order $G \times F$ lexicographically:

$$\langle a, b \rangle \in P(G \times F) \leftrightarrow (a \in P(G) \wedge a \neq 1_G) \vee (a = 1_G \wedge b \in P(F)).$$

As in the proofs on direct products from Chapter 3, this set gives a full order on $G \times F$. Since the map $\psi : F \to G \times F$ is a monomorphism, we can use it to define a new order on F:

$$\tilde{P}(F) = \{a \mid \psi(a) \in P(G \times F)\}.$$

All that is left to show is that φ is order preserving under $\tilde{P}(F)$. Rewriting the definition of $\tilde{P}(F)$ we have that:

$$a \in \tilde{P}(F) \leftrightarrow (\varphi(a) \in P(G) \wedge \varphi(a) \neq 1_G) \vee (\varphi(a) = 1_G \wedge a \in P(F)).$$

Let $\leq_F$ be the order corresponding to $\tilde{P}(F)$. Suppose that $a \leq_F b$. It follows that $a^{-1}b \in \tilde{P}(F)$ and hence $\varphi(a^{-1}b) = \varphi(a)^{-1}\varphi(b) \in P(G)$. This calculation shows that $\varphi(a) \leq_G \varphi(b)$. Now, suppose that $c, d \in G$ and $c <_G d$. Since φ is onto, there are $a, b \in F$ with $\varphi(a) = c$ and $\varphi(b) = d$. Since $c <_G d$, we have that $c^{-1}d \in P(G)$ and $c^{-1}d \neq 1_G$. Because $\varphi(a^{-1}b) = c^{-1}d$ and $c^{-1}d \neq 1_G$, we know that $a \neq b$. By the definition of $\tilde{P}(F)$, we have that $a^{-1}b \in \tilde{P}(F)$ and so $a <_F b$. Therefore, φ is an o-epimorphism from F with the order $\tilde{P}(F)$ onto G. □

5.2 Fully Ordered Rings and Triangular Matrices

Definition 5.8. (RCA_0) A **ring** is a set R together with two functions $+_R$, $\cdot_R$ and two constants 0_R, 1_R which satisfy the usual axioms for a commutative ring with identity.

As with groups, the subscripts will be dropped when the context is clear. Notice that we are using the term ring to mean a commutative ring with identity.

Definition 5.9. (RCA_0) A **partially ordered ring (p.o. ring)** is a ring R together with a binary relation $\leq_R$ such that:

1. $(R, \leq_R)$ is a partial order.
2. $a \leq_R b$ implies $a + c \leq_R b + c$ for all $a, b, c \in R$.
3. $a \leq_R b$ and $c >_R 0$ implies $ca \leq_R cb$ and $ac \leq_R bc$.

If $\leq_R$ is linear, then $(R, \leq_R)$ is a **fully ordered ring (f.o. ring)**.

As with a p.o. group, we define the positive and negative cones of a p.o. ring:

$$P = \{r \in R \mid r \geq 0\}$$
$$-P = \{-r \mid r \in P\}.$$

We can verify properties of P similar to those of the positive cone of a p.o. group. For example, $P \cap -P = \{0\}$ and if P is the positive cone for a full order, then $P \cup -P = R$. These are two of the four required properties for a set P to be the positive cone of some full order on

R. The other two defining properties are that $P + P \subseteq P$ and $PP \subseteq P$. RCA_0 is not strong enough to prove that the sets $P + P$ and PP exist. However, RCA_0 is strong enough to show

$$\forall x, y \in R \ (x \in P \wedge y \in P \rightarrow x + y \in P)$$
$$\forall x, y \in R \ (x \in P \wedge y \in P \rightarrow xy \in P).$$

In the context of RCA_0, we take $P + P \subseteq P$ to stand for the top formula and $PP \subseteq P$ to stand for the bottom formula. With this convention, we can state the next theorem in its standard notation.

Theorem 5.10. *(RCA_0) A subset P of a ring R is the positive cone of some partial order on R if and only if the following conditions are satisfied:*

1. $P \cap -P = \{0\}$
2. $P + P \subseteq P$
3. $PP \subseteq P$

Furthermore, P is the positive cone of some full order on R if and only if in addition P satisfies $P \cup -P = R$.

Proof. We have already mentioned that any positive cone satisfies these requirements. Conversely, if P is a set with these properties, then the order can be defined by:

$$a \leq b \leftrightarrow b - a \in P.$$

RCA_0 suffices to verify that this gives an order on R. □

To prove that the free product of two O-groups is an O-group, we will embed the free product into a group of infinite matrices over an f.o. ring. Hence, we need to develop the definitions and the tools to handle such matrices. Given a f.o. ring K, we are interested in upper triangular matrices whose rows and columns are indexed by the elements of $\mathbb{N}^+$. Furthermore, we want the elements along the main diagonal to be positive and invertible. Such a matrix resembles:

$$\begin{pmatrix} k_{11} & k_{12} & k_{13} & k_{14} & \dots \\ 0 & k_{22} & k_{23} & k_{24} & \dots \\ 0 & 0 & k_{33} & k_{34} & \dots \\ \vdots & \vdots & \vdots & \ddots & \ddots \end{pmatrix}$$

where each k_{ii} is in the positive cone of K and has a multiplicative inverse. Obviously there are an uncountable number of such matrices and hence in second order arithmetic, the best we can do is to represent them as a class of functions.

Definition 5.11. (RCA_0) Let $(K, \leq)$ be a fully ordered ring with positive cone P. The function $f : \mathbb{N}^+ \times \mathbb{N}^+ \rightarrow K$ is in the class Tri_K if and only if it satisfies the following conditions:

1. For all $i > j$, $f(i,j) = 0_K$.
2. For all i, $f(i,i) \in P$ and $\exists x \in K(f(i,i) \cdot x = 1_K)$.

The first of these conditions says that the matrices are upper triangular and the second says that the entries along the main diagonal are positive and invertible. We will use $f \in \mathrm{Tri}_K$ as shorthand to mean that f is a function that satisfies these two conditions.

Since our goal is to use this matrix group to order free products, we need to define both an order and a group structure on Tri_K. First we define the order. Given $f, g \in \mathrm{Tri}_K$, we say that $f < g$ if and only if for some pair $\langle i, j \rangle \in \mathbb{N}^+ \times \mathbb{N}^+$ with $i \leq j$ the following two conditions hold:

1. $f(i,j) <_K g(i,j)$.
2. $f(k, k+s) = g(k, k+s)$ for all k, s such that $i + s < j$ or $i + s = j$ and $k < i$.

A pair $\langle i, j \rangle$ for which these conditions hold is called a witness for $f < g$. These conditions are much easier to understand if f and g are viewed as matrices as opposed to as functions. They mean that we compare f and g down the diagonals, starting with the main diagonal, then the diagonal to its right, and so on, until we find the first place that f and g differ. The entries of f and g are compared in the order indicated in this picture:

$$\begin{pmatrix} 1 & \omega & \omega+\omega & \omega+\omega+\omega & \dots \\ \cdot & 2 & \omega+1 & \omega+\omega+1 & \ddots \\ \cdot & \cdot & 3 & \omega+2 & \ddots \\ \cdot & \cdot & \cdot & 4 & \ddots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

From this picture, it is clear that we are comparing f and g by comparing two ordered sequences of elements of K each with order type ω^ω. If $f \neq g$, then the relationship between f and g is determined by the relationship between the elements of K at the first place where these ordered sequences differ. Unfortunately, RCA_0 is not strong enough to prove that ω^ω is well ordered, and so it cannot prove that there is a least place where they differ. In the next section, we will define a countable subgroup of Tri_K for which the order is much easier to determine. For now, our goal is to define the group structure and to prove that the elements of Tri_K satisfy the axioms for a partially ordered group with this order.

Given $f, g \in \mathrm{Tri}_K$, we define the product $f \cdot g$ to be the function:

$$f \cdot g : \mathbb{N}^+ \times \mathbb{N}^+ \to K$$
$$f \cdot g(i,j) = \sum_{n=0}^{\infty} f(i,n) g(n,j).$$

This definition exactly matches the definition for multiplication of infinite matrices. The first thing to check is that this sum converges. By definition, $f(i,n) = 0$ for $n < i$ and $g(n,j) = 0$ for $n > j$. Hence, if n is not between i and j, then $f(i,n)g(n,j) = 0$. This has two consequences. First, if $i > j$, then the sum is 0. Second, if $i \leq j$, then the infinite sum reduces to the finite sum:

$$\sum_{n=i}^{j} f(i,n)g(n,j).$$

Thus, RCA_0 proves that $f \cdot g$ is a well defined function. Furthermore, $f \cdot g(i,i) = f(i,i)g(i,i)$ and so $f \cdot g(i,i)$ is both positive and invertible. Hence, $f \cdot g$ is in Tri_K. The matrix $I \in \text{Tri}_K$ defined by $I(i,i) = 1_K$ and $I(i,j) = 0_K$ for $i \neq j$ plays the role of the identity element in Tri_K.

The next two lemmas show that RCA_0 proves the associativity of the multiplication and the existence of inverses. We prove Lemma 5.12 to give an example of how to work in this formalism, but the proof of Lemma 5.13 is presented in Appendix A.

Lemma 5.12. *(RCA_0)* $(f \cdot g) \cdot h = f \cdot (g \cdot h)$

Proof. For $j < i$, both of these products have the value 0. For $i \leq j$, we perform two computations.

$$\begin{aligned}
\Big((f \cdot g) \cdot h\Big)(i,j) &= \sum_{m=i}^{j} (f \cdot g)(i,m)\, h(m,j) \\
&= \sum_{m=i}^{j} \sum_{n=i}^{m} f(i,n)g(n,m)h(m,j) \\
&= \sum_{i \leq n \leq m \leq j} f(i,n)g(n,m)h(m,j)
\end{aligned}$$

$$\begin{aligned}
\Big(f \cdot (g \cdot h)\Big)(i,j) &= \sum_{n=i}^{j} f(i,n)\, (g \cdot h)(n,j) \\
&= \sum_{n=i}^{j} \sum_{m=n}^{j} f(i,n)g(n,m)h(m,j) \\
&= \sum_{i \leq n \leq m \leq j} f(i,n)g(n,m)h(m,j)
\end{aligned}$$

□

Lemma 5.13. *(RCA_0) If $f \in Tri_K$, then f has an inverse $g \in Tri_K$, in the sense that $f \cdot g = g \cdot f = I$, given by:*

$$g(i,j) = \begin{cases} 0 & j < i \\ f(i,j)^{-1} & i = j \\ -\frac{f(i,j)}{f(i,i)f(j,j)} + \sum_{i<k_1<j} \frac{f(i,k_1)f(k_1,j)}{f(i,i)f(k_1,k_1),f(j,j)} - \\ \quad -\sum_{i<k_1<k_2<j} \frac{f(i,k_1)f(k_1,k_2)f(k_2,j)}{f(i,i)f(k_1,k_1)f(k_2,k_2)f(j,j)} + \cdots & i < j \\ \quad \cdots + (-1)^{j-i} \frac{f(i,i+1)\cdots f(j-1,j)}{f(i,i)f(i+1,i+1)\cdots f(j,j)} \end{cases}$$

Since $f(n,n)$ is invertible, we write it in the denominator of a fraction as shorthand for $f(n,n)^{-1}$.

Now that we have both a group structure and an order on Tri_K, we need to check that they interact as in an ordered group. Instead of verifying directly that the functions in Tri_K satisfy properties similar to the axioms for a partially ordered group, we give a condition for elements of Tri_K to be in the positive cone and verify that these functions satisfy the appropriate properties. If $f \in \mathrm{Tri}_K$, we say $f \in P(\mathrm{Tri}_K)$ if and only if $f = I$ or $I < f$ in the order given above. If $f \neq I$ this is equivalent to either

$$\exists i \ [f(i,i) > 1 \wedge \forall j < i(f(j,j) = 1)]$$

or

$$\forall i \ (f(i,i) = 1) \ \wedge \ \exists i,j \ \Big(\ i < j \wedge f(i,j) > 0 \ \wedge$$
$$\wedge \ \forall k \ \forall s > 0 \ \big((i + s < j \vee (i + s = j \wedge k < i)) \to f(k, k+s) = 0\big) \Big).$$

Lemma 5.14. *(RCA_0)*

1. *If $f, g \in P(Tri_K)$ then $f \cdot g \in P(Tri_K)$*
2. *If $f \in P(Tri_K)$ and $f \neq I$ then $f^{-1} \notin P(Tri_K)$*
3. *If $f \in P(Tri_K)$ and $g \in Tri_K$ then $gfg^{-1} \in P(Tri_K)$*

One requirement for a fully ordered group is missing: for each $f \in \mathrm{Tri}_K$, either $f \in P(\mathrm{Tri}_K)$ or $f^{-1} \in P(\mathrm{Tri}_K)$. This requirement in fact holds, but it is not provable in RCA_0. All that we will need for the next section, however, is that the conditions in the lemma are satisfied. There is a proof of Lemma 5.14 in Appendix A.

5.3 Free Products of O-Groups

In this section we prove Theorem 5.2. The proof has several steps, so we outline them here. Given two fully ordered groups A, B, we form a larger group, C, of which A and B are direct summands. We take the group ring $\mathbb{Q}[C]$ and use the orders on A and B to fully order $\mathbb{Q}[C]$. Using the definitions introduced in the previous section, we form the ordered matrix group $\mathrm{Tri}_{\mathbb{Q}[C]}$. The free product $A * B$ can be embedded in $\mathrm{Tri}_{\mathbb{Q}[C]}$ and we examine this embedding in detail. The order on $A * B$ is defined using the properties of $\mathrm{Tri}_{\mathbb{Q}[C]}$ proved in the previous section.

Let A and B be fully ordered groups. We first define a larger ordered group C. For each pair $\langle i, j\rangle \in \mathbb{N}^+ \times \mathbb{N}^+$, let x_{ij} and y_{ij} generate copies of $\mathbb{Z}$ ordered such that x_{ij}^n and y_{ij}^n are positive if and only if $n \geq 0$. For each $i \in \mathbb{N}^+$, let u_i and v_i generate copies of $\mathbb{Z}$ ordered in the same way. The notation $\langle x_{ij}\rangle$ is used for the group generated by x_{ij}, and similarly for $\langle y_{ij}\rangle$, $\langle u_i\rangle$, and $\langle v_i\rangle$.

The group C is defined as the restricted direct product:

$$C = A \times B \times \prod_{i,j=1}^{\infty} \langle x_{ij}\rangle \times \prod_{i,j=1}^{\infty} \langle y_{ij}\rangle \times \prod_{i=1}^{\infty} \langle u_i\rangle \times \prod_{i=1}^{\infty} \langle v_i\rangle.$$

Since there is a uniform order on the factors of C, C can be lexicographically ordered in RCA_0. It is important to realize that C is written multiplicatively instead of additively, even though many of the summands are normally written additively. As a notational convenience, we use x_{ij} to denote the element of C which is the identity in all components of C except the $\langle x_{ij}\rangle$ component and has value x_{ij} in the $\langle x_{ij}\rangle$ component. We abuse notation similarly for $a \in A$, $b \in B$ and the generators u_i, v_i, y_{ij}.

Let $\mathbb{Q}[C]$ be the group ring of C over $\mathbb{Q}$. Formally, the elements of $\mathbb{Q}[C]$ are the finite sums $\sum \alpha_i c_i$ with $\alpha_i \in \mathbb{Q} \setminus \{0\}$, $c_i \in C$ and all the c_i distinct. Addition is defined by:

$$\sum_{i\in I} \alpha_i c_i \;+\; \sum_{j\in J} \beta_j c_j \;=$$
$$\sum_{i\in I\setminus J} \alpha_i c_i \;+\; \sum_{j\in J\setminus I} \beta_j c_j \;+\; \sum_{i\in I\cap J} (\alpha_i + \beta_i) c_i$$

with the stipulation that any terms in the third sum with $\alpha_i + \beta_i = 0$ are removed. Multiplication is defined by:

$$\left(\sum_{i\in I} \alpha_i c_i\right)\left(\sum_{j\in J} \beta_j c_j\right) \;=\; \sum_{i\in I}\sum_{j\in J} (\alpha_i \beta_j) c_i c_j$$

where the terms with the same value from C in this finite sum are collected and any term with coefficient 0 is dropped. The additive identity here is the empty sum $I = \emptyset$, and the multiplicative identity is the sum with one element $1_{\mathbb{Q}} 1_C$. RCA_0 proves that $\mathbb{Q}[C]$ exists.

The next goal is to order $\mathbb{Q}[C]$. The positive cone $P(\mathbb{Q}[C])$ is defined from the order $\leq_C$ on C. The sum $\sum_{i \in I} \alpha_i c_i$ is in $P(\mathbb{Q}[C])$ if and only if $I = \emptyset$ or $\alpha_j >_{\mathbb{Q}} 0$ where j is such that c_j is the $\leq_C$-least element among the c_i with $i \in I$. Since I is finite there is such a $\leq_C$-least element. RCA_0 suffices to prove that this gives a full order on $\mathbb{Q}[C]$.

Now that we have a fully ordered ring, we can use the machinery of the previous section to work with $\mathrm{Tri}_{\mathbb{Q}[C]}$. The goal is to embed $A * B$ into $\mathrm{Tri}_{\mathbb{Q}[C]}$ and then use our formal ordering of $\mathrm{Tri}_{\mathbb{Q}[C]}$ to order $A * B$. The embedding is given by uniformly associating to each element of $A * B$ a function in $\mathrm{Tri}_{\mathbb{Q}[C]}$. To do this we specify four matrices in $\mathrm{Tri}_{\mathbb{Q}[C]}$ and denote them by X, Y, U and V. In the definitions, 0 and 1 refer to the additive and multiplicative identities respectively in $\mathbb{Q}[C]$.

$$X(i,j) = \begin{cases} 1 & i = j \\ 0 & i > j \\ x_{ij} & i < j \end{cases}$$

$$Y(i,j) = \begin{cases} 1 & i = j \\ 0 & i > j \\ y_{ij} & i < j \end{cases}$$

$$U(i,j) = \begin{cases} u_i & i = j \\ 0 & i \neq j \end{cases}$$

$$V(i,j) = \begin{cases} v_i & i = j \\ 0 & i \neq j \end{cases}$$

It is useful to see what these functions look like as matrices.

$$X = \begin{pmatrix} 1 & x_{12} & x_{13} & \dots \\ 0 & 1 & x_{23} & \dots \\ 0 & 0 & 1 & \dots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

$$U = \begin{pmatrix} u_1 & 0 & 0 & \dots \\ 0 & u_2 & 0 & \dots \\ 0 & 0 & u_3 & \dots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

In these definitions, u_i denotes the element of $\mathbb{Q}[C]$ that is represented by the sum with the single element $1_{\mathbb{Q}} u_i$. U is upper triangular and has positive elements on the diagonal since u_i is positive in our order on $\langle u_i \rangle$. Also, since $1_{\mathbb{Q}} u_i \cdot 1_{\mathbb{Q}} u_i^{-1} = 1_{\mathbb{Q}[C]}$, U has invertible elements along the diagonal. This point is where it is important to realize that we are using multiplicative instead of additive notation for the groups. Thus, $U \in \mathrm{Tri}_{\mathbb{Q}[C]}$. Similarly, $X, Y, V \in \mathrm{Tri}_{\mathbb{Q}[C]}$.

These matrices are used to define the embedding in several steps. For each $a \in A$, define $\alpha(a) : \mathbb{N}^+ \times \mathbb{N}^+ \to \mathbb{Q}[C]$ by:

$$\alpha(a)(i,j) = \begin{cases} 1 & i = j \text{ and } i \text{ is odd} \\ a & i = j \text{ and } i \text{ is even} \\ 0 & i \neq j \end{cases}$$

As a matrix, this looks like:

$$\alpha(a) = \begin{pmatrix} 1 & 0 & 0 & \dots \\ 0 & a & 0 & \dots \\ 0 & 0 & 1 & \dots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

As above, 1 stands for $1_{\mathbb{Q}[C]}$ and a denotes the sum with one element $1_{\mathbb{Q}}a$. Regardless of whether a is positive or negative in A, $1_{\mathbb{Q}}a$ is positive in $\mathbb{Q}[C]$ since $1_{\mathbb{Q}} > 0_{\mathbb{Q}}$. Also, a is invertible because

$$(1_{\mathbb{Q}}a)(1_{\mathbb{Q}}a^{-1}) = 1_{\mathbb{Q}}1_C = 1_{\mathbb{Q}[C]}.$$

Hence, $\alpha(a) \in \mathrm{Tri}_{\mathbb{Q}[C]}$.

For each $b \in B$ define $\beta(b) \in \mathrm{Tri}_{\mathbb{Q}[C]}$ similarly:

$$\beta(b)(i,j) = \begin{cases} 1 & i = j \text{ and } i \text{ is odd} \\ b & i = j \text{ and } i \text{ is even} \\ 0 & i \neq j \end{cases}$$

As a matrix, $\beta(b)$ looks just like $\alpha(a)$, except it has b's instead of a's. We define two more maps on each of A and B. For each $a \in A$ define:

$$\alpha'(a) = X^{-1} \cdot \alpha(a) \cdot X$$
$$\alpha''(a) = U^{-1} \cdot \alpha'(a) \cdot U.$$

For each $b \in B$ define:

$$\beta'(b) = Y^{-1} \cdot \beta(b) \cdot Y$$
$$\beta''(b) = V^{-1} \cdot \beta'(b) \cdot V.$$

Later, we will use results from the previous section to produce explicit formulas for the entries in these matrices.

Because RCA_0 proves that $\mathrm{Tri}_{\mathbb{Q}[C]}$ is closed under inverses and products, $\alpha''(a)$ and $\beta''(b)$ are both in $\mathrm{Tri}_{\mathbb{Q}[C]}$. Also, since we have explicit formulas for inverses and products in $\mathrm{Tri}_{\mathbb{Q}[C]}$, $\alpha''(a)$ and $\beta''(b)$ can be given uniformly from A and B. The embedding of $A * B$ into $\mathrm{Tri}_{\mathbb{Q}[C]}$ is given by associating to each word $a_1 b_1 \cdots a_n b_n$ the product $\alpha''(a_1)\beta''(b_1) \cdots \alpha''(a_n)\beta''(b_n)$ in $\mathrm{Tri}_{\mathbb{Q}[C]}$. Notice that the term embedding is being used very loosely here. $\mathrm{Tri}_{\mathbb{Q}[C]}$ is not a set, so the correspondence is really a uniform construction of a function in $\mathrm{Tri}_{\mathbb{Q}[C]}$ for each word over A, B. That said, we will continue to use the term embedding and will use $\gamma(w)$ to denote the element of $\text{Tri}_{\mathbb{Q}[C]}$ which corresponds to the word w.

We need to describe and check the properties of this embedding. If $a \in A$, then from the formula for $\alpha(a)$, it is clear that $\alpha(a)^{-1} = \alpha(a^{-1})$. Examining $\gamma(a)$ reveals

$$\begin{aligned}
\gamma(a)^{-1} &= (U^{-1}X^{-1}\alpha(a)XU)^{-1} \\
&= U^{-1}X^{-1}\alpha(a)^{-1}XU \\
&= U^{-1}X^{-1}\alpha(a^{-1})XU \\
&= \gamma(a^{-1}).
\end{aligned}$$

The same property, $\gamma(b)^{-1} = \gamma(b^{-1})$ holds for $b \in B$. In fact, if $a_1b_1 \cdots a_nb_n$ is any, not necessarily reduced, words over A, B, then

$$\gamma\big((a_1b_1 \cdots a_nb_n)^{-1}\big) = \gamma(a_1b_1 \cdots a_nb_n)^{-1}.$$

This equation shows that for every reduced word $w \in A * B$, $\gamma(w)^{-1} = \gamma(w^{-1})$. It also shows that γ respects the reduction of words and hence is a group homomorphism. If w_1, w_2 are reduced words in $A * B$, then

$$\gamma(w_1w_2) = \gamma(w_1)\gamma(w_2).$$

It is much more important and non trivial to check that γ is one-to-one.

Proposition 5.15. *(RCA_0) If $w_1 \neq w_2$ in $A * B$, then $\gamma(w_1) \neq \gamma(w_2)$ in $Tri_{\mathbb{Q}[C]}$.*

In order to prove this proposition, we need several lemmas. The proofs of these lemmas are presented in Appendix A. Throughout these lemmas a is an arbitrary element of A, b is an arbitrary element of B and w_1, w_2 are arbitrary words in $A * B$. Our first goal is to explore $\alpha'(a)$, and by analogy $\beta'(b)$. Let $f = \alpha(a) \cdot X$ and $g = X^{-1}$. We are interested in deriving formulas for $\alpha'(a) = g \cdot f \in \text{Tri}_{\mathbb{Q}[C]}$. More explicitly, g can be given by: $g(i,i) = 1$, $g(i,j) = 0$ for $i > j$ and for $i < j$:

$$\begin{aligned}
g(i,j) &= -x_{ij} + \sum_{i<k_1<j} x_{ik_1}x_{k_1j} - \\
&- \sum_{i<k_1<k_2<j} x_{ik_1}x_{k_1k_2}x_{k_2j} + \cdots + (-1)^{j-i}(x_{i(i+1)} \cdots x_{(j-1)j}).
\end{aligned}$$

As a matrix, this looks like:

$$g = \begin{pmatrix} 1 & -x_{12} & -x_{13} + x_{12}x_{23} & \dots \\ 0 & 1 & -x_{23} & \dots \\ 0 & 0 & 1 & \dots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

f can be given explicitly by:

$$f(i,j) = \begin{cases} 1 & i = j \ \wedge \ i \text{ is odd} \\ a & i = j \ \wedge \ i \text{ is even} \\ x_{ij} & i < j \ \wedge \ i \text{ is odd} \\ ax_{ij} & i < j \ \wedge \ i \text{ is even} \\ 0 & i > j \end{cases}$$

$$f = \begin{pmatrix} 1 & x_{12} & x_{13} & \dots \\ 0 & a & ax_{23} & \dots \\ 0 & 0 & 1 & \dots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

Lemma 5.16. *(RCA_0)*

$$\alpha'(a)(i,i) = \begin{cases} 1 & i \text{ is odd} \\ a & i \text{ is even} \end{cases}$$

Lemma 5.17. *(RCA_0) If $i < j$ and i, j are both even, then*

$$\begin{aligned} \alpha'(a)(i,j) \;=\; (1-a) \sum_{\substack{n=i+1 \\ n \text{ odd}}}^{j-1} \Bigg(& -x_{in}x_{nj} \;+ \sum_{i<k_1<n} (x_{ik_1}x_{k_1n}x_{nj}) \;- \\ & - \sum_{i<k_1<k_2<n} (x_{ik_1}x_{k_1k_2}x_{k_2n}x_{nj}) \;+ \cdots + (-1)^{n-i} x_{i(i+1)} \cdots x_{(n-1)n}x_{nj} \Bigg) \end{aligned}$$

Lemma 5.18. *(RCA_0) If $i < j$, i is even, and j is odd then*

$$\begin{aligned} \alpha'(a)(i,j) = (1-a)(-x_{ij}) + (1-a) \sum_{\substack{n=i+1 \\ n \text{ even}}}^{j-1} \Bigg(& x_{in}x_{nj} - \sum_{i<k_1<n} (x_{ik_1}x_{k_1n}x_{nj}) \;+ \\ & + \sum_{i<k_1<k_2<n} x_{ik_1}x_{k_1k_2}x_{k_nn}x_{nj} \;- \cdots + (-1)^{n-i} x_{ii+1} \cdots x_{n-1n}x_{nj} \Bigg) \end{aligned}$$

Lemma 5.19. *(RCA_0) If $i < j$ and both i, j are odd then*

$$\begin{aligned} \alpha'(a)(i,j) \;=\; (1-a) \sum_{\substack{n=i+1 \\ n \text{ even}}}^{j-1} \Bigg(& x_{in}x_{nj} \;- \sum_{i<k_1<n} (x_{ik_1}x_{k_1n}x_{nj}) \;+ \\ & + \sum_{i<k_1<k_2<n} (x_{ik_1}x_{k_1k_2}x_{k_2n}x_{nj}) \;+ \cdots + (-1)^{n-i} x_{i(i+1)} \cdots x_{(n-1)n}x_{nj} \Bigg) \end{aligned}$$

Lemma 5.20. *(RCA_0) If $i < j$, i is odd, and j is even then*

$$\alpha'(a)(i,j) = (1-a)(x_{ij}) + (1-a)\sum_{\substack{n=i+1 \\ n\ odd}}^{j-1} \Bigg(-x_{in}x_{nj} + \sum_{i<k_1<n} (x_{ik_1}x_{k_1n}x_{nj}) - \\ - \sum_{i<k_1<k_2<n} x_{ik_1}x_{k_1k_2}x_{k_nn}x_{nj} \ + \cdots + (-1)^{n-i}x_{i(i+1)}\cdots x_{(n-1)n}x_{nj} \Bigg)$$

The same results hold for $\beta'(b)$ with b substituted into the formulas for a. From these formulas, it is clear that if $a = 1_A$ then $\alpha'(a) = I$ in $\mathrm{Tri}_{\mathbb{Q}[C]}$, and similarly for b. Also, if $a \neq 1_A$, then in particular, the diagonal elements of $\alpha'(a)$ are not all 1, so $\alpha'(a) \neq I$. A closer look at these formulas reveals the following lemma.

Lemma 5.21. *(RCA_0) If $a \neq 1_A$ and $b \neq 1_B$ then for any i, j with $i \leq j$, $\alpha'(a) \neq 0$ and $\beta'(b) \neq 0$.*

We are now ready to go back and prove Proposition 5.15.

Proof. To show that $w_1 \neq w_2$ in $A*B$ implies that $\gamma(w_1) \neq \gamma(w_2)$ in $\mathrm{Tri}_{\mathbb{Q}[C]}$, it suffices to show that $\gamma(w) \neq I$ for an arbitrary nonidentity element w. Let $w = a_1b_1\cdots a_tb_t$ be an arbitrary nonidentity word in $A * B$ that is reduced, except that possibly $a_1 = 1_A$ or $b_t = 1_B$. It suffices to show for $i < j$ that $\gamma(w)(i,j) \neq 0$.

The multiplication formula in $\mathrm{Tri}_{\mathbb{Q}[C]}$ extends to the following formula for the product of m functions $f_1, \ldots, f_m$ in $\mathrm{Tri}_{\mathbb{Q}[C]}$: for $i > j$, $f_1 \cdots f_m = 0$ and for $i \leq j$

$$f_1 \cdots f_m(i,j) = \sum_{i \leq k_1 \leq \cdots \leq k_{m-1} \leq j} f_1(i,k_1)f_2(k_1,k_2)\cdots f_m(k_{m-1},j).$$

We consider the case in which $a_1 \neq 1_A$ and $b_t \neq 1_B$. By the extended multiplication formula, if

$$c = \alpha''(a_1)\beta''(b_1)\cdots\alpha''(a_t)\beta''(b_t)$$

then

$$c(i,j) = \sum_{i \leq k_i \leq \cdots \leq k_{2t-1} \leq j} \Bigg(\alpha''(a_1)(i,k_1)\beta''(b_1)(k_1,k_2)\cdots \\ \cdots \alpha''(a_t)(k_{2t-2},k_{2t-1})\beta''(b_t)(k_{2t-1},j) \Bigg).$$

Applying the formulas for multiplication and inverses, we can show that:

$$\alpha''(a)(i,j) = \frac{1}{u_i}\alpha'(a)(i,j)u_j$$
$$\beta''(b)(i,j) = \frac{1}{v_i}\beta'(b)(i,j)v_j.$$

As before, the notation $\frac{1}{u_i}$ stands for u_i^{-1} Putting these formulas together gives us:

$$c(i,j) = \sum_{i \leq k_i \leq \cdots \leq k_{2t-1} \leq j} \Bigg(\frac{u_{k_1}}{u_i} \frac{v_{k_2}}{v_{k_1}} \frac{u_{k_3}}{u_{k_2}} \cdots \frac{v_j}{v_{k_{2t-1}}} \alpha'(a_1)(i,k_1) \cdot$$
$$\cdot \ \beta'(b_1)(k_1,k_2) \cdots \alpha'(a_t)(k_{2t-2},k_{2t-1}) \beta'(k_{2t-1},j) \Bigg).$$

Viewing $c(i,j)$ as a polynomial in $u_i, v_i, 1/u_i$ and $1/v_i$, it is clear that none of the terms in the polynomial cancel. Also, since $\alpha'(a_m)(i,j) \neq 0$, $\beta'(b_m)(i,j) \neq 0$, and any group ring has no zero divisors, none of the terms drop out because they are zero. The remaining cases, $a_1 = 1_A, b_t \neq 1_B$ etc., are similar. Thus $c \neq I$. □

Recall that comparing elements of $\mathrm{Tri}_{\mathbb{Q}[C]}$ involved comparing sequences with order type ω^ω. One of the keys to proving Theorem 5.2 is to show that if $w_1 \neq w_2 \in A*B$ then comparing $\gamma(w_1)$ and $\gamma(w_2)$ requires only comparing sequences of elements of $\mathbb{Q}[C]$ with order type ω.

Definition 5.22. (RCA_0) If $r \in \mathbb{Q}[C]$ then define r^{+n} to be the element of $\mathbb{Q}[C]$ that looks just like r except the subscripts on x_{ij}, y_{ij}, u_i and v_i are all adjusted by $+n$. That is, $x_{ij} \mapsto x_{(i+n)(j+n)}$, $u_i \mapsto u_{i+n}$, etc.

Proposition 5.23. *(RCA_0) If $f \in Tri_{\mathbb{Q}[C]}$ is in the image of γ then*

$$f(1,j)^{+2n} = f(1+2n, j+2n)$$
$$f(2,j)^{+2n} = f(2+2n, j+2n).$$

Definition 5.24. (RCA_0) If the conditions in the conclusion of Proposition 5.23 hold for f, then we say f possesses the **shift property**.

The proof of Proposition 5.23 is broken into several lemmas.

Lemma 5.25. *(RCA_0) If $f, g \in Tri_{\mathbb{Q}[C]}$ possess the shift property, then so does $f \cdot g$.*

Proof. Consider $(f \cdot g)(1,j)$. If $j = 1$, then we have:

$$\begin{aligned} f \cdot g(1+2n, 1+2n) &= f(1+2n,1+2n)g(1+2n,1+2n) \\ &= f(1,1)^{+2n} g(1,1)^{+2n} \\ &= \big(f \cdot g(1,1)\big)^{+2n}. \end{aligned}$$

If $j > 1$ then we have:

$$\begin{aligned} f \cdot g(1+2n, j+2n) &= \sum_{m=1+2n}^{j+2n} f(1+2n, m) g(m, j+2n) \\ &= \sum_{m=1}^{j} f(1+2n, m+2n) g(m+2n, j+2n) \\ &= \sum_{m=1}^{j} f(1,m)^{+2n} g(m,j)^{+2n} \\ &= \sum_{m=1}^{j} \big(f(1,m)g(m,j)\big)^{+2n} = \big(f \cdot g(1,j)\big)^{+2n}. \end{aligned}$$

The cases for $f \cdot g(2, j)$ are similar. □

Lemma 5.26. *(RCA_0) If $a \in A$ then $\alpha'(a)$ and $\alpha'(a^{-1})$ have the shift property.*

Proof. This proof utilizes the formulas which we derived for $\alpha'(a)$. Along the principle diagonal, we have:

$$\alpha'(a) = \begin{cases} 1 & i \text{ is odd} \\ a & i \text{ is even} \end{cases}$$

This satisfies the shift property for the cases $\alpha'(a)(1, 1)$ and $\alpha'(a)(2, 2)$. If $j > 1$ and odd, then using our formulas:

$$\begin{aligned} \alpha'(a)(1,j) &= (1-a) \sum_{\substack{m=2 \\ \text{m even}}}^{j-1} \Bigg(x_{1m}x_{mj} - \sum_{1<k_1<m} (x_{1k_1}x_{k_1m}x_{mj}) + \\ &\quad + \sum_{1<k_1<k_2<m} (x_{1k_1}x_{k_1k_2}x_{k_2m}x_{mj}) + \cdots + (-1)^{m-1} x_{12} \cdots x_{m-1m}x_{mj} \Bigg). \end{aligned}$$

When we write the formula for $\alpha'(a)(1 + 2n, j + 2n)$ instead of letting m range from $2 + 2n$ to $j - 1 + 2n$, we let it range from 2 to $j - 1$ and adjust the subscripts inside the sum.

$$\begin{aligned} \alpha'(a)(1+2n, j+2n) &= (1-a) \sum_{\substack{m=2 \\ \text{m even}}}^{j-1} \Bigg(x_{(1+2n)(m+2n)}x_{(m+2n)(j+2n)} - \\ &\quad - \sum_{1<k_1<m} (x_{(1+2n)(k_1+2n)}x_{(k_1+2n)(m+2n)}x_{(m+2n)(j+2n)}) + \cdots \\ &\quad + \cdots (-1)^{m+2n-(1+2n)} (x_{(1+2n)(1+2n+1)} \cdots x_{(m+2n)(j+2n)}) \Bigg) \end{aligned}$$

Once you observe that $m + 2n - (1 + 2n) = m - 1$, it is clear that these two sums can be obtained from one another by a shift in the indices of $+2n$. The other cases follow similarly using the formulas for $\alpha'(a)$ and $\alpha'(a^{-1})$. □

Lemma 5.27. *(RCA_0) If $a \in A$ then $\alpha''(a)$ and $\alpha''(a^{-1})$ have the shift property.*

Proof. This follows from the fact that

$$\alpha''(a)(i,j) = \frac{u_j}{u_i}\alpha'(a)(i,j)$$

We have

$$\begin{aligned} \alpha''(a)(i+2n, j+2n) &= \frac{u_{j+2n}}{u_{i+2n}}\alpha'(a)(i+2n, j+2n) && (5.1)\\ &= \frac{u_{j+2n}}{u_{i+2n}}\alpha'(a)(i,j)^{+2n} && (5.2)\\ &= \alpha''(a)(i,j)^{+2n}. && (5.3)\end{aligned}$$

The case for $\alpha''(a^{-1})$ is similar. □

Lemma 5.28. *(RCA_0) If $b \in B$ then $\beta'(b), \beta'(b^{-1}), \beta''(b)$ and $\beta''(b^{-1})$ have the shift property.*

Proof. The proof is the same as for $\alpha'(a)$ and $\alpha''(a)$. □

We can now prove Proposition 5.23.

Proof. By assumption $\gamma(w) = f$ for some $w \in A * B$. From the facts that w is a word over A and B, that $\gamma(a), \gamma(a^{-1}), \gamma(b)$ and $\gamma(b^{-1})$ have the shift property for all $a \in A$ and $b \in B$, and that the shift property is preserved under multiplication, it follows that f has the shift property. □

It remains to show how to pull the order on $\mathrm{Tri}_{\mathbb{Q}[C]}$ back to $A*B$. Suppose that $f \in \mathrm{Tri}_{\mathbb{Q}[C]}$, $f \neq I$, and f has the shift property. Since $f \neq I$, there is some pair $\langle i,j\rangle$ such that $f(i,j) \neq I(i,j)$. In order to tell if $f \in P(\mathrm{Tri}_{\mathbb{Q}[C]})$ we need to look down the diagonals until we find the first such pair. However, because f has the shift property, if f and I agree on the first two entries in any diagonal, they will agree on all entries in that diagonal. Comparing f and I is now easy. Thinking of them as matrices, we compare the entries in the following order:

$$\begin{pmatrix} 1 & 3 & 5 & 7 & & \dots \\ \cdot & 2 & 4 & 6 & & \dots \\ \multicolumn{6}{c}{--\,irrelevent\,--} \\ \vdots & \vdots & \vdots & \vdots & & \vdots \end{pmatrix}$$

We only need to search through a sequence of elements with order type ω. If we know that $f \neq I$ then we can find the first place they differ in this sequence. We finally show how to define $P(A * B)$ from $P(\mathrm{Tri}_{\mathbb{Q}[C]})$.

$$P(A*B) = \{\langle\rangle\} \cup \{x \in A*B \mid x \neq 1_{A*B} \wedge \gamma(x) \in P(\mathrm{Tri}_{\mathbb{Q}[C]})\}$$

RCA_0 proves the existence of this set because for any $x \neq 1_{A*B}$, we know that $\gamma(x) \neq I$ and $\gamma(x)$ has the shift property. Therefore, RCA_0 proves there is a computable procedure to determine if $\gamma(x) \in P(\mathrm{Tri}_{\mathbb{Q}[C]})$. It remains to show that this set is in fact the positive cone of a full order on $A * B$.

Claim. $P(A * B)$ is closed under multiplication.

Assume $x, y \in P(A * B)$. Since $P(\mathrm{Tri}_{\mathbb{Q}[C]})$ is closed under multiplication and $\gamma(x), \gamma(y) \in P(\mathrm{Tri}_{\mathbb{Q}[C]})$, we have $\gamma(x)\gamma(y) = \gamma(xy) \in P(\mathrm{Tri}_{\mathbb{Q}[C]})$. Also, assuming that at least one of x, y is not 1_{A*B}, then x and y cannot be inverses because $P(\mathrm{Tri}_{\mathbb{Q}[C]})$ is pure. Thus, $\gamma(xy) \in P(\mathrm{Tri}_{\mathbb{Q}[C]})$ implies that $xy \in P(A * B)$ and so $P(A * B)$ is closed under multiplication.

Claim. $P(A * B)$ is pure.

Assume $x \in P(A * B)$ and $x \neq 1_{A*B}$. Since $P(\mathrm{Tri}_{\mathbb{Q}[C]})$ is pure, we have $\gamma(x)^{-1} = \gamma(x^{-1}) \notin P(\mathrm{Tri}_{\mathbb{Q}[C]})$. Therefore, $x^{-1} \notin P(A * B)$, and so $P(A * B)$ is pure.

Claim. $P(A * B)$ is normal.

Assume $x \in P(A * B)$ and $y \in A * B$. Since $\gamma(x) \in P(\mathrm{Tri}_{\mathbb{Q}[C]})$ and $P(\mathrm{Tri}_{\mathbb{Q}[C]})$ is normal,

$$\gamma(y)\gamma(x)\gamma(y)^{-1} = \gamma(yxy^{-1}) \in P(\mathrm{Tri}_{\mathbb{Q}[C]}).$$

Thus, yxy^{-1} is in $P(A * B)$ and $P(A * B)$ is normal.

Claim. $P(A * B)$ is full.

Assume $\gamma(x) \notin P(\mathrm{Tri}_{\mathbb{Q}[C]})$. We need to show that $\gamma(x)^{-1} = \gamma(x^{-1}) \in P(\mathrm{Tri}_{\mathbb{Q}[C]})$. Notice that $\gamma(x) \neq I$. We split this proof into two cases.

Case. Either $\gamma(x)(1,1) \neq 1$ or $\gamma(x)(1,1) = 1$ and $\gamma(x)(2,2) \neq 1$.

Assume that $\gamma(x)(1,1) \neq 1$. The other case is similar. Since $\gamma(x) \notin P(\mathrm{Tri}_{\mathbb{Q}[C]})$ it must be that $\gamma(x)(1,1) < 1$. From the definition of $\gamma(x)^{-1}$:

$$\gamma(x)^{-1}(1,1) = \gamma(x)(1,1)^{-1} > 1.$$

Thus, $\gamma(x^{-1}) \in P(\mathrm{Tri}_{\mathbb{Q}[C]})$.

Case. $\gamma(x)(1,1) = \gamma(x)(2,2) = 1$

Because $\gamma(x)$ has the shift property, there is a least $j > 1$ such that either $\gamma(x)(1,j) \neq 0$ or $\gamma(2,j) \neq 0$ and $\gamma(x)(1,j) = 0$. Assume that $\gamma(x)(1,j) \neq 0$. The other case is similar. Since $\gamma(x) \notin P(\mathrm{Tri}_{\mathbb{Q}[C]})$ it must be that $\gamma(x)(1,j) < 0$. Using the fact that $\gamma(x)(n,n) = 1$ for all n, the formula for $\gamma(x)^{-1}(1,j)$ gives:

$$\gamma(x)^{-1}(i,j) = -\gamma(x)(1,j) \;+ \sum_{1<k_1<j} \gamma(x)(1,k_1)\gamma(x)(k_1,j) \;- \cdots$$
$$\cdots + (-1)^{j-1}(\gamma(x)(1,2)\cdots\gamma(x)(j-1,j)).$$

All the terms drop out except for the first one because $\gamma(x)(1,k) = 0$ for any $1 < k < j$. Thus, $\gamma(x)^{-1}(1,j) = -\gamma(1,j) > 0$. The check that $\gamma(x)^{-1}(k, k+s) = 0$ for the appropriate k, s is similar.

We have completed the proof of Theorem 5.2.

Chapter 6

Divisible Closures and Hölder's Theorem

Three naturally occurring notions of closure in algebra are the algebraic closure of a field, the real closure of an ordered field and the divisible closure of an abelian group. In this chapter, a survey of results on these closure operations is presented along with a proof in RCA_0 of Hölder's Theorem.

6.1 Introduction

Friedman et al. (1983) give definitions for algebraic, real and divisible closures in RCA_0.

Definition 6.1. (RCA_0) A **field** is a set $K \subseteq \mathbb{N}$ together with two binary operations, $+_K, \cdot_K$, a unary operation, $-_K$, and two constants, $0_K, 1_K$ which obey the standard field axioms (see Hungerford (1974)).

If K is a field, then the polynomial ring $K[x]$ is given by

$$\{ \sigma \in \mathrm{Fin}_K \mid \sigma(\mathrm{lh}(\sigma) - 1) \neq 0_G \}.$$

Intuitively, $\langle k_0, \ldots, k_n \rangle$ represents the polynomial

$$k_0 + k_1 x + \ldots + k_n x^n.$$

The restriction that the last element of σ not be 0_G insures that each polynomial has a unique sequence representative. Addition and multiplication of sequences are defined to mimic the corresponding operation on polynomials. If $f \in K[x]$ and $a \in K$, then $f(a) \in K$ is the element

$$k_0 + k_1 a + k_2 a^2 + \ldots + k_n a^n.$$

$f \in K[x]$ is nonconstant if $\mathrm{lh}(f) > 1$ and a is a root of f if $f(a) = 0_K$. If $f = k_0 + k_1 x \ldots + k_n x^n$ and $h : K \to \tilde{K}$ is a field homomorphism, then $h(f) \in \tilde{K}[x]$ is

$$h(k_0) + h(k_1)x + \ldots + h(k_n)x^n.$$

Definition 6.2. (RCA_0) A field K is **algebraically closed** if every nonconstant polynomial $f(x) \in K[x]$ has a root in K. An **algebraic closure** of a field F consists of a monomorphism $h : F \to K$ where K is an algebraically closed field and for each $a \in K$ there is a nonzero polynomial $f(x) \in F[x]$ such that $h(f)(a) = 0$.

Classically, every field has an algebraic closure which is unique up to isomorphism. There are several question to ask about the computability of the algebraic closure. Is it effective? That is, does every computable field have a computable algebraic closure? Is the uniqueness effective? That is, if a computable field has two computable algebraic closures, is there a computable isomorphism between them? Because the range of the function h is the definition of algebraic closure need not be computable, does every computable field have a computable algebraic closure such that the original field is isomorphic to a computable subfield of the closure?

Rabin (1960) proved that every computable field has a computable algebraic closure. Friedman et al. (1983) used Rabin's idea to show that the existence of an algebraic closure is provable in RCA_0. They also gave precise definitions to address the other two questions.

Definition 6.3. (RCA_0) A field F has a **unique algebraic closure** if whenever $h_i : F \to K_i$, $i = 1, 2$, are two algebraic closures of F, there exists an isomorphism $k : K_1 \to K_2$ such that $k(h_1(a)) = h_2(a)$ for all $a \in F$.

Definition 6.4. (RCA_0) Let F be a field. A **strong algebraic closure** of F is an algebraic closure $h : F \to K$ such that h is an isomorphism between F and a subfield of K.

Theorem 6.5 (Friedman et al. (1983)). *(RCA_0)*

1. *Every field has an algebraic closure.*
2. *WKL_0 is equivalent to the statement that every field has a unique algebraic closure.*
3. *ACA_0 is equivalent to the statement that every field has a strong algebraic closure.*

Computationally, this theorem says that computable fields do not necessarily have either a computably unique algebraic closure or a computable strong algebraic closure.

The second type of closure is the real closure of an ordered field. Classically, every formally real field is orderable and every ordered field has a unique real closure. Carrying these notions over into reverse mathematics gives the following definitions and theorems.

Definition 6.6. A field K is **formally real** if K does not contain a finite sequence of nonzero elements $c_0, \ldots, c_n$ such that $c_0^2 + \cdots + c_n^2 = 0$.

Definition 6.7. (RCA_0) An **ordered field** is a field K together with a linear order $\leq_K$ which satisfies the axioms for an ordered field.

Theorem 6.8 (Friedman et al. (1983)). *(RCA_0) The following are equivalent:*

1. *WKL_0*

2. *Every formally real field is orderable.*

Definition 6.9. An ordered field K is **real closed** if for all $g(x) \in K[x]$ and $a < b \in K$ such that $g(a) < 0 < g(b)$, there exists $c \in K$ such that $g(c) = 0$ and $a < c < b$. A **real closure** of an ordered field F consists of a real closed ordered field K and a monomorphism $h : F \to K$ such that for each $b \in K$, there exists a nonconstant polynomial $f(x) \in K[x]$ for which $h(f)(b) = 0$.

The definitions for a strong real closure and a unique real closure are analogous to the same definitions for algebraic closures.

Theorem 6.10 (Friedman et al. (1983)). *(RCA_0)*

1. *Every ordered field has a real closure.*

2. *Every ordered field has a unique real closure.*

3. *ACA_0 is equivalent to the statement that every ordered field has a strong real closure.*

On the computational side, these results show that every computably ordered computable field F has a computably unique computable real closure, but F need not have a computable strong real closure.

The third notion of closure is the divisible closure of an abelian group. Friedman et al. (1983) give the following definitions.

Definition 6.11. (RCA_0) Let D be an abelian group. D is **divisible** if for all $d \in D$ and all $n \geq 1$ there exists a $c \in D$ such that $nc = d$. Here, we are using the additive notation of abelian groups, so nc refers to c added to itself n times.

Definition 6.12. (RCA_0) Let A be an abelian group. A **divisible closure** of A is a divisible abelian group D together with a monomorphism $h : A \to D$ such that for all $d \in D, d \neq 1_D$, there exists $n \in \mathbb{N}$ such that $nd = h(a)$ for some $a \in A, a \neq 1_A$.

Smith (1981) proved that every computable abelian group has a computable divisible closure and that this divisible closure is unique if and only if there is a uniform algorithm which for each prime p decides if an arbitrary element of the original group is divisible by p. Using the ideas in these proofs, Friedman et al. (1983) proved the following theorem.

Theorem 6.13 (Friedman et al. (1983)). *(RCA_0)*

1. *Every abelian group has a divisible closure.*

2. *ACA_0 is equivalent to the statement that every abelian group has a unique divisible closure.*

We will extend these results to strong divisible closures in Section 6.3. Downey and Kurtz (1986) considered another possible extension. They proved that every computably fully ordered computable abelian group has a computably unique divisible closure. An examination of their proof shows that RCA_0 suffices to prove the uniqueness of the divisible closure for fully ordered abelian groups.

Theorem 6.14 (Downey and Kurtz (1986)). *(RCA_0) Every f.o. abelian group G has a f.o. divisible closure $h : G \to D$ such that h is order preserving. This divisible closure is unique up to order preserving isomorphism.*

In Section 6.3, we will consider the strong divisible closure not only for fully ordered groups, but also for the much smaller class of Archimedean fully ordered groups.

Definition 6.15. (RCA_0) If G is an f.o. group, then the **absolute value** of $x \in G$ is given by:

$$|\,x\,| = \max\,\{x, x^{-1}\}$$

Definition 6.16. (RCA_0) If G is an f.o. group, then $a \in G$ is **Archimedean less that** $b \in G$, denoted $a \ll b$, if $|\,a^n\,| < |\,b\,|$ for all $n \in \mathbb{N}$. If there are $n, m \in \mathbb{N}$ such that $|\,a^n\,| \geq |\,b\,|$ and $|\,b^m\,| \geq |\,a\,|$, then a and b are **Archimedean equivalent**, denoted $a \approx b$. The notation $a \lessapprox b$ means $a \approx b \ \vee a \ll b$. G is an **Archimedean fully ordered group** if G is fully ordered and for all $a, b \neq 1_G$, $a \approx b$.

It is not hard to check that $\approx$ is an equivalence relation and that $\ll$ is transitive, antireflexive, and antisymmetric. The next lemma lists several other straightforward properties of $\approx$ and $\ll$. For proofs, see Fuchs (1963).

Lemma 6.17. *(RCA_0) If G is a f.o. group, then the following conditions hold for all $a, b, c \in G$.*

1. *Exactly one of the following holds: $a \ll b$, $b \ll a$, or $a \approx b$.*
2. *$a \ll b$ implies that $xax^{-1} \ll xbx^{-1}$ for all $x \in G$.*
3. *$a \ll b$ and $a \approx c$ imply that $c \ll b$.*
4. *$a \ll b$ and $b \approx c$ imply that $a \ll c$.*

An early conjecture about ordered groups was that the number of full orders of a given O-group was always a power of 2. This conjecture also stated that a group could not have a countable number of orders. Buttsworth (1971) showed part of this conjecture was false by constructing a group with a countably infinite number of orders and Kargapolov et al. (1965) showed it was false for groups with a finite number of orders. Classifying all possible full orders for a given class of O-groups is a harder problem than just counting them. One of the few classes for which this problem has been solved is the class of free abelian groups of finite rank. These results can be found in several places, including Teh (1960). The key ingredient in these results about counting or classifying full orders is Hölder's Theorem. For a more in depth discussion, see either Kokorin and Kopytov (1974) or Mura and Rhemtulla (1977).

Hölder's Theorem states that every f.o. Archimedean group can be embedded in the naturally ordered additive group of the reals. Before examining strong divisible closures, we show that Hölder's Theorem is provable in RCA_0.

6.2 Hölder's Theorem

Because real numbers are given by functions from $\mathbb{N}$ to $\mathbb{Q}$, the first step towards proving Hölder's theorem is to decide what is meant by a subgroup of the real numbers in second order arithmetic.

Definition 6.18. (RCA_0) A **nontrivial subgroup of the additive real numbers** $(\mathbb{R}, +_\mathbb{R})$ is a sequence of reals $A = \langle r_n \mid n \in \mathbb{N} \rangle$ together with a function $+_A : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ and a distinguished number $i \in \mathbb{N}$ such that

1. $r_i = 0_\mathbb{R}$
2. $n +_A m = p$ if and only if $r_n +_\mathbb{R} r_m = r_p$
3. $(\mathbb{N}, +_A)$ satisfies the group axioms with i as the identity element.

Recall that a real number r is a sequence of rationals, $r = \langle q_n | n \in \mathbb{N} \rangle$, such that

$$\forall k \; \forall i \; (\; | \, q_k - q_{k+i} \, | \leq 2^{-k} \;).$$

Thus A is a double indexed sequence of rationals

$$A = \langle \, q_{n,m} \mid n, m \in \mathbb{N} \, \rangle$$

where

$$r_n = \langle \, q_{n,m} \mid m \in \mathbb{N} \, \rangle.$$

Let $(G, \leq)$ be an Archimedean fully ordered group. Because G must be abelian, see Lemma 6.19, we use additive notation for G. The idea of the proof of Hölder's theorem is to pick an element $a \in P(G)$, $a \neq 1_A$, and define the subgroup of $(\mathbb{R}, +)$ by using a to approximate the other elements of G. For now, assume that 2^n divides a in G for all n. That is, assume that for all n there exists $c \in G$ such that $2^n c = a$. To construct the real to which an element $g \neq 1_G$ is sent, we first find $p_0 \in \mathbb{Z}$ such that

$$p_0 \, a \leq g < (p_0 + 1) \, a.$$

Such a p_0 exists by the assumption that G is Archimedean. Next we find p_1 such that

$$p_1 \, \frac{a}{2} \leq g < (p_1 + 1) \, \frac{a}{2}$$

and continue to find p_i such that

$$p_i \frac{a}{2^i} \le g < (n_i + 1)\frac{a}{2^i}.$$

The real corresponding to g will be $\langle p_i/2^i | i \in \mathbb{N}\rangle$. Because the elements $a/2^i$ may not exist, we achieve the same effect by choosing p_i such that

$$p_i\, a \le 2^i\, g < (p_i + 1)\, a.$$

Lemma 6.19. *(RCA_0) Every Archimedean fully ordered group is abelian.*

Proof. The standard proof goes through in RCA_0. For the details, see Kokorin and Kopytov (1974). □

Hölder's Theorem. *(RCA_0) Every nontrivial Archimedean f.o. group is order isomorphic to a nontrivial subgroup of the naturally ordered additive group* $(\mathbb{R}, +)$.

Proof. Let $(G, \le)$ be an Archimedean f.o. group and $g_0, g_1, \ldots$ be an enumeration of G with no repetitions such that $g_0 = 1_G$ and $g_1 \in P(G)$. We construct a subgroup A of $(\mathbb{R}, +)$ by constructing $r_n = \langle\, q_{n,m} \mid m \in \mathbb{N}\,\rangle$ uniformly in n from g_n and g_1. For simplicity of notation, let $a = g_1$. The first two elements of A are

$$r_0 = \langle\, 0 \mid m \in \mathbb{N}\,\rangle$$
$$r_1 = \langle\, 1 \mid m \in \mathbb{N}\,\rangle.$$

To construct r_n for $n > 1$, define $p_{n,m} \in \mathbb{N}$ and $q_{n,m} \in \mathbb{Q}$ by

$$p_{n,m}\, a \le 2^m g_n < (p_{n,m} + 1)\, a$$
$$q_{n,m} = \frac{p_{n,m}}{2^m}.$$

Because G is Archimedean, such $p_{n,m}$ exist and are uniquely determined by the inequality. The real r_n is

$$r_n = \langle\, q_{n,m} \mid m \in \mathbb{N}\,\rangle.$$

It remains to show that $A = \langle\, r_n \mid n \in \mathbb{N}\,\rangle$ is a subgroup of $(\mathbb{R}, +)$ and that the map from G to A that sends g_n to r_n is an order preserving isomorphism.

Claim. Each r_n is a real number.

To prove this claim we must show

$$\forall m\, \forall k\, (\, |\, q_{n,m} - q_{n,m+k}\,| \le 2^{-m}\,).$$

Notice that since

$$p_{n,m}\, a \le 2^m g_n < (p_{n,m} + 1)\, a$$

it follows that

$$2p_{n,m}\,a \leq 2^{m+1}g_n < (2p_{m,n}+2)\,a.$$

Hence, for all m, either $p_{n,m+1} = 2p_{n,m}$, and hence $q_{n,m+1} = q_{n,m}$, or $p_{n,m+1} = 2p_{n,m}+1$, and hence $q_{n,m+1} = q_{n,m} + 1/2^{m+1}$. Thus,

$$|\,q_{n,m} - q_{n,m+k}\,| \;\leq\; \sum_{i=1}^{i=k} \frac{1}{2^{m+i}} \;<\; \frac{1}{2^m}.$$

Claim. If $g_n + g_m = g_k$ then $r_n + r_m = r_k$.

As above, this claim reduces to checking convergence rates. By definition,

$$r_n + r_m = \langle\, q_{n,i+1} + q_{m,i+1} \mid i \in \mathbb{N}\,\rangle.$$

To prove $r_n + r_m = r_k$ we need to show that for every $i \in \mathbb{N}$

$$|\,q_{n,i+1} + q_{m,i+1} - q_{k,i}\,| \;<\; 2^{-i+1}.$$

The definitions of $p_{n,i+1}$ and $p_{m,i+1}$ are

$$p_{n,i+1}\,a \leq 2^{i+1}g_n < (p_{n,i+1}+1)\,a$$
$$p_{m,i+1}\,a \leq 2^{i+1}g_m < (p_{n,i+1}+1)\,a.$$

Adding these two equations together yields

$$(p_{n,i+1} + p_{m,i+1})\,a \leq 2^{i+1}g_k < (p_{n,i+1} + p_{m,i+1} + 2)\,a.$$

Thus $p_{k,i+1}$ is either $p_{n,i+1}+p_{m,i+1}$ or $p_{n,i+1}+p_{m,i+1}+1$. In either case, $q_{k,i+1}-q_{n,i+1}-q_{m,i+1} \leq 2^{-i-1}$ and we have

$$\begin{aligned} |\,q_{n,i+1} + q_{m,i+1} - q_{k,i}\,| &\leq |\,q_{n,i+1} + q_{m,i+1} - q_{k,i+1}\,| + |\,q_{k,i+1} - q_{k,i}\,| \\ &\leq 2^{-i-1} + 2^{-i} \\ &< 2^{-i+1}. \end{aligned}$$

The map that sends g_n to r_n is onto by definition. The following claim implies that it is one-to-one.

Claim. If $n \neq m$, then $r_n \neq r_m$.

To establish $r_n \neq r_m$, we need to find an i such that

$$|\,q_{n,i} - q_{m,i}\,| > 2^{-i+1}.$$

Equivalently, we can find an i such that

$$|\,p_{n,i} - p_{m,i}\,| > 2.$$

Because $n \neq m$ implies $g_n \neq g_m$ assume without loss of generality that $g_n < g_m$. Split into four cases.

Case. $g_n < 1_G \leq g_m$

By the Archimedean property of G there is an i such that

$$2^i\, g_n < -3a < 1_G \leq 2^i\, g_m.$$

It follows that $p_{n,i} < -3$ and $p_{m,i} \geq 0$. Hence $|\, p_{n,i} - p_{m,i}\,| \geq 3$.

Case. $g_n = 1_G < g_m$

There is an i such that

$$1_G < 3a < 2^i\, g_m.$$

It follows that $p_{n,i} = 0$ while $p_{m,i} \geq 3$.

Case. $1_G < g_n < g_m$

Since $1_G < g_m - g_n$, there is an i which yields the following equations:

$$1_G < a < 2^i(g_m - g_n) = 2^i\, g_m - 2^i\, g_n$$
$$2^i\, g_n < a + 2^i\, g_n < 2^i\, g_m$$
$$2^{i+2}\, g_n < 4a + 2^{i+2}\, g_n < 2^{i+2}\, g_m.$$

There is an m such that

$$ma \leq 2^{i+2}\, g_n < (m+1)a.$$

Combining these equations

$$ma \leq 2^{i+1}\, g_n < (m+4)a \leq 4a + 2^{i+2}\, g_n < 2^{i+2}\, g_m.$$

It follows that $p_{n,i+2} = m$ and $p_{m,i+2} \geq m + 4$.

Case. $g_n < g_m < 1_G$

In this case, $1_G < g_m - g_n$ and so the same argument works as in the previous case. This case completes the proof of the claim and shows that the map is one-to-one.

The claims show that A is a subgroup of $(\mathbb{R}, +)$ and that A is isomorphic to G by the map that sends $g_n \mapsto r_n$. Finally, to show that $g_n < g_m$ implies that $r_n < r_m$, notice that from the construction, if $g_n < g_m$ then $q_{n,i} \leq q_{m,i}$ for every i. Thus, $r_n \leq r_m$. But, since $g_n \neq g_m$ implies $r_n \neq r_m$, we have $r_n < r_m$. □

6.3 Strong Divisible Closures

Definition 6.20. (RCA_0) Let A be an abelian group. A **strong divisible closure** of A is a divisible closure $h : A \to D$ such that h is an isomorphism of A onto a subgroup of D. If A is a f.o. group, D is fully ordered and h is order preserving, then we call $h : A \to D$ an f.o. strong divisible closure.

Recall from Theorem 6.14 that RCA_0 suffices to prove the uniqueness of the divisible closure for f.o. abelian groups, but that ACA_0 is required to prove the uniqueness for abelian groups in general. Given these results, it is reasonable to hope that proving the existence of a strong divisible closure would be easier for f.o. abelian group than for abelian groups. The next theorem shows this is not the case.

Theorem 6.21. *(RCA_0) The following are equivalent:*

1. *ACA_0*
2. *Every abelian group has a strong divisible closure.*
3. *Every fully ordered Archimedean group has an f.o. strong divisible closure.*

The idea of proving (3) implies (1) is fairly simple. Let p_k be an enumeration of the primes in increasing order. Given a one-to-one function f, let G be the subgroup of $\mathbb{Q}$ generated by 1 and p^{-k} for each k in the range of f. This group has an Archimedean full order. If D is a strong divisible closure of G, then the image $h(G)$ exists and the range of f can be recovered by

$$\text{range}(f) \; = \; \{ \; k \mid \frac{h(1)}{p_k} \in h(G) \; \}.$$

Lemma 6.22. *(RCA_0) Let p_k enumerate the primes in increasing order. If $k \in \mathbb{Z}$, $j \in \mathbb{N}$ and $\forall i \leq j$ $(0 \leq m_i < p_i)$ then $\sum_{i \leq j} m_i/p_i = k$ implies that $k = 0$ and $m_i = 0$ for all $i \leq j$.*

Proof. For a contradiction, suppose that some $m_i \neq 0$. Notice that $k > 0$ since all $m_i \geq 0$. Let $\hat{p}$ be the product of $p_0, \ldots, p_j$ and $\hat{p}_i$ be $\hat{p}/p_i$. If we multiply the sum by $\hat{p}$ we obtain

$$\sum_{i \leq j} m_i \hat{p}_i \; = \; k\hat{p}.$$

This equation must hold modulo p_i for all $i \leq j$.

$$\left(\sum_{i \leq j} m_i \hat{p}_i \; = \; k\hat{p} \right) \bmod p_i$$

However, if $u \neq i$, then $(m_u \hat{p}_u = 0) \bmod p_i$ because p_i divides $\hat{p}_u$. Therefore, we have

$$\left(\sum_{i \leq j} m_i \hat{p}_i \; = \; m_i \hat{p}_i \right) \bmod p_i.$$

Also, $(k\hat{p} = 0) \bmod p_i$ and so we have

$$(m_i \hat{p}_i = 0) \bmod p_i.$$

It follows that p_i divides m_i. Because $0 \leq m_i < p_i$, m_i must be 0. This argument holds for all $i \leq j$. □

Using Lemma 6.22, we can give a proof of Theorem 6.21.

Proof. (1) implies (2) because ACA_0 is strong enough to show both that the divisible closure exists and that the image of h exists. (2) implies (3) because a full order on D can be defined which makes h order preserving.

$$\begin{aligned} P(D) &= \{ d \in D \mid \exists n > 0 \exists g \in P(G)(nd = h(g)) \} \\ &= \{ d \in D \mid \forall n > 0 \forall g \in P(G)(nd \neq h(g)) \} \end{aligned}$$

Because $P(D)$ has a Δ^0_1 definition, RCA_0 suffices to prove it exists and to verify that it is a full order on D.

To show (3) implies (1), let f be a one-to-one function and let p_k be an enumeration of the primes in increasing order. It suffices to show that the range of f exists. Let G be the group given by the generators a, x_i for $i \in \mathbb{N}$ and the relations $p_{f(i)} x_i = a$. The intuition is that G is isomorphic to a subgroup of $\mathbb{Q}$ with $a \mapsto 1$ and $x_i \mapsto p^{-1}_{f(i)}$. In RCA_0 we can represent elements of G by finite sums:

$$ka + \sum_{i \leq j} m_i \, x_i.$$

where $k \in \mathbb{Z}$, $0 \leq m_i < p_{f(i)}$ and $m_j \neq 0$. Using the relation equations, any element of G can be reduced to one of these finite sums. We need to show that no two of these finite sums represent the same element of G.

Claim. If $ka + \sum_{i \leq j} m_i \, x_i = \tilde{k}a + \sum_{i \leq \tilde{j}} \tilde{m}_i x_i$ then $k = \tilde{k}$, $j = \tilde{j}$ and $\forall i \leq j \ (m_i = \tilde{m}_i)$.

First notice that 1_G has a unique representation as the finite sum $0a$. Indeed, if

$$ka + \sum_{i \leq j} m_i \, x_i = 1_G = 0a$$

then using the relations, we obtain

$$\sum_{i \leq j} m_i \frac{a}{p_{f(i)}} \; = \; -ka.$$

Because G is torsion free, this equation implies

$$\sum_{i \leq j} \frac{m_i}{p_{f(i)}} \; = \; -k.$$

By Lemma 6.22 $k = 0$ and $m_i = 0$. To show that j must equal $\tilde{j}$ as in the claim, suppose that $j < \tilde{j}$ and

$$ka + \sum_{i \leq j} m_i \, x_i = \tilde{k}a + \sum_{i \leq \tilde{j}} \tilde{m}_i x_i.$$

Reducing $(k - \tilde{k})\, a + \sum_{i \le j}(m_i - \tilde{m}_i)x_i$ to $k'a + \sum_{i \le j'} m'_i x_i$, we obtain

$$k'a + \sum_{i \le j'} m'_i x_i + \sum_{j < i < \tilde{j}} \tilde{m}_i x_i = 1_G.$$

Thus, $\tilde{m}_{\tilde{j}} = 0$ which gives the desired contradiction. Hence $j = \tilde{j}$.

A similar argument shows that $m_i = \tilde{m}_i$ for all $i \le j$. Suppose there is an $i \le j$ such that $m_i \ne \tilde{m}_i$. Since we can always subtract off equal terms, we can assume without loss of generality that $m_j \ne \tilde{m}_j$. If

$$(\tilde{k} - k)a \,+ \sum_{i \le j-1} (\tilde{m}_i - m_i)x_i$$

reduces to the normal form

$$k'a \,+ \sum_{i \le j'} m'_i x_i$$

then

$$(\tilde{k} - k)a \,+ \sum_{i \le j} (\tilde{m}_i - m_i)x_i$$

reduces to the normal form

$$k'a \,+ \sum_{i \le j'} m'_i x_i \,+\, (\tilde{m}_j - m_j)x_j = 0_G.$$

By the uniqueness of the normal form for 0_G, we have that $\tilde{m}_j - m_j = 0$, which is a contradiction. Therefore, $\tilde{m}_i = m_i$ for all $i \le j$. Our equation reduces to $ka = \tilde{k}a$ which implies that $k = \tilde{k}$.

Claim. G is fully orderable.

Define the positive cone $P(G)$ by

$$ka \,+ \sum_{i \le j} m_i\, x_i \in P(G) \;\leftrightarrow\; k + \sum_{i \le j} \frac{m_i}{p_{f(i)}} \ge 0.$$

$P(G)$ is normal because G is abelian. To verify the other properties, notice that if there are two finite sums, not necessarily in normal form, that are equivalent under the group relations:

$$ka \,+ \sum_{i \le j} m_i\, x_i \qquad \text{and} \qquad \tilde{k}a \,+ \sum_{i \le \tilde{j}} \tilde{m}_i x_i$$

then:

$$k + \sum_{i \le j} \frac{m_i}{p_{f(i)}} \;=\; \tilde{k} + \sum_{i \le \tilde{j}} \frac{\tilde{m}_i}{p_{f(i)}}.$$

This property is proved by induction on the number of applications of relation equations it takes to transform one sum into the other. This property immediately yields that $P(G)$ is a pure, full semigroup with identity. Furthermore, it shows that G is Archimedean under this order because $\mathbb{Q}$ is Archimedean.

Applying condition (3) from the theorem, we have a divisible closure $h : G \to D$ and the image $h(G)$ exists.

$$X = \{k \mid \frac{h(a)}{p_k} \in h(G)\}$$

$$\begin{aligned}\frac{h(a)}{p_k} \in h(G) &\leftrightarrow p_k \text{ divides } a \text{ in } G \\ &\leftrightarrow \exists i\,(p_k x_i = a) \\ &\leftrightarrow \exists i\,(f(i) = k)\end{aligned}$$

Thus X is the range of f. □

The last issue to discuss before leaving divisible closures is the relationship between the complexity of the full orders on a torsion free abelian group and on its divisible closure. We have already mentioned the following theorem.

Theorem 6.23 (Smith (1981)). *Every computable abelian group has a computable divisible closure.*

Lemma 6.24. *If D is a divisible closure of G, then D is fully orderable if and only if G is fully orderable. Furthermore, each order on G extends uniquely to a full order on D.*

Proof. To prove the first statement, notice that D has torsion elements if and only if G has torsion elements.

Suppose $h : G \to D$ is as in the definition of a divisible closure and P is the positive cone of a full order on G. The second statement claims that $h(P)$ extends uniquely to a full order on D. Consider $d \in D \setminus 1_D$. There exists $n > 0$ and $g \in G \setminus 1_G$ such that $nd = h(g)$. Therefore, if $g \in P$, then $nd \in h(P)$ and so d must be positive. If $g \notin P$, then $g^{-1} \in P$ and so $nd^{-1} \in h(P)$ and d must be negative. Therefore, the unique extension of $h(P)$ to the positive cone of a full order on D is

$$\{d \in D | d = 1_D \vee \big(d \neq 1_D \wedge \exists n > 0 \exists g \in P \setminus 1_G(nd = h(g))\big)\}.$$

□

Proposition 6.25. *Let G be a computable torsion free abelian group and D a computable divisible closure of G. There is a Turing degree preserving bijection ψ from the space of full orders on G to the space of full orders on D.*

$$\psi : \mathbb{X}(G) \to \mathbb{X}(D)$$

Proof. By Lemma 6.24, $\mathbb{X}(G)$ can be mapped bijectively to $\mathbb{X}(D)$ by sending P to its unique extension on D. An examination of the definition of this extension shows that the two orders have the same degree. □

Chapter 7

Order Types

One of the fundamental problems in the theory of ordered groups is to classify all possible orders for various classes of O-groups. In general, this problem is extremely difficult to solve. An easier problem is to classify the possible order types for countable fully ordered groups. Mal'tsev (1949) proved that the order type of a countable f.o. group is $\mathbb{Z}^\alpha\mathbb{Q}^\epsilon$ where $\mathbb{Z}$ denotes the order type of the integers, $\mathbb{Q}$ denotes the order type of the rationals, α is a countable ordinal, and ϵ is either 0 or 1. The goal of this chapter is to prove that this theorem is equivalent over RCA_0 to $\Pi^1_1 - CA_0$.

7.1 Order Type of a Group

The definitions for a linear order and a well order were given in Chapter 1. The definition of a well order X says there are no infinite descending chains in X. In keeping with the notation of set theory, we will use the letters α, β, γ to stand for well orders. If X is a linear order, it is useful to talk about the largest initial segment which is well ordered.

Definition 7.1. (RCA_0) The **well ordered initial segment** of X is defined by

$$W(X) \ = \ \big\{x \in X \mid \neg\exists f : \mathbb{N} \to X\big(f(0) = x \wedge \forall i(f(i+1) < f(i))\big)\big\}.$$

Notice that $W(X)$ need not exist in systems like RCA_0. From the definition it may require $\Pi^1_1 - CA_0$, but the only place we will use it is inside $\Pi^1_1 - CA_0$. It is clear from the definition that if $(W(X), \leq)$ does exist, then it is a well order and that if $y \in W(X)$ and $z \leq y$ then $z \in W(X)$.

Definition 7.2. (RCA_0) Let $(X, \leq_X)$ and $(Y, \leq_Y)$ be linear orders. The product $X \cdot Y$ is the linear order $(Z, \leq_Z)$ where

$$Z = \{\ \langle x, y\rangle \mid x \in X \wedge y \in Y\ \}$$
$$\langle x_1, y_1\rangle \ \leq_Z \ \langle x_2, y_2\rangle \leftrightarrow y_1 <_Y y_2 \vee (y_1 = y_2 \wedge x_1 \leq_X x_2).$$

$X \cdot Y$ is frequently written XY.

We also need a definition of $\mathbb{Z}^X$ for a well order X. In set theoretic terms, $\mathbb{Z}^X$ is given by the set of functions $f : X \to \mathbb{Z}$ with finite support. If $f \neq g$, then $f < g$ if and only if $f(x) <_{\mathbb{Z}} g(x)$ where x is the maximum value of X on which f and g disagree. To represent $\mathbb{Z}^X$ in second order arithmetic, we use finite sequences of pairs $\langle x, z \rangle$ with $x \in X$ and $z \in \mathbb{Z} \setminus 0$. To give a normal form for the sequences, we require that the X-components in each sequence be in decreasing order. By convention, $\mathbb{Z}^\emptyset$ is the single element linear order. Recall that π_1 and π_2 are the projection functions for pairs.

Definition 7.3. (RCA_0) Let X be a non-empty linear order and $Y = X \times (\mathbb{Z} \setminus \{0\})$. $\mathbb{Z}^X$ is given by

$$\{\, x \,|\, x \in \mathrm{Fin}_Y \wedge \forall i < (\mathrm{lh}(x) - 1) \big(\pi_1(x(i)) >_X \pi_1(x(i+1))\big) \,\}.$$

Two elements x, y are equal if and only if they are identical as sequences. If $x \neq y$ and $\mathrm{lh}(x) \leq_{\mathbb{N}} \mathrm{lh}(y)$, then there are two cases to consider.

1. If $x \subset y$ then $x < y \leftrightarrow \pi_2\big(y(\mathrm{lh}(x))\big) > 0$
2. If $x \not\subset y$, let i be the least number such that $x(i) \neq y(i)$ and suppose $x(i) = \langle x_i, u_i \rangle$ and $y(i) = \langle y_i, v_i \rangle$.
   (a) If $x_i <_X y_i$ then $x < y \leftrightarrow v_i > 0$
   (b) If $x_i >_X y_i$ then $x < y \leftrightarrow u_i < 0$
   (c) If $x_i = y_i$ then $x < y \leftrightarrow u_i < v_i$

To see why this definition captures the set theoretic notion, think of each sequence $x \in \mathbb{Z}^X$ as representing the function that sends $\pi_1(x(i))$ to $\pi_2(x(i))$ for all $i < \mathrm{lh}(x)$ and sends all other values in X to 0. In case 1 of the definition, $\pi_1(y(\mathrm{lh}(x)))$ represents the largest value of X on which the functions associated to x and y differ. The function for x sends this element to 0, so $x < y$ if and only if y maps this element to something greater than 0. The other cases have similar explanations.

Definition 7.4. (RCA_0) If G is an f.o. group and X is a linear order, then X is the **order type** of G if there is an order preserving bijection $f : G \to X$.

If $f : G \to X$ and $g : G \to Y$ are two order types of G, then the map $g \circ f^{-1} : X \to Y$ is an order preserving bijection between X and Y. So, in RCA_0 the order type is unique up to order preserving bijection.

To clear up a possibly confusing point of terminology, an order preserving bijection is a bijection between linearly ordered structures that preserves the order, but ignores any other structure they might have. On the other hand, an order isomorphism, or o-isomorphism, is a group isomorphism that preserves order. We can now state the main theorem of this chapter.

Theorem 7.5. *(RCA_0) The following are equivalent:*

1. $\Pi^1_1 - CA_0$

2. *Let G be a countable f.o. group. There is a well order α and $\epsilon = 0$ or 1 such that $\mathbb{Z}^\alpha\mathbb{Q}^\epsilon$ is the order type of G.*

3. *Let G be an abelian countable f.o. group. There is a well order α and $\epsilon = 0$ or 1 such that $\mathbb{Z}^\alpha\mathbb{Q}^\epsilon$ is the order type of G.*

In this section, we prove that (1) implies (2). The idea of the proof is that if G is an f.o. group, then either G has a least strictly positive element or it does not. If G does not have such an element, then it has order type $\mathbb{Q}$. If G does have a least strictly positive element a, then the order type of G is the product of $\mathbb{Z}$ and $G/\langle a\rangle$, where $\langle a\rangle$ is the convex normal subgroup generated by a. This process is repeated with $G/\langle a\rangle$ and continues to be repeated until we have either used up all of G or found a quotient of G which has order type $\mathbb{Q}$. The recursion can be done in ATR_0, but $\Pi^1_1 - CA_0$ is required to prove that the process eventually terminates.

The implication from (2) to (3) is trivial. In the next section, we show that ACA_0 proves that (3) implies (1). First, we prove that RCA_0 plus statement (3) suffices to prove that the well ordered initial segment of every linear order exists. This fact is used together with properties of the Kleene-Brouwer order on trees (which require ACA_0) to prove $\Pi^1_1 - CA_0$ in the form given in Theorem 1.19.

In the last section, we prove that the reversal can be done over RCA_0 instead of ACA_0. We show that any model of RCA_0 and statement (3) is closed under the Turing jump and hence is a model of ACA_0. By Gödel's Completeness Theorem, RCA_0 and statement (3) prove the axioms of ACA_0, which in turn prove $\Pi^1_1 - CA_0$.

Lemma 7.6. *(RCA_0) Let G be an f.o. group and H a convex normal subgroup. If X is the order type of H and Y is the order type of the induced order on G/H, then XY is the order type of G.*

Proof. Since G/H is a set of representatives for the cosets, each element of G can be uniquely written as ah where $a \in G/H$ and $h \in H$. If $g_1 \neq g_2$, $g_1 = a_1h_1$ and $g_2 = a_2h_2$, then by the definition of the induced order $g_1 <_G g_2$ if and only if $a_1 <_{G/H} a_2$ or $a_1 = a_2$ and $h_1 <_G h_2$. Suppose $f_H : H \to X$ and $f_{G/H} : G/H \to Y$ are the order preserving bijections. Define

$$f : G \to XY$$
$$g \mapsto \langle f_H(h), f_{G/H}(a)\rangle$$

where $g = ah$ is the decomposition of g given above. This map is the desired order preserving bijection. □

Definition 7.7. (RCA_0) Let G be an f.o. group. The set Arch(G) is a set of unique representatives of the Archimedean classes of G.

$$\text{Arch}(G) \;=\; \big\{g \in G \mid \forall h \in G \big(h <_{\mathbb{N}} g \to \neg(h \approx g)\big)\big\}$$

In general, RCA_0 is not strong enough to prove the existence of Arch(G). Arch(G) is ordered by taking $x < y$ if and only if $x \ll y$. If Arch(G) exists, then we can define a function $a : G \to \text{Arch}(G)$ which assigns to each g the element in Arch(G) to which it is Archimedean equivalent.

$$\begin{aligned} a(g) = d \;&\Leftrightarrow\; d \in \text{Arch}(G) \wedge d \approx g \\ &\Leftrightarrow\; d \in \text{Arch}(G) \wedge \exists n \exists m \,(|g^m| > |d| \wedge |d^n| > |g|) \\ &\Leftrightarrow\; d \in \text{Arch}(G) \wedge \forall y <_{\mathbb{N}} g \forall n \forall m \,\big(y \neq d \to (|y^m| < |g| \vee |g^n| < |y|)\big) \end{aligned}$$

Since $a(g)$ has a Δ^0_1 definition with Arch(G) as a parameter, it is definable in RCA_0 if Arch(G) exists.

Lemma 7.8. *(RCA_0) Let G be an f.o. group. Suppose Arch(G), $Y = W(\text{Arch}(G))$ and $H = \{\, g \in G \mid \exists y \in Y (g \ll y \vee g \approx y) \,\}$ exist and $Y \neq \text{Arch}(G)$. Then H is a convex normal subgroup of G and G/H has order type $\mathbb{Q}$.*

Proof. H is clearly a convex subgroup. To show H is normal, suppose $h \in H$, $g \in G$ and $ghg^{-1} \notin H$. Let $a \in \text{Arch}(G)$ be such that $a \approx ghg^{-1}$. Because $ghg^{-1} \notin H$, it follows that $a \notin Y$ and there is an infinite descending chain $f : \mathbb{N} \to \text{Arch}(G)$ below a. By Lemma 6.17, $f(n+1) \ll f(n)$ implies $g^{-1}f(n+1)g \ll g^{-1}f(n)g$. Define $\tilde{f} : \mathbb{N} \to \text{Arch}(G)$ by setting $\tilde{f}(n)$ to be the element of Arch(G) which is Archimedean equivalent to $g^{-1}f(n)g$. $\tilde{f}$ is an infinite descending chain below $\tilde{f}(0)$, and so $\tilde{f}(0)$ is not in Y. However, $\tilde{f}(0) = h$ which contradicts the fact that $h \in H$.

Because G is fully ordered, RCA_0 suffices to form G/H with the induced order. To finish the proof, it suffices to show that this order is dense with no endpoints. The key fact is that for any $b \in \text{Arch}(G) \setminus Y$ there is a $c \in \text{Arch}(G) \setminus Y$ such that $c \ll b$. For example, if $1_G H < g_1 H < g_2 H$, then there are $b, c \in \text{Arch}(G) \setminus Y$ such that $g_1 \approx b$ and $c \ll g_1$. Since $h \ll c$ for all $h \in H$ and $g_1 + |c| \ll g_2$, it follows that $(g_1 + |c|)H$ is strictly between $g_1 H$ and $g_2 H$. The other cases showing that G/H is dense and has no endpoints are similar. □

Lemma 7.9. *(ACA_0) Let G be an f.o. group. If G has a least strictly positive element x then $\forall g \in G(gx = xg)$ and the subgroup generated by x is convex.*

Proof. Let P^+ be the set of strictly positive elements of G. Suppose there is a g with $gx \neq xg$. Without loss of generality assume $gx < xg$. It follows that $gxg^{-1} < x$. But, $x \in P^+$ implies $gxg^{-1} \in P^+$ which contradicts the fact that x is the least strictly positive element. The subgroup generated by x has a Σ^0_1 definition, so its existence can be proved in ACA_0. The elements of this subgroups have the form x^n for $n \in \mathbb{Z}$. Suppose there is an $n \in \mathbb{Z}$ and a $c \in G$ such that $x^n < c < x^{n+1}$. It follows that $1_G < cx^{-n} < x$ which contradicts the hypothesis. □

Lemma 7.10. *(RCA_0) Let G be an f.o. group. If G contains elements a_1, a_2 such that $a_1 < a_2$ and $\forall g \big(a_1 \leq g \leq a_2 \to (a_1 = g \vee a_2 = g)\big)$, then G has a least strictly positive element.*

Proof. Let $x = a_2 a_1^{-1}$. $1_G < x$ and if $1_G < b < x$, then $a_1 < ba_1 < a_2$ which contradicts the hypothesis. □

Lemma 7.11. *($\Pi^1_1 - CA_0$) For any linear order X, the well ordered initial segment $W(X)$ exists.*

Proof. For each $a \in X$, let

$$T_a \;=\; \{\,\sigma \in \mathrm{Fin}_X \,|\, \sigma(0) = a \wedge \forall i < (\mathrm{lh}(\sigma) - 1)\ (\sigma(i+1) < \sigma(i))\,\}.$$

T_a has a path if and only if there is an infinite descending chain below a. Hence

$$W(X) \;=\; \{\,a \,|\, T_a \text{ has no path}\,\}.$$

By Theorem 1.19, $\Pi^1_1 - CA_0$ proves that this set exists. □

We are ready to prove that (1) implies (2) in Theorem 7.5.

Proof. Let G be an f.o. group. By Lemma 7.11, $\Pi^1_1 - CA_0$ suffices to prove that $W(\mathrm{Arch}(G))$ exists. Let $X = W(\mathrm{Arch}(G))$ if $W(\mathrm{Arch}(G)$ has a greatest element and otherwise let X be the well ordered obtain by adding a greatest element onto $W(\mathrm{Arch}(G))$. We use ordinal notation for elements of X: 0 denotes the least element of X, $\beta + 1$ denotes the successor of β, and γ is a limit if γ has no immediate predecessor. For any $\beta \in X$, let

$$\hat{\beta} \;=\; \{\,y \in X \,|\, y < \beta\,\}.$$

The strategy is to use ATR_0 to construct a chain of convex normal subgroups, $A_\beta \subseteq G$ for $\beta \in X$. At each step, we prove the order type of A_β is $\mathbb{Z}^{\hat{\beta}}$ and that unless β is the maximal element of X, A_β is strictly contained in G. If we reach a step where A_β cannot be extended to $A_{\beta+1}$, the construction terminates early.
Construction: Define $A_0 \;=\; \{1_G\}$.
Successor Step: Assume A_β is a convex normal subgroup, $A_\beta \neq G$ and the order type of A_β is $\mathbb{Z}^{\hat{\beta}}$. G/A_β is an f.o. group with the induced order. There are two cases to consider:

1. If G/A_β has no least strictly positive element, then terminate the construction early at β. In this case, G/A_β has order type $\mathbb{Q}$.

2. If G/A_β has a least strictly positive element, let $a_{\beta+1} \in G$ represent this least positive coset. Define $A_{\beta+1}$ to be the subgroup generated by A_β and $a_{\beta+1}$.

Limit Step: If λ is a limit ordinal in X, $A_\lambda = \bigcup_{\beta<\lambda} A_\beta$.
End of Construction

We need to verify that at each step of the construction, A_β is a convex normal subgroup with order type $\mathbb{Z}^{\hat{\beta}}$. Consider the successor step $\beta + 1$. Since $a_{\beta+1}A_\beta$ is the least positive element of G/A_β, Lemma 7.9 says that $a_{\beta+1}A_\beta$ is in the center of G/A_β and the subgroup it generates is convex. This fact means that $a_{\beta+1}$ commutes with elements of G modulo A_β. That is, for every g there is an $a \in A_\beta$ such that $ga_{\beta+1} = a_{\beta+1}ga$. Thus any element of $A_{\beta+1}$ can be written in the form $a^n_{\beta+1}b$ for some $n \in \mathbb{Z}$ and $b \in A_\beta$. Also, since A_β is convex and $a_{\beta+1} \notin A_\beta$, $a_{\beta+1}$ is Archimedean greater than all the elements of A_β. We can now verify the following facts:

1. $A_{\beta+1}$ is normal: Let $x = a_{\beta+1}^n b$. Because $a_{\beta+1}$ commutes with elements of G modulo A_β, there is a $\tilde{b} \in A_\beta$ such that

$$gxg^{-1} = ga_{\beta+1}^n bg^{-1} = a_{\beta+1}^n g\tilde{b}bg^{-1}.$$

The fact that A_β is normal implies that $g\tilde{b}bg^{-1} \in A_\beta$ and therefore that $gxg^{-1} \in A_{\beta+1}$.

2. $A_{\beta+1}$ is convex: If $a_{\beta+1}^n b < z < a_{\beta+1}^m \tilde{b}$ then $a_{\beta+1}^n A_\beta \leq zA_\beta \leq a_{\beta+1}^m A_\beta$. Since the subgroup of G/A_β generated by $a_{\beta+1}A_\beta$ is convex, $zA_\beta = a_{\beta+1}^p A_\beta$ for some p. It follows that $z = a_{\beta+1}^p c$ for some $c \in A_\beta$, so $z \in A_{\beta+1}$.

3. The order type of $A_{\beta+1}/A_\beta$ is $\mathbb{Z}$: Elements of $A_{\beta+1}/A_\beta$ are of the form $a_{\beta+1}^n A_\beta$. Since $b \ll a_{\beta+1}$ for all $b \in A_\beta$, it follows that $a_{\beta+1}^n \neq a_{\beta+1}^m$ modulo A_β if $n \neq m$.

4. For all $b \in A_{\beta+1}$, either $b \ll a_{\beta+1}$ or $b \approx a_{\beta+1}$: If $a_{\beta+1} \ll b$, then $a \ll b$ for all $a \in A_\beta$ and so b is not in the subgroup generated by $a_{\beta+1}$ and A_β.

(4) shows that unless $\beta + 1$ is the maximum element of X, $A_{\beta+1} \neq G$. By Lemma 7.6 and the induction hypothesis, (3) shows that the order type of $A_{\beta+1}$ is $\mathbb{Z}^{\widehat{\beta+1}}$.

To check the properties at a limit step, assume λ is a limit in X. From the construction it is clear that A_λ is a convex normal subgroup and that unless λ is the maximum element of X, there are elements of Arch(G) above A_λ, and so $A_\lambda \neq G$. For $\beta < \gamma$ assume $f_\beta : A_\beta \to \mathbb{Z}^{\hat{\beta}}$ is an order preserving bijection. Define

$$\begin{aligned} f_\lambda : A_\lambda &\to \mathbb{Z}^{\hat{\lambda}} \\ a &\mapsto f_\beta(a) \end{aligned}$$

where β is the least element of X such that $a \in A_\beta$. Notice that $\mathbb{Z}^{\hat{\beta}} \subset \mathbb{Z}^{\hat{\lambda}}$, so we can view $f_\beta(a)$ as an element of $\mathbb{Z}^{\hat{\lambda}}$. This map is an order preserving bijection, so A_λ has the desired order type.

Since the construction may have terminated early and W(Arch(G)) may or may not be Arch(G), there are four cases to consider to finish the proof.

1. If $W(\text{Arch}(G)) = \text{Arch}(G)$
   (a) If the construction terminates early at β, then A_β has order type $\mathbb{Z}^{\hat{\beta}}$ and G/A_β has order type $\mathbb{Q}$, so G has order type $\mathbb{Z}^{\hat{\beta}}\mathbb{Q}$.
   (b) If the construction completes and β is the maximum element of X, then $G = A_\beta$ and so G has order type $\mathbb{Z}^{\hat{\beta}}$.

2. If Arch(G) is not well ordered:
   (a) If the construction terminates early at β, then as in the first case, G has order type $\mathbb{Z}^{\hat{\beta}}\mathbb{Q}$

(b) If the construction is completed and β is the maximum element of X, then G/A_β has order type $\mathbb{Q}$ by Lemma 7.8 and G has order type $\mathbb{Z}^{\hat{\beta}}\mathbb{Q}$.

□

7.2 The Reversal

The goal of this section is to show that ACA_0 suffices to prove that (3) implies (1) in Theorem 7.5. The proof takes place in two steps. First, we show that RCA_0 plus statement (3) in Theorem 7.5 suffices to prove the well ordered initial segments of every linear order exists. Second, we use this fact plus some properties of the Kleene-Brouwer order on trees to prove in ACA_0 that (3) implies (1).

Definition 7.12. (RCA_0) For a linear order X, $U \subseteq X$ is **dense** if U has at least two elements and for every $u, v \in U$, if $u <_X v$ then there is a $w \in U$ such that $u <_X w <_X v$.

Lemma 7.13. *(RCA_0) Let X be a well order and U be a dense subset of $\mathbb{Z}^X$. There are sequences of elements of U, $u_0, u_1, \ldots$ and $v_0, v_1, \ldots$ such that for each $n \in \mathbb{N}$*

1. $u_n < u_{n+1} < v_{n+1} < v_n$
2. $lh(u_n) > n$ *and* $lh(v_n) > n$
3. $u_n(0) = v_n(0), u_n(1) = v_n(1), \ldots, u_n(n) = v_n(n)$

Proof. If $X = \emptyset$, then $\mathbb{Z}^X$ has only one element and hence has no dense subsets. Assume that $X \neq \emptyset$ and $U \subseteq \mathbb{Z}^X$ is dense. We define the sequences by induction starting with u_0 and v_0.

Claim. There are $u \neq v$ such that $\pi_1(u(0)) = \pi_1(v(0))$.

Suppose there are no such u and v. We will produce a contradiction to the fact that X is a well order. Since U is infinite, we can pick u and v such that either $\pi_2(u(0))$ and $\pi_2(v(0))$ are both positive or are both negative. Without loss of generality, assume they are both positive and $u <_{\mathbb{Z}^X} v$. Define a function $g : \mathbb{N} \to \mathbb{Z}^X$ such that $g(0) = v$ and $g(i+1)$ is the $\mathbb{N}$-least element of U strictly between u and $g(i)$. The density of U insures that $g(i+1)$ is defined. For any $i \in \mathbb{N}$ we have

$$u <_{\mathbb{Z}^X} g(i+1) <_{\mathbb{Z}^X} g(i) <_{\mathbb{Z}^X} v.$$

We verify that $\pi_1(u(0)) <_X \pi_1(g(i+1)(0))$. Assume that this inequality does not hold. By assumption, $\pi_1(u(0)) \neq \pi_1(g(i+1)(0))$, so we must have $\pi_1(g(i+1)(0)) <_X \pi_1(u(0))$. However, by the definition of $\leq_{\mathbb{Z}^X}$ and because $\pi_2(u(0)) > 0$, this inequality implies that $g(i+1) <_{\mathbb{Z}^X} u$, which is a contradiction.

Because $\pi_1(u(0)) <_X \pi_1(g(i+1)(0))$ and $u <_{\mathbb{Z}^X} g(i+1)$, the definition of $\leq_{\mathbb{Z}^X}$ implies that $\pi_2(g(i+1)(0)) > 0$. Therefore, we can apply the reasoning of the previous paragraph to $g(i+1) <_{\mathbb{Z}^X} g(i)$ and conclude that $\pi_1(g(i+1)(0)) <_X \pi_1(g(i)(0))$. Define the function

$h : \mathbb{N} \to X$ by $h(i) = \pi_1(g(i)(0))$. The properties of g imply that $h(i+1) <_X h(i)$ for all i, which contradicts the fact that X is a well order and proves the claim.

Let $u, v \in U$ be such that $u < v$ and $\pi_1(u(0)) = \pi_1(v(0))$. Let $U_1 = \{x \in U | u \leq x \leq v\}$. U_1 is also a dense subset of X and for any $x \in U_1$, $\pi_1(x(0)) = \pi_1(u(0))$. To finish the $n = 0$ case, it suffices to find $r, s \in U_1$ such that $r \neq s$ and $\pi_2(r(0)) = \pi_2(s(0))$. Suppose there are no such elements. If $r \neq s \in U_1$, then

$$r <_{\mathbb{Z}^X} s \;\Leftrightarrow\; \pi_2(r(0)) < \pi_2(s(0)).$$

However, if $r \in U_1$, then $\pi_2(r(0))$ is between $\pi_2(u(0))$ and $\pi_2(v(0))$. Thus there are a finite number of elements in U_1, which contradicts the density of U_1. Let $\langle u_0, v_0 \rangle$ be the $\mathbb{N}$-least pair of elements of U such that $u_0 < v_0$ and $u_0(0) = v_0(0)$.

The argument for the induction step is similar. Assume we have u_n and v_n. Consider the set V of elements $x \in U$ with $u_n \leq_{\mathbb{Z}^X} x \leq_{\mathbb{Z}^X} v_n$. For any $x \in V$, $x(i) = u_n(i)$ for $0 \leq i \leq n$. By a notationally cumbersome, but similar argument, we can find $r, s \in V$ such that $r \neq s$ and $r(n+1) = s(n+1)$. Let $\langle u_{n+1}, v_{n+1} \rangle$ be the $\mathbb{N}$-least pair in V such that $u_{n+1} < v_{n+1}$ and $u_{n+1}(n+1) = v_{n+1}(n+1)$. □

Lemma 7.14. *(RCA_0) If X is a well order, then there are no dense subsets of $\mathbb{Z}^X$.*

Proof. Suppose X is a well order and U is a dense subset of $\mathbb{Z}^X$. Let $u_0, u_1, \ldots$ and $v_0, v_1, \ldots$ be the sequences from Lemma 7.13. Define $F : \mathbb{N} \to X$ by

$$F(n) = \pi_1(u_n(n)).$$

F is an infinite descending chain which contradicts the fact that X is a well order. □

Proposition 7.15. *(RCA_0) (1) implies (2) where*

1. *For any countable abelian f.o. group A, there is a well order α and $\epsilon = 0$ or 1 such that $\mathbb{Z}^\alpha \mathbb{Q}^\epsilon$ is the order type of A.*
2. *The well ordered initial segment $W(X)$ exists for all linear orders X.*

The proof of Proposition 7.15 follows from the next two lemmas. Let $X = \{x_0, x_1, \ldots\}$ be an infinite linear order and G be the free abelian group on the generators $\{a_0, a_1, \ldots\}$. Elements of G are represented by finite sums,

$$\sum_{i \in I} r_i a_i$$

where I is a finite set and $r_i \in \mathbb{Z} \setminus \{0\}$. For our purposes, it is more convenient to represent the elements of $\mathbb{Z}^X$ as finite sums rather than as sequences

$$\sum_{i \in I} r_i x_i$$

where I is a finite set and $r_i \in \mathbb{Z} \setminus \{0\}$. When G and $\mathbb{Z}^X$ are presented this way, there is a natural bijection between them that sends $\sum_{i \in I} r_i a_i$ to $\sum_{i \in I} r_i x_i$.

X is used to define a full order on G. To compare two distinct elements, $\sum_{i \in I} r_i a_i$ and $\sum_{j \in J} s_j a_j$, let $K = I \cup J$, let $r_k = 0$ for $k \in J \setminus I$ and let $s_k = 0$ for $k \in I \setminus J$. Let n be such that x_n is X-maximal in $\{x_k | k \in K \wedge r_k \neq s_k\}$. The order is defined by

$$\sum_{i \in I} r_i a_i \ < \ \sum_{j \in J} s_j a_j \ \leftrightarrow \ r_n < s_n.$$

This definition yields a full order on G. Furthermore, under this order, the bijection from G to $\mathbb{Z}^X$ is order preserving. Statement (1) in Proposition 7.15 gives an order preserving bijection from G to $\mathbb{Z}^\alpha \mathbb{Q}^\epsilon$ for some well order α and $\epsilon = 0$ or 1.

Lemma 7.16. *X is a well order if and only if $\epsilon = 0$.*

Proof.
Case. ($\Rightarrow$)

Suppose X is a well order. Because there is an order preserving bijection between G and $\mathbb{Z}^X$ and between G and $\mathbb{Z}^\alpha \mathbb{Q}^\epsilon$, it follows that there is an order preserving bijection between $\mathbb{Z}^X$ and $\mathbb{Z}^\alpha \mathbb{Q}^\epsilon$. If $\epsilon = 1$, then the set $\{\langle \ \langle\rangle, q \ \rangle \mid q \in \mathbb{Q}\}$ is dense in $\mathbb{Z}^\alpha \mathbb{Q}$. Because RCA_0 proves that the image of any subset of the domain of a bijection exists, the image of this set exists and is dense in $\mathbb{Z}^X$. This statement contradicts Lemma 7.14.

Case. ($\Leftarrow$)

Suppose X is not a well ordering and $g : \mathbb{N} \to X$ is an infinite descending chain in X. There is an infinite descending chain of generators in G,

$$\ldots \ll a_{g(2)} \ll a_{g(1)} \ll a_{g(0)}.$$

Let H be the subgroup of G generated by $p_n a_{g(n)}$ where p_n is the n^{th} prime.

$$\sum_{i \in I} r_i a_i \in H \ \leftrightarrow \ \forall i \in I \, \exists p_n \leq |r_i| \, (g(n) = i \ \wedge \ p_n \text{ divides } r_i)$$

Because the quantification is bounded, this condition is Σ^0_0. It suffices to show that H is dense, for in that case, the image of H in $\mathbb{Z}^\alpha \mathbb{Q}^\epsilon$ is dense and by Lemma 7.14, ϵ must be 1.

To show H is dense, consider two elements of H,

$$\sum_{i \in I} r_i a_i \ < \ \sum_{j \in J} s_j a_j.$$

Define the coefficients in the sums for all the elements of $I \cup J$ by setting $r_j = 0$ for $j \in J \setminus I$ and $s_i = 0$ for $i \in I \setminus J$. Let n be such that x_n is X-maximal in $\{x_k | k \in K \wedge s_k \neq r_k\}$. n is in the range of g, so there is a k with $g(k) = n$. The element $\sum_{i \in I} r_i a_i \ + \ p_{k+1} a_{g(k+1)}$ lies in H and is strictly between the two elements given above. □

If X is not well ordered, then by Lemma 7.16 G has order type $\mathbb{Z}^\alpha\mathbb{Q}$. Let $f : G \to \mathbb{Z}^\alpha\mathbb{Q}$ be the order preserving bijection. For any $x \in X$, there is an associated generator a_x in G. $f(a_x)$ has two components, one from $\mathbb{Z}^\alpha$ and one from $\mathbb{Q}$. The second component is the key to defining $W(X)$.

Lemma 7.17. *If X is not well ordered, then $x \in X$ is in $W(X)$ if and only if $\pi_2(f(a_x)) = \pi_2(f(1_G))$.*

Proof.

Case. ($\Rightarrow$)

Suppose $x \in W(X)$. Let H be the subgroup generated by a_y for $y \leq_X x$. H exists since its elements are exactly those of the form $\sum_{i\in I} r_i a_i$ where $\forall i \in I(x_i \leq_X x)$.

Claim. H is convex.

Let $\sum_{i\in I} r_i a_i <_G \sum_{j\in J} s_j a_j$ be two elements in H and let $g \in G$ lie strictly between them. $\sum_{i\in I} r_i a_i <_G g$ implies that for all $y >_X x$, the coefficient of a_y in g is greater than or equal to 0. On the other hand, $g <_G \sum_{j\in J} s_j a_j$ implies that for all $y >_X x$, the coefficient of a_y in g is less than or equal to 0. Hence, $g \in H$ as required.

$f(H)$ exists because f is a bijection and $f(H)$ is convex because f is order preserving. Suppose $\pi_2(f(a_x)) \neq \pi_2(f(1_G))$. The contradiction we derive is that $f(H)$ has a dense subordering while H does not.

Define the well order $\hat{X}$ by

$$\hat{X} \;=\; \{\ y \in X \mid y \leq x\ \}.$$

Since H is the torsion free abelian group on the generators a_y with $y \in \hat{X}$, it follows from the definition of $\leq_G$ that the order type of H is $\mathbb{Z}^{\hat{X}}$. Lemma 7.14 shows that H has no dense suborderings.

As for $f(H)$, since $\pi_2(f(a_x)) \neq \pi_2(f(1_G))$ and $1_G \leq_G a_x$, it follows that $\pi_2(f(1_G)) <_\mathbb{Q} \pi_2(f(a_x))$. Thus, for any $q \in \mathbb{Q}$ strictly between these values, $\langle\ \langle\rangle, q\ \rangle$ is strictly between $f(1_G)$ and $f(a_x)$. Since $f(H)$ is convex, the set of such points is in $f(H)$. Thus $f(H)$ has a dense subordering.

Case. ($\Leftarrow$)

This case is similar to the proof of Lemma 7.16. Suppose x is not in the well ordered initial segment of X. Let $g : \mathbb{N} \to X$ be an infinite descending chain below x. This function also gives a descending chain of generators.

$$\ldots \ll a_{g(2)} \ll a_{g(1)} \ll a_{g(0)}$$

Let H be the subgroup of G which is generated by the elements of the form $p_n a_{g(n)}$ for $n \geq 1$. Let P be the positive cone of G. As in the proof of Lemma 7.16, $P \cap H$ exists and is a dense subordering of G. Now, suppose that $\pi_2(f(a_x)) = \pi_2(f(1_G))$. To complete the proof, we show that $f(P \cap H)$ does not have a dense subordering.

Claim. For any $y \in f(H \cap P)$, $\pi_2(y) = \pi_2(f(1_G))$.

Suppose not. If $\pi_2(y) <_{\mathbb{Q}} \pi_2(f(1_G))$ then $y <_{\mathbb{Z}^\alpha\mathbb{Q}} f(1_G)$ and $f^{-1}(y) <_G 1_G$. This contradicts the fact that 1_G is the least element of $f(H \cap P)$. If $\pi_2(f(1_G)) <_{\mathbb{Q}} \pi_2(y)$, then by the similar reasoning and the fact that $\pi_2(f(1_G)) = \pi_2(f(a_x))$ we have that $a_x <_G f^{-1}(y)$. However, since H is generated by $p_n a_{g(n)}$ for $n \geq 1$, any element of H is below a_x.

To show that $f(H \cap P)$ has no dense suborderings, let $\tilde{f} : f(H \cap P) \to \mathbb{Z}^\alpha$ be the map that takes y to $\pi_1(y)$. $\tilde{f}$ is order preserving and one-to-one, but is not necessarily a bijection. However, the range of $\tilde{f}$ is

$$\{ \ z \in \mathbb{Z}^\alpha \mid \langle z, \pi_2(f(1_G))\rangle \ \in f(H \cap P) \ \}.$$

This condition is Σ^0_0, so the range exists. Also, if $U \subseteq f(H \cap P)$ then

$$\tilde{f}(U) \ = \ \{ \ z \in \mathbb{Z}^\alpha \mid \langle z, \pi_2(f(1_G))\rangle \ \in U \ \}.$$

If $U \subseteq f(H \cap P)$ is dense, so is $\tilde{f}(U) \subseteq \mathbb{Z}^\alpha$. Hence, by Lemma 7.14, there are no dense subsets of $f(H \cap P)$ □

We can now give a proof of Proposition 7.15.

Proof. If X is well ordered, then $W(X) = X$. Otherwise, given the definitions above

$$W(X) = \{x \in X \mid \pi_2(f(a_x)) = \pi_2(f(1_G))\}.$$

□

We now define the Kleene-Brouwer order on a tree and use properties of this order to prove the reversal of Theorem 7.5 in ACA_0.

Definition 7.18. (RCA_0) The **Kleene-Brouwer order**, **KB**, on $\mathrm{Fin}_{\mathbb{N}}$ is given by: $\sigma \leq_{KB} \tau$ if and only if $\sigma \supseteq \tau$ or there is a $j < \min(\mathrm{lh}(\sigma), \mathrm{lh}(\tau))$ with $\sigma(j) < \tau(j)$ and $\sigma(i) = \tau(i)$ for all $i < j$. If T is a tree, then $KB(T)$, the Kleene-Brouwer order of T, is $KB \cap (T \times T)$.

Lemma 7.19. *(ACA_0) A tree T has a path if and only if $KB(T)$ is not a well ordering.*

Lemma 7.20. *(ACA_0) In Theorem 7.5, (3) implies (1).*

Proof. Assume (3) and let $\langle T_i \mid i \in \mathbb{N}\rangle$ be a sequence of trees. By Theorem 1.19, it suffices to construct the set

$$\{ \ i \mid T_i \text{ has a path } \}.$$

If none of the T_i's has a path, then RCA_0 can form X. Therefore, assume at least one T_i has a path.

First we define a tree T that contains each T_i as a subtree.

$$T \ = \ \{ \ \langle\rangle \ \} \ \cup \ \{ \ i^\frown\tau \mid \tau \in T_i \ \}$$

T is ordered by the Kleene-Brouwer order, $KB(T)$. Since at least one T_i has a path, T has a path and $KB(T)$ is not a well order. Define A_i by

$$A_i \;=\; \{\, \tau \in T \,|\, \langle i-1 \rangle <_{KB} \tau \leq_{KB} \langle i \rangle \,\}.$$

The map which sends $\tau \in T_i$ to $i^\frown\tau \in T$ is one-one, preserves the tree structure and has image A_i. Thus, T_i and A_i are isomorphic as trees, and $KB(T_i)$ and $KB(T) \cap (A_i \times A_i)$ are isomorphic as linear orders.

By Lemma 7.19, T_i has a path if and only if $KB(T_i)$ is not well ordered, which holds if and only if $KB(T) \cap (A_i \times A_i)$ is not well ordered. Thus it suffices to form the set:

$$\{\, i \,|\, KB(T) \cap (A_i \times A_i) \text{ is not well ordered} \,\}.$$

Let G be the torsion free group on generators the a_τ, $\tau \in T$. Order the generators by $a_\tau \ll a_\gamma$ if and only if $\tau <_{KB} \gamma$. As above, this order of the generators determines a full order on G. By statement (3) in Theorem 7.5, there is an order preserving bijection $f : G \to \mathbb{Z}^\alpha \mathbb{Q}^\epsilon$. Because $KB(T)$ is not a well order, it follows that $\epsilon = 1$.

Claim. If $Y \subseteq T$ and $KB(T) \cap (Y \times Y)$ is well ordered, then there is an order preserving bijection between $\mathbb{Z}^Y$ and the subgroup generated by a_τ with $\tau \in Y$, denoted $\langle a_\tau | \tau \in Y \rangle$.

As shown above, when the elements of $\langle a_\tau | \tau \in Y \rangle$ and $\mathbb{Z}^Y$ are represented as finite sums, there is a natural order preserving bijection between them.

Claim. For each i, $\langle a_\tau | \tau \in A_i \rangle$ has a dense subordering if and only if A_i is not well ordered by $KB(T) \cap (A_i \times A_i)$.

If A_i is well ordered, then by the first claim $\langle a_\tau | \tau \in A_i \rangle$ has no dense suborderings. If A_i is not well ordered, then we can use a descending chain to build a dense subordering as in Lemma 7.16.

Claim. For each $i > 0$, $\langle a_\tau | \tau \in A_i \rangle$ has a dense subordering if and only if $\pi_2(f(a_{\langle i-1 \rangle})) \neq \pi_2(f(a_{\langle i \rangle}))$.

Suppose $\pi_2(f(a_{\langle i-1 \rangle})) \neq \pi_2(f(a_{\langle i \rangle}))$. Then

$$U \;=\; \{\, \gamma \in T \,|\, \pi_2(f(a_{\langle i-1 \rangle})) < \pi_2(f(a_\gamma)) < \pi_2(f(a_{\langle i \rangle})) \,\}$$

is contained in A_i by the definition of the Kleene-Brouwer ordering. Since the elements of T are all actually elements of $\mathbb{N}$ we can trim this set down father.

$$V = \{\, \tau \in U \,|\, \forall \gamma \in U (\gamma <_{\mathbb{N}} \tau \to \pi_2(f(a_\gamma)) \neq \pi_2(f(a_\tau)) \,\}$$

$V \subseteq A_i$ is dense so by the second claim $\langle a_\tau | \tau \in A_i \rangle$ has a dense subordering. To prove the other direction, suppose $\pi_2(f(a_{\langle i-1 \rangle})) = \pi_2(f(a_{\langle i \rangle})) = q$. The image of $\langle a_\tau | \tau \in A_i \rangle$ in $\mathbb{Z}^\alpha \mathbb{Q}$ is contained in $\mathbb{Z}^\alpha \times \{q\}$ which has no dense suborderings.

Similarly, we can show $\langle\ a_\tau | \tau \leq \langle 0 \rangle\ \rangle$ has a dense suborder if and only if $\pi_2(f(a_{\langle 0 \rangle})) \neq \pi_2(f(1_G))$.

For $i > 0$ we have shown $KB(T) \cap (A_i \times A_i)$ is not well ordered if and only if $\pi_2(f(a_{\langle i-1 \rangle})) \neq \pi_2(f(a_{\langle i \rangle}))$. For $i = 0$, $KB(T) \cap (A_0 \times A_0)$ is not well ordered if and only if $\pi_2(f(a_0)) \neq \pi_2(f(1_G))$. These equivalences give us a Σ^0_0 condition to form the set

$$\{ i \mid KB(T) \cap (A_i \times A_i) \text{ is not well ordered} \}.$$

□

7.3 Coding Turing Jumps

This section shows that RCA_0 can prove the implication from (3) to (1) in Theorem 7.5. The idea is that for any given set Y, RCA_0 can produce a linear order X such that the well ordered initial segment of X codes the Turing jump of Y. Thus, by Proposition 7.15, any model of RCA_0 and condition (3) from Theorem 7.5 is closed under Turing jumps and hence is a model for ACA_0. By Gödel's Completeness Theorem, RCA_0 plus condition (3) suffice to prove ACA_0, which in turn proves $\Pi^1_1 - CA_0$. Once we have proved Lemma 7.23, the proof of Theorem 7.5 will be complete.

Definition 7.21. (RCA_0) Let $\pi(e, r, X)$ be a Π^0_1 formula with exactly the displayed variables free. π is **universal lightface $\mathbf{\Pi^0_1}$** if for all Π^0_1 formulas $\psi(e, r, X)$ with the same free variables

$$RCA_0 \vdash \forall e \exists e' \forall r \forall X \left(\pi(e', r, X) \leftrightarrow \psi(e, r, X) \right).$$

Definition 7.22. (RCA_0) Let $\pi(e, r, Y)$ be a fixed universal lightface Π^0_1 formula. The **Turing jump** of Y, $TJ(Y)$, is given by

$$TJ(Y) = \{ \langle e, r \rangle \mid \pi(e, r, Y) \}.$$

Notice that in contrast to the usual definition of the Turing jump as a complete Σ^0_1 set, this definition makes it a complete Π^0_1 set.

Lemma 7.23. *(RCA_0) (1) implies (2):*

1. *Let G be a countable abelian f.o. group. There is a well order α and $\epsilon = 0$ or 1 such that $\mathbb{Z}^\alpha \mathbb{Q}^\epsilon$ is the order type of G.*
2. *ACA_0*

The strategy for building X so that $W(X)$ codes $TJ(Y)$ is to use a marker construction. The function $m(n, t)$ gives the marker for n at stage t. At stage t we will only have markers for $n \leq t$, so $m(n, t) = 0$ for all $n > t$. For this reason, X will order $\mathbb{N}^+$. There is also a function $b(t)$ such that at the end of stage t, X_t will order $1, \dots b(t)$. While the markers may change during the construction, the limit of $m(n, t)$ always exists and

$$n \in TJ(Y) \leftrightarrow \lim_{t \to \infty} m(n, t) \in W(X).$$

To build X we keep track of which elements we know are not in $TJ(Y)$ and which elements we guess may be in $TJ(Y)$. Because the formula $\pi(e, r, Y)$ introduced in the definition of the Turing jump is Π^0_1, it can be written as $\forall x \varphi(e, r, x, Y)$. If we find a number x such that $\neg\varphi(e, r, x, Y)$ then we know $\langle e, r\rangle \notin TJ(Y)$. Once we find such a witness, we begin to build an infinite descending chain below the marker for $\langle e, r\rangle$ so that this marker will not be in $W(X)$.

To keep track of this knowledge, at stage t each number $n < b(t)$ is labeled either not fixed or possibly fixed. A number labeled not fixed will have an infinite descending chain below it when the construction of X is completed. Once a number is labeled not fixed, it remains not fixed forever. However, a possibly fixed number may be changed at a later stage to not fixed. However, as long as a number remains possibly fixed, nothings enters X below it. Thus, at each stage the possibly fixed numbers form an initial segment of the part of X defined so far.

At stage $t + 1$ of the construction, we check if $\neg\varphi(e, r, x, Y)$ holds where $t = \langle e, r, x\rangle$. If it does not hold, then we do not yet have a witness for $\langle e, r\rangle \notin TJ(Y)$. In this case, we want to extend the construction of the infinite descending chain below the not fixed elements and otherwise leave X as it is.

However, if $\neg\varphi(e, r, x, Y)$ and $m(\langle e, r\rangle, t)$ is possibly fixed, then we have found a witness to $\langle e, r\rangle \notin TJ(Y)$ and we did not already know this fact. In this case we label $m(\langle e, r\rangle, t)$ not fixed and begin to build a descending chain below $m(\langle e, r\rangle, t)$. The complication is that there may be other numbers $m(n, t)$ which are possibly fixed and such that $m(\langle e, r\rangle, t) <_X m(n, t)$. We do not want to build a descending chain below $m(n, t)$. To handle this problem, we define the marker $m(n, t + 1)$ to be a new large number, place this number below $m(\langle e, r\rangle, t)$ in X, label the number $m(n, t)$ not fixed since we no longer care about it, and label $m(n, t + 1)$ possibly fixed. This redefinition of markers will happen only finitely often for each n.

We now give the formal construction. X_t denotes the portion of X defined by the end of stage t.

Construction:

Stage 0: Define $m(n, 0) = 0$ for all $n > 0$, $m(0, 0) = 1$, and $b(0) = 1$. X_0 consists of a single element 1 which is labeled possibly fixed.

Stage t+1: By induction, assume the following facts hold at the end of stage t.

1. Each $l \leq b(t)$ except 0 is labeled either not fixed or possibly fixed.
2. The numbers labeled possibly fixed form an initial segment of X_t.
3. If l is not fixed, then either $l \neq m(n, t)$ for any $n \leq t$ or $l = m(n, t)$, $n = \langle e, r\rangle$ and $\exists k \leq t(\neg\varphi(e, r, k, Y))$.
4. If l is possibly fixed then there is an $n \leq t$ such that $l = m(n, t)$.
5. If $m(n, t)$ and $m(\tilde{n}, t)$ are both possibly fixed, then $m(n, t) <_X m(\tilde{n}, t)$ if and only if $n <_{\mathbb{N}} \tilde{n}$.
6. $b(t)$ is the least not fixed element in X_t.

There are two cases to consider in the construction. Assume $t = \langle e, r, x\rangle$.

Case. $\neg\varphi(e, r, x, Y)$ and $m(\langle e, r\rangle, t)$ is possibly fixed.

We have a new witness to the fact that $\langle e, r\rangle \notin TJ(Y)$. Let $n = \langle e, r\rangle$ and suppose X_t looks like

$$\underbrace{m(b_l, t) < \ldots < m(b_1, t) < m(n, t) < m(a_1, t) < \ldots < m(a_k, t)}_{\text{possibly fixed}} \underbrace{< b(t) < \ldots}_{\text{not fixed}}.$$

For all c, define $m(c, t+1)$ as follows. If $c > t+1$, $m(c, t)$ is not fixed, or $m(c, t) \leq_X m(n, t)$, then $m(c, t+1) = m(c, t)$. For the elements $m(a_1, t)$ through $m(a_k, t)$, define $m(a_i, t+1) = b(t)+i$ and define $m(t+1, t+1) = b(t)+k+1$. The numbers $m(a_i, t)$ and $m(n, t) = m(n, t+1)$ have their labels changed to not fixed. The new elements $m(a_i, t+1)$ are labeled possibly fixed and are placed below $m(n, t+1)$, above $m(b_1, t+1)$ and in $\leq_{\mathbb{N}}$-order on the a_i's. The new element $b(t) + k + 1 = m(t+1, t+1)$ is labeled possibly fixed and inserted as the largest possibly fixed element. Finally, the number $b(t) + k + 2$ is labeled not fixed and added to X as the least not fixed element. $b(t+1)$ is set to $b(t) + k + 2$. X_{t+1} looks like

$$\underbrace{m(b_l, t+1) < \ldots m(b_1, t+1) < m(a_1, t+1) < \ldots}_{\text{possibly fixed}}$$
$$\underbrace{\ldots < m(a_k, t+1) < m(t+1, t+1)}_{\text{possibly fixed}} < \underbrace{b(t+1) < m(n, t+1) < \ldots}_{\text{not fixed}}.$$

Case. Either $\varphi(e, r, x, Y)$ or $m(\langle e, r\rangle, t)$ is labeled not fixed.

Define $m(c, t+1) = m(c, t)$ for all c except $c = t+1$, define $m(t+1, t+1) = b(t)+1$ and define $b(t+1) = b(t)+2$. The labels on $n \leq b(t)$ remain the same, $b(t)+1$ is labeled possibly fixed and $b(t)+2 = b(t+1)$ is labeled not fixed. $b(t)+1$ is added to X as the greatest possibly fixed element and $b(t+1)$ is added as the least not fixed element. If X_t had the numbers n_1 and n_2 as the greatest possibly fixed and the least not fixed elements respectively, then X_{t+1} looks like

$$\underbrace{\ldots < n_1 < m(t+1, t+1)}_{\text{possibly fixed}} < \underbrace{b(t+1) < n_2 < \ldots}_{\text{not fixed}}.$$

Notice that in either case, the inductive assumptions are satisfied at the end of stage $t+1$.

End of Construction

The following facts are clear from the construction.

1. If $m(n, t)$ is not fixed, then $\forall t' \geq t\,(m(n, t') = m(n, t))$.

2. If $m(n, t)$ and $m(n', t)$ are possibly fixed, then $m(n, t) <_X m(n', t)$ if and only if $n <_{\mathbb{N}} n'$.

3. If $n \notin TJ(Y)$ and $n = \langle e, r\rangle$, then there is a least $t = \langle e, r, x\rangle$ such that $\neg\varphi(e, r, x, Y)$. The number $m(n, t+1)$ is labeled not fixed at stage $t+1$.

4. If $n \in TJ(Y)$ and $n = \langle e, r \rangle$ then for all $t = \langle e, r, x \rangle$, we have $\varphi(e, r, x, Y)$ and hence $m(n, t)$ is never labeled not fixed at stage $t + 1$. If the number $m(n, t)$ is later labeled not fixed at stage $t' > t$ then $m(n, t') \neq m(n, t)$.

5. If $m(n, t)$ is labeled possibly fixed and $m(a, t) <_X m(n, t)$ with $m(a, t + 1) \neq m(a, t)$, then $m(n, t + 1) \neq m(n, t)$.

It remains to show that $\lim_{t\to\infty} m(n, t)$ exists for all n, that there is an infinite descending chain below $\lim_{t\to\infty} m(n, t)$ in X if and only if $n \notin TJ(Y)$, and that this fact can be used to give a Δ^0_1 definition of $TJ(Y)$.

Lemma 7.24. *(RCA_0) For all n, there exists t such that for all $t' > t$, $m(n, t') = m(n, t)$. That is, $\lim_{t\to\infty} m(n, t)$ exists.*

Proof. This lemma cannot be proved by induction in RCA_0 because it would require Σ^0_2 induction. We fix n and prove the lemma for this specific n.

Case. $n \notin TJ(Y)$ and $n = \langle e, r \rangle$

There is a $t = \langle e, r, x \rangle$ with $\neg\varphi(e, r, x, Y)$. At stage $t + 1$, $m(n, t + 1)$ is labeled not fixed and $\forall t' > t\,(m(n, t') = m(n, t + 1))$.

Case. $n \in TJ(Y)$

Notice that $m(n, t + 1) \neq m(n, t)$ if and only if $t = \langle e, r, x \rangle$, $\neg\varphi(e, r, x, Y)$, $m(\langle e, r \rangle, t)$ is labeled possibly fixed, and $m(\langle e, r \rangle, t) <_X m(n, t)$. Since $m(n, t)$ is labeled possibly fixed at stage t, it follows from $m(\langle e, r \rangle, t) <_X m(n, t)$ that $\langle e, r \rangle <_{\mathbb{N}} n$. Thus we have

$$m(n, t) \neq m(n, t + 1)$$

if and only if

$$\exists \langle e, r \rangle \leq n \exists x \leq t \forall k \leq x \left(t = \langle e, r, x \rangle \wedge \neg\varphi(e, r, x, Y) \wedge \varphi(e, r, k, Y) \right).$$

Therefore the set

$$\{\, t \mid m(n, t) \neq m(n, t + 1) \,\}$$

exists. It is finite since for each $\langle e, r \rangle \leq n$ there is at most one x such that $\neg\varphi(e, r, x, Y)$ and $\varphi(e, r, k, Y)$ for all $k \leq x$. Hence $\lim_{t\to\infty} m(n, t)$ exists. □

Lemma 7.25. *(RCA_0) If $n \notin TJ(Y)$ then there is a $t \geq n$ such that $m(n, t)$ is labeled not fixed at stage t.*

Proof. Let $t = \langle e, r, x \rangle$ where $\neg\varphi(e, r, x, Y)$ and $\forall k \leq t(\varphi(e, r, k, Y))$. □

Lemma 7.26. *(RCA_0) If $n \notin TJ(Y)$ and $m(n, \tilde{t})$ is labeled not fixed at stage $\tilde{t}$, then $m(n, \tilde{t}) = \lim_{t\to\infty} m(n, t)$ and there is an infinite descending chain below $m(n, \tilde{t})$ in X.*

Proof. The function $f : \mathbb{N} \to \mathbb{N}$ given by $k \mapsto b(\tilde{t} + k)$ is an infinite descending chain below $m(n, \tilde{t})$. □

In fact it is clear that if n is any number labeled not fixed at stage $\tilde{t}$ then the function f in the proof of the previous lemma gives an infinite descending chain below n.

Lemma 7.27. *(RCA_0) If $n \in TJ(Y)$ and $\lim_{t\to\infty} m(n,t) = \tilde{n}$ then there is a finite number of elements below $\tilde{n}$ in X.*

Proof. Let $\tilde{t}$ be such that $m(n,\tilde{t}) = \tilde{n}$. Since $m(n,t)$ is an increasing function, $m(n,t)$ never changes after $\tilde{t}$ and since $n \in TJ(Y)$, $\tilde{n}$ is labeled possibly fixed at all stages after $\tilde{t}$. Because $\tilde{n}$ is labeled possibly fixed, nothing is ever placed below $\tilde{n}$ in X after stage $\tilde{t}$. Since the size of $X_{\tilde{t}}$ is bounded by $b(\tilde{t})$, there are only a finite number of elements below $\tilde{n}$ in X. □

Lemma 7.28. *(RCA_0) $n \in TJ(Y)$ if and only if $\exists t(m(n,t) \in W(X))$.*

Proof. We have shown that any number labeled not fixed has an infinite descending chain below it and that $n \in TJ(Y)$ if and only if $\lim_{t\to\infty} m(n,t) \in W(X)$. Notice that if $m(n,t{+}1) \neq m(n,t)$, then the number $m(n,t)$ is labeled not fixed and hence $m(n,t) \notin W(X)$. Thus, a number k is in $W(X)$ if and only if $k = \lim_{t\to\infty} m(n,t)$ for some n and $n \in TJ(Y)$. However, if $m(n,\tilde{t}) \in W(X)$, then the label on $m(n,\tilde{t})$ never changes to not fixed. Hence, $m(n,\tilde{t}) = \lim_{t\to\infty} m(n,t)$ and so $n \in TJ(Y)$. If $m(n,t) \notin W(X)$ for all t, then in particular $\lim_{t\to\infty} m(n,t) \notin W(X)$ and so $n \notin TJ(Y)$. □

To complete the proof of Lemma 7.23, notice that the original definition of $TJ(Y)$ was given by a Π^0_1 formula. Lemma 7.28 gives a definition of $TJ(Y)$ that is Σ^0_1 in $W(X)$. However, by Proposition 7.15, we know that RCA_0 plus statement (1) of Lemma 7.23 imply that $W(X)$ exists. Hence, assuming statement (1), $TJ(Y)$ is defined by a Δ^0_1 condition. This step completes the proof of Lemma 7.23, which in turn completes the proof of Theorem 7.5.

Chapter 8

Spaces of Orders and Computable Presentations

In this chapter, we turn our attention to two questions from Downey and Kurtz (1986). First, is every c.b. Π^0_1 class representable up to Turing degree by the space of orders on some computable torsion free abelian group? Second, is every fully orderable computable group classically isomorphic to a computably fully orderable computable group? Since we will only be concerned with full orders, the terms order and full order will be used interchangeably.

8.1 Π^0_1 Classes and Spaces of Orders

Recall that for an orderable group G, $\mathbb{X}(G)$ denotes the space of positive cones of full orders on G. We proved the following connection between $\mathbb{X}(G)$ and c.b. Π^0_1 classes in Chapter 3.

Theorem 8.1. *Let G be a fully orderable computable group. There is a c.b. Π^0_1 class C and a Turing degree preserving bijection $\varphi : \mathbb{X}(G) \to C$.*

Metakides and Nerode (1979) proved a similar result for ordered fields. Let $\mathbb{X}(F)$ denote the set of positive cones of orders on an orderable field F. As with groups, there is a set of algebraic conditions that determines if a subset of F is the positive cone of a full order.

Theorem 8.2 (Metakides and Nerode (1979)). *Let F be a computable field. There is a c.b. Π^0_1 class C and a Turing degree preserving bijection $\varphi : \mathbb{X}(F) \to C$.*

Metakides and Nerode (1979), however, carried this argument one step farther. They proved that every c.b. Π^0_1 class can be represented by $\mathbb{X}(F)$ for some computable field F.

Theorem 8.3 (Metakides and Nerode (1979)). *Let C be a c.b. Π^0_1 class. There is a computable field F and a degree preserving bijection $\varphi : \mathbb{X}(F) \to C$.*

Downey and Kurtz (1986) asked if there is a result similar to Theorem 8.3 for computable torsion free abelian groups. Unfortunately, it is not possible to have a result this strong. For groups, if P is the positive cone of a full order and

$$P^{-1} = \{ g^{-1} \mid g \in P \}.$$

then P^{-1} is also the positive cone of a full order. Notice that $P \equiv_T P^{-1}$, so any degree which contains a member of $\mathbb{X}(G)$ contains at least two members of $\mathbb{X}(G)$. However, there is a c.b. Π^0_1 class C such that for any $f, g \in C$, if $f \neq g$ then $\deg(f) \neq \deg(g)$. Therefore, there cannot be a degree preserving bijection between C and $\mathbb{X}(G)$ for any fully orderable computable group G.

There are two natural modifications of the question of representing c.b. Π^0_1 classes. Given a c.b. Π^0_1 class C:

1. Is there a computable torsion free abelian group G such that

$$\{ \deg(f) | f \in C \} = \{ \deg(P) | P \in \mathbb{X}(G) \} ?$$

2. Is there a fully orderable computable group G and a two-to-one degree preserving map $\varphi : \mathbb{X}(G) \to C$?

The answer to both questions turns out to be no. Notice that if the answer to (1) is no, then the answer to (2) is also no. Before answering (1), we need some abelian group theory.

Definition 8.4. Let G be an abelian group. The elements $g_0, \ldots, g_n \in G \setminus 1_G$ are **linearly independent** if and only if for any $\alpha_0, \ldots, \alpha_n \in \mathbb{Z}$ the equality

$$\alpha_0 g_0 + \alpha_1 g_1 + \cdots + \alpha_n g_n = 0_G$$

implies $\alpha_i g_i = 0_G$ for all i. If G is torsion free, this condition means that $\alpha_i = 0$ for all i. An infinite set $B \subseteq G \setminus 1_G$ is linearly independent if every finite subset of B is linearly independent. A maximal set of linearly independent elements is called a **basis** for G and the cardinality of any basis is called the **rank** of G.

For example, G has rank 1 if and only if G is isomorphic to a subgroup of $\mathbb{Q}$. If G is a torsion free divisible abelian group, then G can be viewed as a vector space over $\mathbb{Q}$. In this case, the definitions of linear independence, basis and rank for G as a group agree exactly with the definitions of the same terms for G as a vector space.

Our study of computable torsion free abelian groups breaks into three categories: groups of rank 1, groups of finite rank > 1, and groups of infinite rank. Recall that if G is a computable torsion free abelian group and D is a computable divisible closure of G, then there is a degree preserving bijection $\varphi : \mathbb{X}(G) \to \mathbb{X}(D)$. Therefore, when studying the cardinality of $\mathbb{X}(G)$ or the degrees of members of $\mathbb{X}(G)$, we can assume without loss of generality that G is divisible.

Lemma 8.5. *If G is a computable torsion free abelian group of rank 1, then G has exactly two orders, both of which are computable.*

Proof. Any divisible closure of G is computably isomorphic to $\mathbb{Q}$. $\mathbb{Q}$ has exactly two orders both of which are computable, so G has exactly two orders both of which are computable. $\square$

Lemma 8.6. *If G is a computable torsion free abelian group with finite rank strictly greater than 1, then G has 2^ω orders and has orders of every Turing degree.*

Proof. We assume that G is divisible. Since G has finite rank, we can also assume that we have a basis for G. For simplicity, we consider the case when G has rank 2 and later prove the lemma for larger ranks.

Let $\{a, b\}$ be a basis for G. Any element of G can be written as $p_1 a + p_2 b$ for some $p_1, p_2 \in \mathbb{Q}$. The lexicographic order on G is computable:

$$p_1 a + p_2 b \in P \;\Leftrightarrow\; p_1 > 0 \;\vee\; (p_1 = 0 \wedge p_2 \geq 0).$$

Therefore, G has a computable order. Let $\mathbf{a}$ be an arbitrary noncomputable degree and $r \in \mathbf{a}$ be a real such that $0 < r < 1$. Notice that r must be irrational since $0 <_T r$. We define the map $f_r : G \to \mathbb{R}$ that sends $p_1 a + p_2 b$ to $p_1 + p_2 r$. Because r is irrational, this map is a monomorphism and defines an isomorphism between G and a subgroup of $\mathbb{R}$. We use the structure of $\mathbb{R}$ to define a full order $\leq_r$ on G. For $g, h \in G$

$$g \leq_r h \;\Leftrightarrow\; f_r(g) \leq_{\mathbb{R}} f_r(h).$$

It remains to show that $\deg(r) = \deg(\leq_r)$, for then we have $\deg(\leq_r) = \mathbf{a}$.

Claim. $\deg(r) \leq_T \deg(\leq_r)$

The idea is to use $\leq_r$ to compute a binary expansion for r. We need to determine the coefficients $a_i \in \{0, 1\}$ in

$$r \;=\; \sum_{i=1}^{\omega} \frac{a_i}{2^i}.$$

To compute a_1, notice that

$$r >_{\mathbb{R}} \frac{1}{2} \Leftrightarrow 2r >_{\mathbb{R}} 1 \Leftrightarrow 2b >_r a$$
$$r <_{\mathbb{R}} \frac{1}{2} \Leftrightarrow 2r <_{\mathbb{R}} 1 \Leftrightarrow 2b <_r a.$$

Using $\leq_r$ we compute:

$$2b >_r a \Rightarrow a_1 = 1$$
$$2b <_r a \Rightarrow a_1 = 0.$$

To compute a_{n+1}, we assume by induction that we know $a_1, \ldots, a_n$ and that

$$\sum_{i=1}^{n} \frac{a_i}{2^i} \;<_{\mathbb{R}}\; r \;<_{\mathbb{R}}\; \sum_{i=1}^{n} \frac{a_i}{2^i} \;+\; \frac{1}{2^n}.$$

To find a_{n+1}, we need to know if

$$r \;<_{\mathbb{R}}\; \sum_{i=1}^{n} \frac{a_i}{2^i} \;+\; \frac{1}{2^{n+1}}.$$

If this inequality holds, then $a_{n+1} = 0$ and otherwise $a_{n+1} = 1$. By the definition of $\leq_r$, we have that

$$r \;<_{\mathbb{R}}\; \sum_{i=1}^{n} \frac{a_i}{2^i} \;+\; \frac{1}{2^{n+1}} \;\Leftrightarrow\; b \;<_r\; \sum_{i=1}^{n} \frac{a_i}{2^i}a \;+\; \frac{a}{2^{n+1}}.$$

Note that the required induction hypothesis holds once we set a_{n+1} to the correct value. The claim is proved.

Claim. $\deg(\leq_r) \leq_T \deg(r)$

Assume we have coefficients $a_i \in \{0, 1\}$ for the sum

$$r \;=\; \sum_{i=1}^{\omega} \frac{a_i}{2^i}.$$

We need to be able to compare elements of the form

$$\frac{p}{q}a + \frac{p'}{q'}b \;\text{ and }\; \frac{m}{n}a + \frac{m'}{n'}b$$

where the numbers in the fractions are from $\mathbb{Z}$ and $q, q', n, n' > 0$. If we multiply by $qq'nn'$ we see that it suffices to be able to compare elements of the form

$$n_1a + m_1b \;\text{ and }\; n_2a + m_2b.$$

However, by collecting terms we have

$$n_1a + m_1b \leq_r n_2a + m_2b \;\Leftrightarrow\; (n_1 - n_2)a \leq_r (m_2 - m_1)b.$$

Therefore, it suffices to be able to compare na and mb for $n, m \in \mathbb{Z}$. We will further assume that $n, m \in \mathbb{N} \setminus 0$ since the other cases are either easy (i.e. $n = 0$ and $m > 0$) or reduce to this case (i.e. $n < 0$ and $m < 0$).

The map f_r sends $na \mapsto n$ and $mb \mapsto mr$. To compare n and mr as elements of $\mathbb{R}$, we need to compute an approximation to r to an accuracy such that there are no integers within the error bounds for m times the approximation. For any k we know that

$$m \cdot \sum_{i=1}^{k} \frac{a_i}{2^i} \;<_{\mathbb{R}}\; m \cdot r \;<_{\mathbb{R}}\; m \cdot \left(\sum_{i=1}^{k} \frac{a_i}{2^i} \;+\; \frac{1}{2^k} \right).$$

We need to find a k such that there are no integers in the interval

$$\left[m \cdot \sum_{i=1}^{k} \frac{a_i}{2^i} \,,\; m \cdot \left(\sum_{i=1}^{k} \frac{a_i}{2^i} + \frac{1}{2^k} \right) \right].$$

Once we know such a k exists, we can find it by searching. Because mr is irrational, it must sit strictly between two integers. Let d be the distance from mr to the nearest integer and let k be such that $m/2^k < d$. It follows that

$$m \cdot \left(r - \sum_{i=1}^{k} \frac{a_i}{2^i} \right) < \frac{m}{2^k} < d$$

and

$$m \cdot \left(\sum_{i=1}^{k} \frac{a_i}{2^i} + \frac{1}{2^k} - r \right) < \frac{m}{2^k} < d.$$

Thus, there is a k as required for the approximation. We can now compare na and mb as follows:

$$na <_r mb \;\Leftrightarrow\; n <_{\mathbb{R}} mr \;\Leftrightarrow\; n <_{\mathbb{R}} m \cdot \sum_{i=1}^{k} \frac{a_i}{2^i}.$$

The claims show that $\deg(r) = \deg(\leq_R)$ and hence G has orders of every degree. Since there are 2^ω degrees, G has 2^ω distinct orders. This completes the proof for groups of rank 2.

Assume G is a computable torsion free abelian group of finite rank $n > 2$. We assume that G is divisible and that we have a basis $\{g_1, \ldots, g_n\}$ for G. Any element of G can be written as

$$q_1 g_1 + \cdots + q_n g_n$$

for some $q_1, \ldots, q_n \in \mathbb{Q}$. G is the direct product of the computable subgroups generated by $\{g_1, g_2\}$ and $\{g_3, \ldots, g_n\}$, so we can lexicographically order G using the orders on these subgroups as in Theorem 3.21.

For any degree $\mathbf{a}$, the subgroup generated by $\{g_1, g_2\}$ has an order of degree $\mathbf{a}$. The subgroup generated by $\{g_3, \ldots, g_n\}$ is computably orderable and therefore, the direct product has an order of degree $\mathbf{a}$. □

Lemma 8.7. *If G is a computable torsion free abelian group with infinite rank, then G has 2^ω distinct orders and has orders of every degree $\mathbf{a} \geq_T 0'$*

Proof. Unlike in the proof of Lemma 8.6, we cannot assume that we have a basis for G. However, there is a basis computable in $0'$. Define

$$A \;=\; \{\, \langle g_1, \ldots, g_{n+1} \rangle \mid \exists \langle q_1, \ldots, q_n \rangle \, (g_{n+1} = q_1 g_1 + \cdots + q_n g_n) \,\}.$$

A is defined by a Σ^0_1 statement, so $A \leq_T 0'$. To obtain a basis for G, define a sequence of finite sequences

$$\langle e_1 \rangle,\ \langle e_1, e_2 \rangle,\ \ldots,\ \langle e_1, \ldots, e_n \rangle,\ \ldots$$

by: e_1 is the least nonidentity element of G and e_{n+1} is the $\mathbb{N}$-least element of G such that $\langle e_1, \ldots, e_n, e_{n+1} \rangle \notin A$. A basis for G is given by

$$B \ = \ \{\, g \,|\, g \text{ appears in a sequence } \langle e_1, \ldots, e_n \rangle \,\}.$$

B is computable from A, so $B \leq_T 0'$.

Once we have a basis $e_1, e_2, \ldots$ for G, we can write each element of G as

$$q_1 e_1 + \cdots + q_n e_n$$

for some $q_1, \ldots q_n \in \mathbb{Q}$ with $q_n \neq 0$. We split G into the direct product of the subgroup generated by $\{e_1, e_2\}$ and the subgroup generated by $\{e_3, e_4, \ldots\}$. The lexicographic order on the subgroup generated by $\{e_3, e_4, \ldots\}$ is computable from the basis B.

Suppose $\mathbf{a}$ is any degree above $0'$. The basis B is computable from $\mathbf{a}$ and so the subgroup generated by $\{e_3, e_4, \ldots\}$ has an order computable in $\mathbf{a}$. By Lemma 8.6, the subgroup generated by $\{e_1, e_2\}$ has an order exactly of degree $\mathbf{a}$. Therefore, the lexicographic product of these orders has degree exactly $\mathbf{a}$. □

Theorem 8.8. *There is a c.b. Π^0_1 class C such that for any computable torsion free abelian group G*

$$\{\, deg(f) \,|\, f \in C \,\} \ \neq \ \{\, deg(p) \,|\, P \in \mathbb{X}(G) \,\}.$$

Proof. Recall from Theorem 1.9 that there is an infinite c.b. Π^0_1 class C such that for any $f, g \in C$, if $f \neq g$ then f and g are Turing incomparable. Let C be such a c.b. Π^0_1 class. Let G be any computable torsion free abelian group. By Lemmas 8.5, 8.6 and 8.7 we know that G has either only computable orders, orders of every degree or orders of every degree above $0'$. In any of these cases, it is impossible for the set of degrees of elements of $\mathbb{X}(G)$ to be equal to the set of degrees of elements of C. □

Theorem 8.8 shows that the spaces of orders on computable torsion free abelian groups do not suffice to represent all c.b. Π^0_1 classes even in a weak sense. The next theorem shows that they cannot represent even the restricted class of Π^0_1 classes of separating sets.

Theorem 8.9. *There is a Π^0_1 class of separating sets C such that for any computable torsion free abelian group G*

$$\{\, deg(f) \,|\, f \in C \,\} \ \neq \ \{\, deg(p) \,|\, P \in \mathbb{X}(G) \,\}.$$

Proof. The proof is exactly the same as the proof of Theorem 8.8 except that it relies on a different result about Π^0_1 classes of separating sets. From Theorem 1.10 we know that there is a Π^0_1 class of separating sets C such that for any $A, B \in C$ either $A \equiv_T B$ or A and B are Turing incomparable. □

8.2 Extension to Nilpotent Groups

Recall from Theorem 3.34 that the space of orders of any orderable computable group can be represented by a c.b. Π^0_1 class. So far in this chapter we have only looked at torsion free abelian groups. Perhaps we need to widen our view to the class of all fully orderable groups if we want to represent all c.b. Π^0_1 classes. This problem of whether all orderable computable groups suffice to represent c.b. Π^0_1 classes is still open. We can, however, extend the negative results from abelian groups to nilpotent groups. The goal for this section is to show that there is a c.b. Π^0_1 class C such that for any computable torsion free nilpotent group G we have

$$\{\deg(f) \mid f \in C\} \neq \{\deg(p) \mid P \in \mathbb{X}(G)\}.$$

Before proving results about the number and complexity of full orders on nilpotent groups, we need a description of a general method for building these full orders. Recall that if N is a normal subgroup of an O-group G, then a full order $\leq_N$ on N is called a G-order if for any $a, b \in N$ and $g \in G$

$$a \leq_N b \Rightarrow gag^{-1} \leq_G gbg^{-1}.$$

Let $P(N)$ be the positive cone of a full G-order on N and $\leq_{G/N}$ be a full order on the quotient group. These orders induce a full order on G defined by

$$g \leq_G h \;\Leftrightarrow\; aN <_{G/N} bN \;\vee\; (aN = bN \wedge a^{-1}b \in P(N)).$$

Under $\leq_G$, N is convex and the induced orders on N and G/N are the same as the ones used to build $\leq_G$.

Let G be a torsion free nilpotent group. Recall that this means G has a finite upper central series

$$\langle 1_G \rangle = \zeta_0(G) \leq \zeta_1(G) \leq \cdots \leq \zeta_n(G) = G$$

where $\zeta_1(G)$ is the center of G and for each $0 \leq i < n$, $\zeta_{i+1}(G)/\zeta_i(G)$ is the center of $G/\zeta_i(G)$. By Lemma 3.17, we know that each $\zeta_{i+1}(G)/\zeta_i(G)$ is a torsion free abelian group and therefore is fully orderable. We will use this structure to build orders on G under which the terms in the upper central series are convex.

To order G, start by ordering the torsion free abelian subgroup $\zeta_1(G)$. Because $\zeta_1(G)$ is the center of G, any order we put on it will be a G-order. Next, consider $\zeta_2(G)/\zeta_1(G)$. This quotient group is torsion free and abelian, so it is orderable. Because $\leq_{\zeta_1(G)}$ is a G-order, and hence a $\zeta_2(G)$-order, we have an induced order, $\leq_{\zeta_2(G)}$, on $\zeta_2(G)$.

The key fact is that the order $\leq_{\zeta_2(G)}$ is a G-order. Suppose $a <_{\zeta_2(G)} b$. There are two cases to consider. If $a\zeta_1(G) \neq b\zeta_1(G)$, then it must be that $a\zeta_1(G) < b\zeta_1(G)$. Because $\zeta_2(G)/\zeta_1(G)$ is the center of $G/\zeta_1(G)$ we have that

$$gag^{-1}\zeta_1(G) = a\zeta_1(G) < b\zeta_1(G) = gbg^{-1}\zeta_1(G).$$

Therefore, by the definition of the induced order, $gag^{-1} <_{\zeta_2(G)} gbg^{-1}$. The second case is when $a\zeta_1(G) = b\zeta_1(G)$. In this case, $gag^{-1}\zeta_1(G) = gbg^{-1}\zeta_1(G)$ and the order on these elements is determined by $\leq_{\zeta_1(G)}$, which we already know is a G-order.

Now that we have ordered $\zeta_2(G)$, we proceed up the upper central series ordering each term from the order on the previous term and the order on the quotient. This method does not construct all the possible orders on G, but it will give enough for our purposes. In particular, it is possible to have orders under which the terms in the upper central series are not convex and this procedure will never yield an order like that.

Proposition 8.10. *Let G be a properly 2 step torsion free nilpotent group and C be the center of G. The rank of G/C is greater than or equal to 2.*

Proof. For a contradiction, suppose that the rank of G/C is 1. This statement is equivalent to saying that G/C is isomorphic to a subgroup of $\mathbb{Q}$. Since G is properly 2 step nilpotent, and hence not abelian, there must be elements $a, b \in G$ such that $ab \neq ba$. Thus, neither a nor b is in C and so $aC \neq 1_G C$ and $bC \neq 1_G C$.

Since G/C is a subgroup of $\mathbb{Q}$, there must be integers $p, q \neq 0$ such that

$$a^p C = b^q C.$$

This equality implies that there is a $c \in C$ such that $a^p = b^q c$ and we get

$$a^p b = b^q cb = b^q bc = bb^q c = ba^p.$$

Thus a^p commutes with b and so $[a^p, b] = 1_G$. By commutator identities we have that

$$[x^2, y] \;=\; [x, y] \cdot \big[[x, y], x\big] \cdot [x, y] \;=\; [x, y]^2.$$

The second inequality follows because in a 2 step nilpotent group the commutators commute with all elements of the group. By induction, we have that

$$[a^p, b] = [a, b]^p$$

for any $p \geq 0$. In a 2 step nilpotent group $[x^{-1}, y] = [y, x]$, so $[a^p, b] = [b, a^{-p}]$ for $p < 0$. Applying another commutator identity for 2 step nilpotent groups, $[x, y^n] = [x, y]^n$, we have that for $p < 0$

$$[a^p, b] = [b, a^{-p}] = [b, a]^{-p} = [a, b]^p.$$

So, for any $p \in \mathbb{Z}$, $[a^p, b] = [a, b]^p$. Therefore, since $[a^p, b] = 1_G$, we know that $[a, b]^p = 1_G$. But, G is torsion free, so $[a, b] = 1_G$. This fact contradicts our original choice of a and b as noncommuting elements. □

Corollary 8.11. *If G is a countable properly 2 step torsion free nilpotent group, then G has 2^ω distinct full orders.*

Proof. For any O-group there is always a full order under which the center is convex (see Kokorin and Kopytov (1974)). In fact, our general method for constructing full orders on nilpotent groups makes the center convex. Let $\leq$ be such an order on G and let C be the center of G. Notice $\leq |_C$ is a full G-order. Therefore, if we have any order on G/C, we can combine it lexicographically with $\leq|_C$ to get a full order on G. Furthermore, if we take two distinct orders on G/C, this process yields distinct orders on G.

By Proposition 8.10, G/C has rank ≥ 2 and so by Lemma 8.6, G/C has 2^ω distinct orders. Therefore, G has 2^ω orders. □

Lemma 8.12 (Robinson (1982)). *If $m \geq 3$ and G is a properly m step nilpotent group, then $G/\zeta_{m-2}(G)$ is a properly 2 step nilpotent group.*

Corollary 8.13. *If $m \geq 2$ and G is a torsion free properly m step nilpotent group, then G has 2^ω orders.*

Proof. The case for $m = 2$ was handled in Corollary 8.11. If $m \geq 3$, then by Lemma 8.12, $G/\zeta_{m-2}(G)$ is a properly 2 step nilpotent and hence has 2^ω orders.

Let $\leq$ be an order on G under which the terms in the upper central series are convex as in our general method. As in the proof of Corollary 8.11, the restriction $\leq|_{\zeta_{m-2}(G)}$ is a full G-order on $\zeta_{m-2}(G)$. Therefore, $\leq|_{\zeta_{m-2}(G)}$ can be combined lexicographically with any order on $G/\zeta_{m-2}(G)$ to give an order of G. Thus, G has 2^ω orders. □

We need to know not only about the number of orders, but also about the degrees of orders of computable torsion free nilpotent groups.

Lemma 8.14. *A computable torsion free properly 2 step nilpotent group has orders of every degree above $0''$.*

Proof. Let G be a computable torsion free properly 2 step nilpotent group. The center C is computable in $0'$, so G/C is a torsion free abelian group computable in $0'$ with rank > 1. By the relativized versions of Lemmas 8.6 and 8.7, G/C has orders of every degree above $0''$.

Since C is a torsion free abelian group computable in $0'$, it has an order computable in $0''$ (in fact, it has an order which is low over $0'$). Fix such an order. Because C is the center of G, any order on C is a G-order. Let $\mathbf{a}$ be any degree above $0''$. An order on G/C of degree $\mathbf{a}$ can be lexicographically combined with the order on C to produce an order on G which has degree $\mathbf{a}$. □

We want to use similar ideas to handle nilpotent groups with longer upper central series. Notice that $\zeta_1(G)$ is computable in $0'$, so $G/\zeta_1(G)$ is computable in $0'$ and $\zeta_1(G)$ has a G-order computable in $0''$. The center of $G/\zeta_1(G)$ is computable in $0''$, so $\zeta_2(G)$ and $G/\zeta_2(G)$ are both computable in $0''$. Therefore, $\zeta_2(G)/\zeta_1(G)$ has a G-order computable in $0^{(3)}$ and there is an induced order on $\zeta_2(G)$ computable in $0^{(3)}$. Continuing this process, it is clear that $\zeta_n(G)$ will be computable in $0^{(n)}$ and have a G-order computable in $0^{(n+1)}$.

Lemma 8.15. *Let $n > 1$ and let G be a computable torsion free properly n step nilpotent group. For every degree $\mathbf{a} \geq_T 0^{(n)}$, G has an order of degree $\mathbf{a}$.*

Proof. The case for $n = 2$ was done in Lemma 8.14, so assume that $n > 2$. By Lemma 8.12 and the comments above, we know that $G/\zeta_{n-2}(G)$ is a torsion free properly 2 step nilpotent group computable in $0^{(n-2)}$. By the relativized version of Lemma 8.14, $G/\zeta_{n-2}(G)$ has orders of every degree above $0^{(n)}$. By the comments made above, $\zeta_{n-2}(G)$ is computable in $0^{(n-2)}$ and has a G-order computable in $0^{(n-1)}$.

Let $\mathbf{a}$ be any degree above $0^{(n)}$. An order of degree $\mathbf{a}$ on $G/\zeta_{n-2}(G)$ together with a G-order of degree $0^{(n-1)}$ on $\zeta_{n-2}(G)$ induces an order of degree $\mathbf{a}$ on G. □

Theorem 8.16. *There is a c.b. Π^0_1 class of separating sets C such that for any torsion free nilpotent group G*

$$\{\, deg(f) \mid f \in C \,\} \;\neq\; \{\, deg(p) \mid P \in \mathbb{X}(G) \,\}.$$

Proof. If G is abelian, the theorem follows from Theorem 8.9. Otherwise, G must be properly n step nilpotent for some $n > 1$. The theorem now follows from Lemma 8.15 and the proof of Theorem 8.9. □

8.3 Computable Presentations

In this section, we turn our attention to the question of whether every orderable computable group is classically isomorphic to a computably orderable computable group. Downey and Kurtz (1986) asked this question because their example of a computable torsion free abelian group with no computable order was isomorphic to $\Pi^{\omega}_{i=1}\mathbb{Z}_i$, which with the right presentation is computably orderable. The answer to this question for general groups is still unknown, but we will answer it for abelian groups and for finitely generated nilpotent groups.

In Section 8.1, we made the simplifying assumption that our abelian groups were divisible because it did not change the change the number or the complexity of the orders. Here, we cannot make such an assumption because it changes the structure of the group. The next lemma shows that we can reduce the problem of finding computable orders to the problem of finding a computable basis.

Lemma 8.17. *Let G be a computable torsion free abelian group. If B is a basis for G, then G has a full order that is computable from B.*

Proof. Let $e_1, e_2, \dots, e_n, \dots$ be a (possible finite) list of the elements of B. We order the elements of the basis by

$$e_1 \ll e_2 \ll \cdots \ll e_n \ll \cdots .$$

This order of the basis elements induces an order on all of G. To compare g and $h \in G$ with $g \neq h$, first write each element in the form

$$ng \;=\; \sum_{i \in I} p_i e_i$$
$$mh \;=\; \sum_{j \in J} q_j e_j$$

where I, J are finite sets and n, m, p_i and $q_j \in \mathbb{Z} \setminus \{0\}$. Let K be the maximum of $I \cup J$ and set $p_k = 0$ if $k \notin I$ and $q_k = 0$ if $k \notin J$. The order on g and h is given by

$$g < h \;\Leftrightarrow\; \frac{p_k}{n} <_{\mathbb{Q}} \frac{q_k}{m}.$$

Because the summation forms for each element are computable from B, this order is computable from B. □

Theorem 8.18. *Every computable torsion free abelian group of finite rank has a computable order.*

Proof. This theorem follows immediately from Lemma 8.17 because every finite set is computable. □

We know that Theorem 8.18 is not true for groups of infinite rank because of the Downey and Kurtz (1986) example and the fact that WKL_0 is required to prove that every torsion free abelian group is orderable. However, we can use the following result from the study of computable abelian groups.

Theorem 8.19 (Dobritsa (1983)). *Let G be a computable torsion free abelian group. There is a computable group H which is classically isomorphic to G and has a computable basis.*

This theorem was originally stated and proved using the terminology of the Russian school's approach to computable mathematics (i.e. using the language of constructivizations). The proof below is written using the language of the Western approach.

Definition 8.20. Let G be a torsion free abelian group. The elements $a_0, \dots, a_k$ are **t-dependent** if there are integers $m_0, \dots, m_k$ such that each $|m_i| \leq t$, at least one $m_i \neq 0$ and

$$m_0 a_0 + m_1 a_1 + \cdots + m_k a_k = 0_G.$$

If there are no such integers, then $a_0, \dots a_k$ are called **t-independent**.

Proof. Notice that if G has finite rank, then G has a computable basis. Assume that G has infinite rank. The main idea is to build H in stages while approximating a basis for G. During the construction, we define the elements of H and a bijection

$$\psi : H \to G.$$

Only at the end, when we have verified certain properties of the construction, do we define the group structure on H and verify that ψ is a group isomorphism. Because the approximation of ψ changes frequently, ψ will not be computable, but will be Δ^0_2.

Before starting the construction, it is worth introducing the notation that is used. c_i^t is the guess at the i^{th} basis element of G at stage t. There is a computable function $f(t)$ which defines the domain of H at stage t,

$$H_t \;=\; \{h_0, h_1, \dots, h_{f(t)}\}.$$

The first $t+1$ basis elements of H are denoted by

$$\{b_0, \dots, b_t\} \subseteq H_t.$$

If $i > 0$ and h_i enters H at stage t, then h_i is assigned a $(t+2)$-tuple of integers from $[-t, t]$. The statement $\langle \alpha, \alpha_0, \dots, \alpha_t \rangle$ is assigned to h_i is written as

$$\alpha h_i = \alpha_0 b_0 + \alpha_1 b_1 + \cdots + \alpha_t b_t.$$

The intuition is that these tuples uniquely determine each element of H in terms of the basis elements. A slight technical point about our use of tuples in this proof is that we only consider tuples up to trailing zeros. That is, the tuples $\langle 1, 2 \rangle$, $\langle 1, 2, 0 \rangle$ and $\langle 1, 2, 0, 0, 0, 0 \rangle$ are considered equal. Also, any tuple which is assigned will have the property that the greatest common divisor of $\alpha, \alpha_0, \dots, \alpha_t$ is 1.

The approximation to ψ at stage t is denoted ψ_t. The elements

$$\{c_0^t, \dots, c_t^t\}$$

are defined at stage t. We guarantee at stage t that

$$\alpha h_i = \alpha_0 b_0 + \cdots + \alpha_t b_t$$

if and only if

$$\alpha \psi_t(h_i) = \alpha_0 c_0^t + \cdots + \alpha_t c_t^t.$$

If at a later stage any of the c_i^t change, we will change the approximation of ψ to guarantee that this equality continues to hold. At stage t, all tuples of the form $\langle 1, \alpha_0, \dots, \alpha_t \rangle$ with each $|\alpha_i| \le t$ will be assigned and possibly some tuples of the form $\langle \alpha, \alpha_0, \dots, \alpha_t \rangle$ where the greatest common divisor of the elements of the tuple is 1.

Construction

Stage 0: Define c_0^0 to be the $\mathbb{N}$-least nonidentity element of G. Set $f(0) = 1$, so H_0 contains 0 and 1, which to avoid confusion are denoted h_0 and h_1. The map $\psi_0 : H_0 \to G$ sends $h_0 \mapsto 0_G$ and $h_1 \mapsto c_0^0$. b_0 is set to h_1 and the tuples $1 \cdot h_1 = 1 \cdot b_0$ and $1 \cdot h_0 = 0 \cdot b_0$ are assigned.

Stage $\mathbf{t+1}$: At the end of stage t we have the following objects:

$$\{b_0, \dots, b_t\} \subseteq \{h_0, \dots, h_{f(t)}\} = H_t$$
$$\psi_t : H_t \to G$$
$$\{c_0^t, \dots, c_t^t\} \subseteq G.$$

Each h_i, $0 < i \le f(t)$, has been assigned to a tuple, the length of which depends on the stage at which h_i entered H. The following property is satisfied, assuming h_i entered H at stage $s \le t$:

$$\alpha h_i = \alpha_0 b_0 + \cdots + \alpha_s b_s \Leftrightarrow \alpha \psi_t(h_i) = \alpha_0 c_0^t + \cdots + \alpha_s c_s^t.$$

The construction proceeds are follows. Let $c^t_{t+1} = 0_G$. Let I be the least number such that $c^t_0, \ldots, c^t_I$ are $t+1$-dependent. Find the $\mathbb{N}$-least elements c'_{I+j}, $0 \le j \le t+1-I$, of G such that

$$c^t_0, \ldots, c^t_{I-1}, c'_I, \ldots, c'_{t+1}$$

are $(t+1)$-independent. Define $c^{t+1}_k = c^t_k$ for $k < I$ and $c^{t+1}_k = t!c'_k + c^t_k$ for $I \le k \le t+1$.

Let N be the number of tuples $\langle 1, \alpha_0, \ldots, \alpha_{t+1} \rangle$ where $|\alpha_i| \le t+1$ for each $i \le t+1$ and either $\alpha_{t+1} \ne 0$ or $|\alpha_i| = t+1$ for at least one $i \le t$. Notice that none of these tuples has been assigned at a previous stage. Let M be the number of elements of G which are less than $t+1$ and satisfy an equation of the form

$$\alpha g = \alpha_0 c^{t+1}_0 + \cdots + \alpha_{t+1} c^{t+1}_{t+1}$$

with $\alpha \ne 0, 1$, the greatest common divisor of $\alpha, \alpha_0, \ldots, \alpha_{t+1}$ is 1 and the tuple $\langle \alpha, \alpha_0, \ldots, \alpha_{t+1} \rangle$ has not been used before. Recall, that we equate tuples up to trailing zeros, so these tuples could have been used before.

Define $f(t+1) = f(t) + N + M$. The definition of ψ_{t+1} splits into cases. For $i = 0$,

$$\psi_{t+1}(h_0) = 0_G.$$

For $1 \le i \le f(t)$, assume that h_i was introduced at stage $s \le t$ and assigned the tuple

$$\alpha h_i = \alpha_0 b_0 + \cdots + \alpha_s b_s$$

with $|\alpha|, |\alpha_0|, \ldots, |\alpha_s| \le s$. By assumption we know that

$$\alpha_0 c^t_0 + \cdots + \alpha_s c^t_s = \alpha \psi_t(h_i). \tag{8.1}$$

We split into two subcases. If $s < I$, then set $\psi_{t+1}(h_i) = \psi_t(h_i)$. Because $c^{t+1}_0 = c^t_0, \ldots, c^{t+1}_s = c^t_s$, we know that $\psi_{t+1}(h_i)$ still satisfies Equation (8.1). If $s \ge I$, then

$$\alpha_0 c^t_0 + \cdots + \alpha_s c^t_s \ne \alpha_0 c^{t+1}_0 + \cdots + \alpha_s c^{t+1}_s.$$

However, by the definition of the elements c^{t+1}_k for $k \ge I$ we have

$$\alpha_0 c^t_0 + \cdots + \alpha_s c^t_s = \alpha_0 c^t_0 + \cdots + \alpha_s c^t_s + t!(c'_I + \cdots + c'_s).$$

Because $\alpha_0 c^t_0 + \cdots + \alpha_s c^t_s$ appears on one side of Equation 8.1, we know it is divisible by α in G. Notice that if $s = t+1$, then this statement is not quite true because $\alpha_{t+1} c^t_{t+1}$ does not appear in Equation 8.1. However, we can leave this term out because $c^t_{t+1} = 0_G$. Because $|\alpha| \le s \le t$, $t!(c'_I + \cdots + c'_s)$ is also divisible by α in G. Let $\psi_{t+1}(h_i)$ be the $\mathbb{N}$-least solution to

$$\alpha_0 c^{t+1}_0 + \cdots + \alpha_s c^{t+1}_s = \alpha x$$

in G. Notice that we have extended Equation 8.1 to stage $t+1$.

For $f(t) < i \leq f(t) + N$, let $\langle 1, \alpha_0, \ldots, \alpha_{t+1} \rangle$ be the $(i - f(t))^{\text{th}}$ tuple satisfying the conditions in the definition of N. Let

$$\psi_{t+1}(h_i) = \alpha_0 c_0^{t+1} + \cdots + \alpha_{t+1} c_{t+1}^{t+1}$$

and assign h_i the tuple

$$1 \cdot h_i = \alpha_0 b_0 + \cdots + \alpha_{t+1} b_{t+1}.$$

b_{t+1} is defined to be whichever h_i is assigned the tuple

$$1 \cdot h_i = 0b_0 + \cdots + 0b_t + 1b_{t+1}.$$

For $f(t) + N < i \leq f(t+1)$, let g be the $(i - f(t) - N)^{\text{th}}$ element of G satisfying the conditions in the definition of M. Suppose g satisfies the equation

$$\alpha g = \alpha_0 c_0^{t+1} + \cdots + \alpha_{t+1} c_{t+1}^{t+1}$$

with the same restrictions on the coefficients as in the definition of M. Set $\psi_{t+1}(h_i) = g$ and assign h_i the tuple

$$\alpha h_i = \alpha_0 b_0 + \cdots + \alpha_{t+1} b_{t+1}.$$

This case completes stage $t+1$ of the construction. Notice that we have met the induction requirements assumed at the beginning of state t.

End of Construction

The following lemmas verify the required properties of the construction.

Lemma 8.21. *For each i, $\lim_{t\to\infty} c_i^t = c_i$ exists and the set of elements c_i is independent.*

Proof. The lemma is proved by induction on i. Because $c_0^0 \neq 0_G$, it never changes and so $c_0 = c_0^0$.

Assume s is a stage such that $c_0 = c_0^s, \ldots, c_{i-1} = c_{i-1}^s$. Let g be the $\mathbb{N}$-least element of G such that

$$\{c_0, \ldots, c_{i-1}, g\}$$

is an independent set. Let $t \geq s$ be the least stage such that each $\tilde{g} \leq_{\mathbb{N}} g$ is $(t+1)$-dependent on $\{c_0, \ldots, c_{i-1}\}$. By definition, at stage $t+1$ we set $c_i' = g$ and $c_i^{t+1} = c_i^t + t!g$. Notice that $\{c_0, \ldots, c_{i-1}, c_i^t + t!g\}$ is independent, so c_i^{t+1} never changes again. Therefore, $c_i = c_i^{t+1}$. □

Lemma 8.22. *For each $i \in \omega$, $\lim_{t\to\infty} \psi_t(h_i) = \psi(h_i)$ exists.*

Proof. Fix i and we show that $\lim_{t\to\infty} \psi_t(h_i)$ exists. Suppose h_i is assigned the tuple

$$\alpha h_i = \alpha_0 b_0 + \cdots + \alpha_s b_s.$$

Let t be a stage such that $c_0^t = c_0, \ldots, c_s^t = c_s$. For any stage $t' \geq t$, when defining $\psi_{t'+1}(h_i)$ we will be in the case of $1 \leq i \leq f(t')$ and $s < I$. Thus, $\psi_{t'+1}(h_i) = \psi_{t'}(h_i)$ for every $t' \geq t$. □

Lemma 8.23. *The domain of ψ is ω and the range of ψ is G.*

Proof. The domain of ψ is all of ω because $f(t)$ is a strictly increasing function. To show that the range of ψ is G, let $g \in G$. Let t be a stage such that $c_0^t = c_0, \ldots, c_s^t = c_s$ and $\alpha g = \alpha_0 c_0 + \cdots + \alpha_s c_s$, where the greatest common divisor of the coefficients in 1 and $\alpha_s \neq 0$. Let t' be the maximum of t, the code for g, and the absolute values of α and the α_i's. If the tuple $\langle \alpha, \alpha_0, \ldots, \alpha_s \rangle$ has not been assigned by stage t', it will be assigned at stage t'. In either case, whichever element h_i is assigned this tuple will satisfy

$$\alpha \psi_{t'}(h_i) = \alpha_0 c_0^{t'} + \cdots + \alpha_s c_s^{t'} = \alpha_0 c_0 + \cdots + \alpha_s c_s = \alpha g.$$

Notice that because the approximations to the basis elements of G have stabilized by stage t', we know that $\psi_{t'}(h_i) = \psi(h_i)$. Thus, we have

$$\alpha \psi(h_i) = \alpha g.$$

Because G is torsion free, this equation implies that $\psi(h_i) = g$. □

We have now shown that ψ is a bijection and that $\{c_0, c_1, \ldots\}$ is a basis for G. It remains to show how to define the group structure on H and to check that ψ is a group homomorphism.

To define $+_H$, consider $h_i +_H h_j$. By possibly adding some zeros to the end of the tuples assigned to h_i or h_j, we can assume that we have

$$\alpha \psi(h_i) = \alpha_0 c_0 + \cdots + \alpha_t c_t$$
$$\beta \psi(h_j) = \beta_0 c_0 + \cdots + \beta_t c_t.$$

Multiplying the top equation by β, the bottom equation by α and adding them together we get

$$\alpha\beta\big(\psi(h_i) + \psi(h_j)\big) = (\alpha_0\beta + \alpha\beta_0)c_0 + \cdots + (\alpha_t\beta + \alpha\beta_t)c_t.$$

Let n be the greatest common divisor of $\alpha\beta$ and the $\alpha_i\beta + \alpha\beta_i$ terms. We define $h_i +_H h_j$ to be the element h_k that is assigned the tuple

$$\langle \frac{\alpha\beta}{n}, \frac{\alpha_0\beta + \alpha\beta_0}{n}, \ldots, \frac{\alpha_t\beta + \alpha\beta_t}{n} \rangle.$$

Notice that because ψ is onto G, there must be some h_k that is assigned this tuple. In fact, h_k is exactly the element such that $\psi(h_k) = \psi(h_i) +_G \psi(h_j)$.

Lemma 8.24. *H is a group under this definition of $+_H$ and ψ is an isomorphism.*

Proof. It is clear that $+_H$ is defined to mimic $+_G$. That is

$$h_i +_H h_j = h_k \iff \psi(h_i) +_G \psi(h_j) = \psi(h_k).$$

The fact that G is a group implies that H is a group and this equivalence shows that ψ is an isomorphism. □

The set of elements $\{b_0, b_1, \ldots\}$ is a basis for H. This set is computably enumerable and so is its complement. To test if g is not one of the b_i, just look for an equation of the form

$$\alpha x = \alpha_0 b_0 + \cdots + \alpha_t b_t$$

that is satisfied by g. Thus, H has a computable basis, which completes the proof of Theorem 8.19. □

Theorem 8.25. *Every computable torsion free abelian group is classically isomorphic to a computable group with a computable order.*

Proof. Let G be a computable torsion free abelian group. Theorem 8.18 has already handled the case when G has finite rank. If G has infinite rank, then let H be as in Theorem 8.19. By Lemma 8.17, H has a computable order. □

As in Section 8.2, we would like to extend this result to the class of nilpotent groups. Unfortunately, for reasons explained below, we are only able to extend it to finitely generated nilpotent groups.

The class of finitely generated nilpotent groups has been extensively studied in computational algebra. These groups has many nice computational properties. For example, every finitely generated nilpotent group is finitely presented, they have the max property, which implies that every subgroup is finitely generated, and they are residually finite which implies that the word problem is solvable. In addition, the conjugacy and isomorphism problems are solvable.

Theorem 8.26 (Baumslag et al. (1991)). *Let G be a computable finitely generated nilpotent group. Each term in the upper central series of G is computable.*

Theorem 8.27. *If G be a computable torsion free finitely generated nilpotent group, then G has a computable order.*

Proof. The idea is to build up the computable order using the terms in the upper central series as in Section 8.2. Notice that since each subgroup $\zeta_i(G)$ is computable, the factors $\zeta_{i+1}(G)/\zeta_i(G)$ are computable. Also, because every subgroup of G is finitely generated, the groups $\zeta_{i+1}(G)/\zeta_i(G)$ are finitely generated torsion free abelian groups. In particular, they have finite rank and therefore, by Theorem 8.18, they are computably orderable.

All that remains is to put together the computable orders on the finite number of fact groups. Because $\zeta_1(G)$ is a subgroup of G, $\zeta_1(G)$ is finitely generated and so computably orderable. Combining this order with a computable order on $\zeta_2(G)/\zeta_1(G)$ induces a computable order on $\zeta_2(G)$. We continue ordering the terms of the upper central series until we reach G. □

The proof of Theorem 8.27 does not work for infinitely generated nilpotent groups because the terms in the upper central series are not necessarily computable. In Theorem 3.28, we saw that even for 2 step nilpotent groups, the center need not be computable.

Appendix A

Miscellaneous Definitions and Proofs

In this appendix, we present some of the background definitions and technical proofs required in Chapter 5. Section A.1 contains the definitions and basic facts about free groups and free products. Section A.2 contains the proofs of the basic formulas for the class of triangular matrices. Section A.3 contains the proofs of the formulas used in the embedding of the free product $A * B$ into the class of triangular matrices.

A.1 Free Groups and Free Products

Let $A \subseteq \mathbb{N}$. For the purposes of defining the free group on the set of generators A, it is convenient to think of the elements of A as distinct symbols in some alphabet. Let a^1 stand for the pair $\langle a, 1 \rangle$ and a^{-1} stand for the pair $\langle a, -1 \rangle$. In this section ϵ will always denote either 1 or -1, and hence a^ϵ is either $\langle a, 1 \rangle$ or $\langle a, -1 \rangle$.

Definition A.1. (RCA_0) If $A \subseteq \mathbb{N}$, then the set of **words over A**, denoted by Word_A, is the set of finite sequences of pairs $\langle a, \epsilon \rangle$ where $a \in A$ and $\epsilon = \pm 1$. In our notation,

$$\text{Word}_A = \text{Fin}_{\tilde{A}}$$

where $\tilde{A} = \{a^\epsilon \mid a \in A \wedge \epsilon = \pm 1\}$. The empty sequence in Word_A is denoted by 1_A.

In keeping with standard mathematical notation, we write $a_1^{\epsilon_1} \cdots a_k^{\epsilon_k}$ for the sequence $\sigma \in \text{Word}_A$ with $\sigma(i) = a_i^{\epsilon_i}$ for $1 \leq i \leq k$. We also write $w_1 \cdot w_2$ for the concatenation of the sequences w_1, w_2 in Word_A.

A sequence $x \in \text{Word}_A$ is called reduced if there is no place in the sequence where a^1 and a^{-1} appear next to each other for any $a \in A$. This notion is defined formally below.

Definition A.2. (RCA_0) The set of **reduced words over A**, denoted by Red_A, is the subset of Word_A such that $x \in \text{Red}_A$ if and only if $x \in \text{Word}_A$ and

$$\forall i < (\text{lh}(x) - 1) \; \big(\; \pi_1(x(i)) \neq \pi_1(x(i+1)) \vee \pi_2(x(i)) = \pi_2(x(i+1)) \; \big)$$

where π_1 and π_2 are the standard projection functions on pairs.

Both Word_A and Red_A have Σ^0_0 definitions, so RCA_0 proves they exist. We next want to define an equivalence relation on Word_A such that each equivalence class contains exactly one element of Red_A. This equivalence relation is used to put a group structure on Red_A. Two words are 1 step equivalent if either they are the same sequence or one results from the other by deleting a pair a^1, a^{-1} that appear next to each other.

Definition A.3. (RCA_0) Two words $x, y \in \text{Word}_A$ are **1 step equivalent**, $x \sim_1 y$, if and only if one of the following conditions holds:

1. $x = y$
2. $\text{lh}(x) = \text{lh}(y) + 1$ and

$$\exists i < \text{lh}(x) \Big(\forall j < i \,\big(x(j) = y(j)\big) \wedge \\ \wedge\ \forall j \geq i\ \big(\ j < \text{lh}(y) \rightarrow y(j) = x(j+2)\ \big) \wedge \\ \wedge\, \pi_1(x(i+1)) = \pi_1(x(i)) \wedge \pi_2(x(i+1)) + \pi_2(x(i)) = 0\Big)$$

3. Same as 2 with the roles of x and y switched.

The elements $x(i)$ and $x(i+1)$ are said to be **cancelled** in x or **inserted** in y.

The conditions in this definition are Σ^0_0 so RCA_0 proves the existence of the set of all pairs $\langle x, y\rangle$ with $x \sim_1 y$.

Definition A.4. (RCA_0) Two words $x, y \in \text{Word}_A$ are **freely equivalent**, $x \sim y$, if there is a finite sequence σ of elements of Word_A such that

1. $\sigma(0) = x$
2. $\sigma(\text{lh}(\sigma) - 1) = y$
3. $\sigma(i) \sim_1 \sigma(i+1)$ for all $i < \text{lh}(\sigma) - 1$.

This defines an equivalence relation. Notice that the condition in this definition is Σ^0_1, so we have to work harder to prove the existence of the set of pairs $\langle x, y\rangle$ with $x \sim y$ in RCA_0. In order to form this set, we define a function ρ by recursion.

$$\rho : \text{Word}_A \rightarrow \text{Red}_A$$
$$\rho(1_A) = 1_A$$
$$\rho(a^\epsilon) = a^\epsilon \text{ for } a \in A, \epsilon = \pm 1$$

If $\rho(U) = a_1^{\epsilon_1} \cdots a_k^{\epsilon_k}$ then

$$\rho(U \cdot a^\epsilon) = \begin{cases} a_1^{\epsilon_1} \cdots a_k^{\epsilon_k} a^\epsilon & \text{if } a \neq a_k \text{ or } a = a_k \wedge \epsilon_k + \epsilon \neq 0 \\ a_i^{\epsilon_1} \cdots a_{k-1}^{\epsilon_{k-1}} & \text{if } a = a_k \wedge \epsilon_k + \epsilon = 0 \end{cases}$$

Lemma A.5. *(RCA_0) The following properties hold of ρ for all words W, W_1 and W_2 in $Word_A$ and all $a \in A$.*

1. $\rho(W) \in Red_A$
2. $\rho(W) \sim W$
3. $W \in Red_A \to \rho(W) = W$
4. $\rho(W_1 \cdot W_2) = \rho(\rho(W_1) \cdot W_2)$
5. $\rho(W \cdot a^\epsilon \cdot a^{-\epsilon}) = \rho(W)$
6. $\rho(W_1 \cdot a^\epsilon \cdot a^{-\epsilon} \cdot W_2) = \rho(W_1 \cdot W_2)$

Proof. The proofs are all by induction either on the length of W or on the length of W_2. To prove that $\rho(W) \in \text{Red}_A$, we prove $\forall n \varphi(n)$ by induction where $\varphi(n)$ is

$$\text{lh}(W) = n \to \rho(W) \in \text{Red}_A.$$

The only element of Word_A with length 0 is 1_A. Since $\rho(1_A) = 1_A$, we have that $\varphi(0)$ holds. If $\text{lh}(W) = 1$, then $W = a^\epsilon$ for some $a \in A$. By the definition of ρ, $\rho(a^\epsilon) = a^\epsilon$ and so $\varphi(1)$ holds. In the case when $\text{lh}(W) > 1$, we write W as the concatenation $W = U \cdot a^\epsilon$. By the induction hypothesis, $\rho(U) \in \text{Red}_A$. Assume $\rho(U) = a_1^{\epsilon_1} \cdots a_k^{\epsilon_k}$ and split into two cases.

If $a_k \neq a$ or $a_k = a$ but $\epsilon_k + \epsilon \neq 0$, then by definition $\rho(W) = a_1^{\epsilon_1} \cdots a_k^{\epsilon_k} a^\epsilon$ and $\rho(W) \in \text{Red}_A$. If $a_k = a$ and $\epsilon_k + \epsilon = 0$, then $\rho(W) = a_1^{\epsilon_1} \cdots a_{k-1}^{\epsilon_{k-1}}$. Again, since $\rho(U) \in \text{Red}_A$ we have $\rho(W) \in \text{Red}_A$. This proves property (1).

To prove $\rho(W) \sim W$, we use Σ^0_1 induction on $\text{lh}(W)$. If $\text{lh}(W) = 0$ or $\text{lh}(W) = 1$, then the argument is the same as for property 1. Assume $\text{lh}(W) > 1$ and $W = U \cdot a^\epsilon$ with $U \sim \rho(U) = a_1^{\epsilon_1} \cdots a_k^{\epsilon_k}$. Let σ be the sequence which shows the free equivalence of U and $\rho(U)$. Split into the same two cases as in the proof of property 1. If $\rho(W) = a_1^{\epsilon_1} \cdots a_k^{\epsilon_k} a^\epsilon$ then $\tilde{\sigma}$ gives the free equivalence of W and $\rho(W)$ where $\tilde{\sigma}$ is defined from σ by

$$\tilde{\sigma}(i) = \sigma(i) a^\epsilon.$$

If $\rho(W) = a_1^{\epsilon_1} \cdots a_{k-1}^{\epsilon_{k-1}}$ then $\tilde{\sigma}$ gives the free equivalence of W and $\rho(W)$ where $\tilde{\sigma}$ is defined by

$$\forall i < \text{lh}(\sigma)(\tilde{\sigma}(i) = \sigma(i) \cdot a^\epsilon)$$
$$\tilde{\sigma}(\text{lh}(\sigma)) = \rho(W)).$$

To verify that this proof is indeed Σ^0_1 induction, notice that we proved $\forall n \varphi(n)$ where

$$\varphi(n) \equiv (W \in \text{Word}_A \wedge \text{lh}(W) = n) \to \rho(W) \sim W.$$

$\varphi(n)$ is Σ^0_1.

The proofs of the remaining properties involve similar case analysis, except for the last property. Property 6 is a direct consequence of Properties 3 and 5. For more details, see Magnus et al. (1965) □

Lemma A.6. *(RCA_0) If $x \sim y$ then $\rho(x) = \rho(y)$.*

Proof. From the definition of 1 step equivalence and from Property 6 of Lemma A.5, it follows that if $x \sim_1 y$, then $\rho(x) = \rho(y)$. Assume $x \sim y$ and let σ be the sequence that shows $x \sim y$. Since $\sigma(i) \sim_1 \sigma(i+1)$ for all $i < (\mathrm{lh}(\sigma) - 1)$, we have $\rho(\sigma(i)) = \rho(\sigma(i+1))$. Thus, $\rho(\sigma(0)) = \rho(\sigma(\mathrm{lh}(\sigma) - 1))$ and so $\rho(x) = \rho(y)$. □

Proposition A.7. *(RCA_0) For every $x \in Word_A$ there is a unique $y \in Red_A$ such that $x \sim y$.*

Proof. Since $\rho(x) \in \mathrm{Red}_A$ and $x \sim \rho(x)$, we know that there is at least one $y \in \mathrm{Red}_A$ such that $x \sim y$. It remains to show that if $x \sim y$ and $y \in \mathrm{Red}_A$ then $y = \rho(x)$. Because $x \sim y$ implies that $\rho(x) = \rho(y)$ and $y \in \mathrm{Red}_A$ implies $\rho(y) = y$, we have $\rho(x) = y$ as required. □

Because free equivalence is an equivalence relation, it follows that if $\rho(x) = \rho(y)$ then $x \sim y$. Together with Lemma A.6 this shows that $x \sim y$ if and only if $\rho(x) = \rho(y)$. The set of pairs $\langle x, y\rangle$ such that $x \sim y$ can be formed by Σ^0_0 comprehension.

$$\{\langle x, y\rangle \mid x \sim y\} \;=\; \{\langle x, y\rangle \mid \rho(x) = \rho(y)\}$$

Using this set, we can give the formal definition of the free group on the set of generators A.

Definition A.8. (RCA_0) Let $A \subseteq \mathbb{N}$. The set of elements of the **free group on the set of generators A** is Red_A. The empty sequence 1_A is the identity element and multiplication is defined by

$$x \cdot y = \rho(x \cdot y)$$

where $\rho(x \cdot y)$ is ρ applied to the concatenation of the strings x and y.

The definition of the free product of two groups $A * B$ is similar to this definition of free groups. Instead of using sequences of generators and inverses as elements, we will use sequences whose elements alternate between A and B. For example, if $a_i \in A$ and $b_i \in B$ then strings such as

$$\langle a_1, b_3, a_2\rangle \text{ and } \langle b_2, a_1\rangle$$

are in $A * B$. To form this group, we start with the set of finite strings over $A \cup B$. Strings are reduced by removing occurrences of 1_A and 1_B and by multiplying elements of the same group which appear next to each other in the string. For example,

$$\langle a_1, 1_A, b_2, b_3\rangle \;\mapsto\; \langle a_1, b_2 \cdot_B b_3\rangle.$$

The definitions and lemmas for free products parallel those given for free groups.

Definition A.9. (RCA_0) If A, B are groups then Word_{A*B} is the set of finite sequences of elements of $A \cup B$.

$$\mathrm{Word}_{A*B} = \mathrm{Fin}_{A\cup B}$$

1_{A*B} denotes the empty sequence.

Definition A.10. (RCA_0) The set of **reduced words**, Red_{A*B}, is the subset of Word_{A*B} such that $x \in \mathrm{Red}_{A*B}$ if and only if $x \in \mathrm{Word}_{A*B}$ and one of the following conditions holds:

1. $x = 1_{A*B}$
2. For all $i < \mathrm{lh}(x)$, $\sigma(i)$ is not 1_A or 1_B, and for all $i < (\mathrm{lh}(x) - 1)$, if $\sigma(i) \in A$ then $\sigma(i+1) \in B$ and if $\sigma(i) \in B$ then $\sigma(i+1) \in A$.

Definition A.11. (RCA_0) Two words $x, y \in \mathrm{Word}_{A*B}$ are **1 step equivalent**, $x \sim_1 y$, if and only if one of the following conditions holds:

1. $x = y$
2. $\mathrm{lh}(x) = \mathrm{lh}(y) + 1$ and the sequence y is the same as x except one occurrence of 1_A or 1_B is removed.
3. $\mathrm{lh}(x) = \mathrm{lh}(y) + 1$ and the sequence y is the same as x except there is an $i < \mathrm{lh}(y)$ such that either $x(i), x(i+1) \in A$ and $y(i) = x(i) \cdot_A x(i+1)$ or $x(i), x(i+1) \in B$ and $y(i) = x(i) \cdot_B x(i+1)$.
4. Switch the roles of x and y in condition 2.
5. Switch the roles of x and y in condition 3.

Definition A.12. (RCA_0) Two words $x, y \in \mathrm{Word}_{A*B}$ are **freely equivalent**, $x \sim y$, if there exists a finite sequence σ of elements of Word_{A*B} such that

1. $\sigma(0) = x$
2. $\sigma(\mathrm{lh}(\sigma) - 1) = y$
3. $\forall i < (\mathrm{lh}(\sigma) - 1)\ (\sigma(i) \sim_1 \sigma(i+1))$.

As in the case of free groups, this is a Σ^0_1 condition and so we have to use a function $\rho : \mathrm{Word}_{A*B} \to \mathrm{Red}_{A*B}$ to help form the set of pairs $\langle x, y\rangle$ with $x \sim y$. Unlike the case of free groups, we will retain the sequence notation to make the definition clearer.

$$\rho(1_{A*B}) = 1_{A*B}$$

$$\rho(\langle g\rangle) = \begin{cases} 1_{A*B} & \text{if } g = 1_A \vee g = 1_B \\ \langle g\rangle & \text{otherwise} \end{cases}$$

If $\rho(U) = \langle h_1, h_2, \ldots, h_r\rangle$ then

$$\rho(U^\frown\langle g\rangle) = \begin{cases} \langle h_1, \ldots, h_r\rangle & \text{if } g = 1_A \ \vee \ g = 1_B \\ \langle h_1, \ldots, h_{r-1}\rangle & \text{if } g = h_r^{-1} \\ \langle h_1, \ldots, h_r, g\rangle & \text{if } (g \in A \setminus 1_A \wedge h_r \in B) \\ & \quad \vee\ (g \in B \setminus 1_B \wedge h_r \in A) \\ \langle h_1, \ldots, h_{r-1}, h_r \cdot_A g\rangle & \text{if } g \in A \setminus 1_A \ \wedge \ h_r \in A \setminus g^{-1} \\ \langle h_1, \ldots h_{r-1}, h_r \cdot_B g\rangle & \text{if } g \in B \setminus 1_B \ \wedge \ h_r \in B \setminus g^{-1} \end{cases}$$

As in the free group case, we want to show that each word in Word_{A*B} is freely equivalent to a unique reduced word. To prove this fact, we prove various properties of ρ.

Lemma A.13. *(RCA_0) The following properties of ρ hold for all W_1, W_2, W in $Word_{A*B}$.*

1. $\rho(W) \in Red_{A*B}$
2. $\rho(W) \sim W$
3. $W \in Red_{A*B} \to \rho(W) = W$
4. $\rho(W_1^\frown W_2) = \rho(\rho(W_1)^\frown W_2)$
5. $\rho(W^\frown\langle 1_A\rangle) = \rho(W^\frown\langle 1_B\rangle) = \rho(W)$
6. $\rho(W_1^\frown\langle 1_A\rangle^\frown W_2) = \rho(W_1^\frown\langle 1_B\rangle^\frown W_2) = \rho(W_1^\frown W_2)$
7. *If* $g, h \in A$ *then* $\rho(W^\frown\langle g, h\rangle) = \rho(W^\frown\langle g \cdot_A h\rangle)$
8. *If* $g, h \in B$ *then* $\rho(W^\frown\langle g, h\rangle) = \rho(W^\frown\langle g \cdot_B h\rangle)$
9. *If* $g, h \in A$ *then* $\rho(W_1^\frown\langle g, h\rangle^\frown W_2) = \rho(W_1^\frown\langle g \cdot_A h\rangle^\frown W_2)$
10. *If* $g, h \in B$ *then* $\rho(W_1^\frown\langle g, h\rangle^\frown W_2) = \rho(W_1^\frown\langle g \cdot_B h\rangle^\frown W_2)$

The proof of this lemma is a series of inductions as in Lemma A.5. For more details, see Magnus et al. (1965). As in the free group case, we use this lemma to show that $x \sim y$ if and only if $\rho(x) = \rho(y)$. The proof of the following proposition is also the same as in the free group case.

Proposition A.14. *(RCA_0) For every $x \in Word_{A*B}$ there is a unique $y \in Red_{A*B}$ such that $x \sim y$.*

From this proposition, we obtain

$$\{\langle x, y\rangle \mid x \sim y\} = \{\langle x, y\rangle \mid \rho(x) = \rho(y)\}.$$

Thus, RCA_0 can form the set of pair $\langle x, y\rangle$ such that $x \sim y$. Using this set we give the formal definition of the free product $A * B$.

Definition A.15. (RCA_0) The set of elements of the **free product** of the groups A and B, denoted $A*B$, is Red_{A*B}. The empty sequence 1_{A*B} is the identity element and multiplication is given by

$$x \cdot y = \rho(x^\frown y).$$

Unraveling the definitions, we can find a connection between free products of $\mathbb{Z}$ and free groups.

Proposition A.16. *(RCA_0) The free product $\mathbb{Z} * \mathbb{Z}$ is isomorphic to F_2, the free group on two generators.*

Proof. Let a, b denote the generators of F_2. A typical element of F_2 has the form $\langle a, a, b^{-1}, a, b, b \rangle$. For notational convenience, let a also denote 1 in the first copy of $\mathbb{Z}$ and b denote 1 in the second copy of $\mathbb{Z}$. A typical element of $\mathbb{Z} * \mathbb{Z}$ has the form $\langle 2a, -b, a, 2b \rangle$. The isomorphism is built by expanding elements resembling na in sequences in $\mathbb{Z} * \mathbb{Z}$ to n-tuple $\langle a, a, \ldots, a \rangle$. For example

$$\langle 2a, -b, a, 2b \rangle \;\mapsto\; \langle a, a, b^{-1}, a, b, b \rangle.$$

Writing this map formally, we obtain the isomorphism. □

A.2 Proofs for $\mathbf{Tri}_{\mathbb{Q}[C]}$

In this section, we prove some of the technical results about Tri_K that were left out of Chapter 5. We are looking at the class of infinite upper triangular matrices with entries from an f.o. ring K such that the elements along the main diagonal are positive and invertible.

Definition A.17. (RCA_0) Let $(K, \leq)$ be a fully ordered ring with positive cone P. The function $f : \mathbb{N}^+ \times \mathbb{N}^+ \to K$ is in the class Tri_K if and only if it satisfies the following conditions:

1. For all $i > j$, $f(i,j) = 0_K$.
2. For all i, $f(i,i) \in P$ and $\exists x \in K(f(i,i) \cdot x = 1_K)$.

We use the notation $f \in \mathrm{Tri}_K$ to mean that f is a function satisfying the conditions of this definition. The product of f and g is defined to be the function

$$f \cdot g : \mathbb{N}^+ \times \mathbb{N}^+ \to K$$
$$f \cdot g(i,j) = \sum_{n=i}^{j} f(i,n) g(n,j).$$

The identity function $I \in \mathrm{Tri}_K$ is given by $I(i,i) = 1_K$ and $I(i,j) = 0_K$ for $i \neq j$.

Given $f, g \in \mathrm{Tri}_K$, we say that $f < g$ if and only if for some pair $\langle i,j \rangle \in \mathbb{N}^+ \times \mathbb{N}^+$ with $i \leq j$ the following two conditions hold:

1. $f(i,j) <_K g(i,j)$
2. $f(k, k+s) = g(k, k+s)$ for all k, s such that $i + s < j$ or $i + s = j$ and $k < i$.

A pair $\langle i, j\rangle$ for which these conditions hold is called a witness for $f < g$. Writing this condition in terms of a positive cone, we say that $f \in P(\mathrm{Tri}_K)$ if and only if $f = I$ or $I < f$ in the order given above. If $f \neq I$ this is equivalent to either

$$\exists i\ [f(i,i) > 1 \wedge \forall j < i(f(j,j) = 1)]$$

or

$$\forall i\ (f(i,i) = 1)\ \wedge\ \exists i,j\ [\ i < j \wedge f(i,j) > 0\ \wedge$$
$$\wedge\ \forall k\ \forall s > 0\ ((i+s < j \vee (i+s = j \wedge k < i)) \rightarrow f(k,k+s) = 0)\ ].$$

We want to verify that the elements of Tri_K satisfy the axioms of a f.o. group. In Chapter 5, we proved in RCA_0 that the multiplication is associative. Here, we verify that there are inverse elements and that $P(\mathrm{Tri}_K)$ is normal, pure and closed under multiplication. As pointed out in Chapter 5, RCA_0 is not strong enough to show that $P(\mathrm{Tri}_K)$ is full.

Lemma A.18. *(RCA_0) If $f \in Tri_K$, then f has an inverse $g \in Tri_K$, in the sense that $f \cdot g = g \cdot f = I$, given by:*

$$g(i,j) = \begin{cases} 0 & j < i \\ f(i,j)^{-1} & i = j \\ -\frac{f(i,j)}{f(i,i)f(j,j)} + \sum_{i<k_1<j} \frac{f(i,k_1)f(k_1,j)}{f(i,i)f(k_1,k_1),f(j,j)} - & \\ \quad - \sum_{i<k_1<k_2<j} \frac{f(i,k_1)f(k_1,k_2)f(k_2,j)}{f(i,i)f(k_1,k_1)f(k_2,k_2)f(j,j)} + \cdots & i < j \\ \quad \cdots + (-1)^{j-i} \frac{f(i,i+1)\cdots f(j-1,j)}{f(i,i)f(i+1,i+1)\cdots f(j,j)} & \end{cases}$$

Since $f(n,n)$ is invertible, we write it in the denominator of a fraction as shorthand for $f(n,n)^{-1}$.

Proof. We verify that $f \cdot g(i,j) = I(i,j)$ by splitting into the cases of $i = j$, $i < j$ and $i > j$. If $i = j$ then

$$f \cdot g(i,j) = f(i,i)f(i,i)^{-1} = 1.$$

If $i > j$ then we have already noted that for $f, g \in \mathrm{Tri}_K$

$$f \cdot g(i,j) = 0.$$

The case for $i < j$ is more complicated. For each fixed j, this case is proved by induction on $j - i$. The base case is when $j - i = 0$ and is given by our calculation above. If $j - i = l$, then the induction hypothesis is that the formula is correct for $g(j-k, j)$ for all $0 \leq k < l$. We need to show that $f \cdot g(j-l, j) = 0$. To prove this, we start by assuming that $f \cdot g = I$ and work backwards to derive $g(j-l, j)$. If $f \cdot g(j-l, j) = 0$ then we must have

$$f(j-l, j-l)g(j-l, j) + f(j-l, j-l+1)g(j-l+1, j) + \cdots$$
$$\cdots + f(j-l, j)g(j,j) = 0.$$

Solving this equation for $g(j-l, j)$ we have

$$g(j-l, j) = \sum_{n=0}^{l-1} - \frac{f(j-l, j-n)}{f(j-l, j-l)} g(j-n, j). \tag{A.1}$$

To finish the proof, we need to show that this sum is equal to

$$\begin{aligned} & - \frac{f(j-l, j)}{f(j-l, j-l) f(j, j)} + \sum_{k_1=1}^{l-1} \frac{f(j-l, j-k_1) f(j-k_1, j)}{f(j-l, j-l) f(j-k_1, j-k_1) f(j, j)} - \\ & - \sum_{k_1=1}^{l-2} \sum_{k_2=k_1+1}^{l-1} \frac{f(j-l, j-k_2) f(j-k_2, j-k_1) f(j-k_1, j)}{f(j-l, j-l) f(j-k_1, j-k_1) f(j-k_2, j-k_2) f(j, j)} + \cdots \\ & \cdots + (-1)^l \frac{f(j-l, j-l+1) f(j-l+1, j-l+2) \cdots f(j-1, j)}{f(j-l, j-l) f(j-l+1, j-l+1) \cdots f(j, j)}. \end{aligned} \tag{A.2}$$

To prove this equality, we will split equation (A.2) into a sum with summands of the form

$$- \frac{f(j-l, j-n)}{f(j-l, j-l)} \cdot X$$

and show that $X = g(j-n, j)$. For the case $n = 0$ we see that

$$- \frac{f(j-l, j)}{f(j-l, j-l)}$$

appears only in the first summand of equation (A.2). That is, it only appears in

$$- \frac{f(j-l, j)}{f(j-l, j-l) f(j, j)}.$$

In this case $X = f(j, j)^{-1} = g(j, j)$ as required.

For the case of $n = 1$

$$- \frac{f(j-l, j-1)}{f(j-l, j-l)}$$

appears only in the second sum of equation (A.2) and only when $k_1 = 1$. Thus in this case, we have

$$X = - \frac{f(j-1, j)}{f(j-1, j-1) f(j, j)}.$$

By the bounded induction hypothesis, this is exactly $g(j-1, j)$.

In general, for $1 \leq n < l$, we have

$$- \frac{f(j-l, j-n)}{f(j-l, j-l)}$$

does not appear in the first summand, but does appear in each of the other summands of equation (A.2) up to the $(n+1)^{\text{st}}$ one. If we examine how it appears in each of these summands, we see that in the 2^{nd} term, we get

$$-\frac{f(j-n,j)}{f(j-n,j-n)f(j,j)}$$

which is exactly the first term in $g(j-n,j)$. From the 3^{rd} term, we have something every time $k_2 = n$ and hence we get

$$\sum_{k_1=1}^{n-1} \frac{f(j-n,j-k_1)f(j-k_1,j)}{f(j-n,j-n)f(j-k_1,j-k_1)f(j,j)}.$$

This sum is exactly the second term in $g(j-n,j)$. This process continues until we reach the $(n+1)^{\text{st}}$ term. From this term, we only get something when $k_1 = 1, k_2 = 2, \ldots k_n = n$. This give us

$$(-1)^n \frac{f(j-n,j-n+1)\cdots f(j-1,j)}{f(j-n,j-n)\cdots f(j,j)}.$$

This product is exactly the last term of $g(j-n,j)$ and shows $X = g(j-n,j)$ as required. We have now shown that $f \cdot g = I$. From here, we have that $g \cdot f \cdot g = g$. By a simpler induction, it can be shown that if $h \cdot g = g$ then $h = I$. Hence $g \cdot f = I$ as well. □

Lemma A.19. *(RCA_0)*

1. *If $f, g \in P(\mathit{Tri}_K)$ then $f \cdot g \in P(\mathit{Tri}_K)$*
2. *If $f \in P(\mathit{Tri}_K)$ and $f \neq I$ then $f^{-1} \notin P(\mathit{Tri}_K)$*
3. *If $f \in P(\mathit{Tri}_K)$ and $g \in \mathit{Tri}_K$ then $gfg^{-1} \in P(\mathit{Tri}_K)$*

Proof. To prove the first statement of the lemma, assume $f, g \in P(\mathrm{Tri}_K)$. For notational purposes, let $h = f \cdot g$. We need to show $h \in P(\mathrm{Tri}_K)$. Without loss of generality, assume that $f, g, h \neq I$. There are two cases to consider.

Case. $\exists i(f(i,i) \neq 1 \vee g(i,i) \neq 1)$

Let i be the least such number. Then, $h(i,i) = f(i,i)g(i,i) > 1$ and for all $j < i$, $h(j,j) = 1$. Thus $h \in P(\mathrm{Tri}_K)$.

Case. $\forall i(f(i,i) = 1 \wedge g(i,i) = 1)$

Let the pair $\langle i,j \rangle$ be a witness for $f > I$. Without loss of generality, assume that $g(i,j) \geq 0$ and that $g(k,k+s) = 0$ for all k and $s > 0$ such that $i + s < j$ or $i + s = j$ and $k < i$. That is, assume that the witness to $g > I$ comes later in the order on the diagonals than the witness for f. We need to show that $h(i,j) > 0$, that $h(k,k+s) = 0$ for k, s as above and that $h(n,n) = 1$ for all n.

Since $f(n,n) = g(n,n) = 1$, it is clear that $h(n,n) = 1$. To show that $h(i,j) > 0$, we examine

$$h(i,j) = \sum_{n=i}^{j} f(i,n)g(n,j).$$

By the assumptions made above on f and g, we have that $f(i,i) = g(j,j) = 1$ and $f(i,i+1)$ though $f(i,j-1)$ are all 0. Thus, this sum reduces to $g(i,j) + f(i,j)$. Since $g(i,j) \geq 0$ and $f(i,j) > 0$, we have that $h(i,j) > 0$ are required.

Suppose $s > 0$, $i + s < j$ or $i + s = j$ and $k < i$. We have the following equalities:

$$\begin{aligned} h(k,k+s) &= \sum_{n=k}^{k+s} f(k,n)g(n,k+s) \\ &= \sum_{n=0}^{s} f(k,k+n)g(k+n,k+s) \\ &= f(k,k)g(k,k+s) + f(k,k+s)g(k+s,k+s) + \\ &\quad + \sum_{n=1}^{s-1} f(k,k+n)g(k+n,k+s). \end{aligned}$$

The first term in the last equation is 0 because $g(k,k+s) = 0$. The second term is 0 because $f(k,k+s) = 0$. For the third term, since $i+s \leq j$ we have that $i+n < j$ for all n in the sum. Thus $f(k,k+n) = 0$ and the third term is 0. This shows that $h(k,k+s) = 0$ and finishes the proof of the first statement of the lemma.

To prove the second assertion of the lemma, assume that $f \neq I$, $f \in P(\mathrm{Tri}_K)$ and $g = f^{-1}$. We need to show that $g \notin P(\mathrm{Tri}_K)$. There are two cases to consider.

Case. $\exists i(f(i,i) \neq 1)$

Let i be the least such number. Since $f \in P(\mathrm{Tri}_K)$ we know $f(i,i) > 1$. By the formula for inverses, $g(i,i) = f(i,i)^{-1} < 1$. Hence, $g \notin P(\mathrm{Tri}_K)$.

Case. $\forall i(f(i,i) = 1)$

It follows from the formula for inverses that $g(i,i) = 1$ for all i as well. Let the pair $\langle i,j \rangle$ be a witness for $f > I$. Using the formula for inverses and the fact that $f(i,i) = 1$ for all i, we have

$$g(i,j) = -f(i,j) \;+ \sum_{i<k_1<j} f(i,k_1)f(k_1,j) \;- \cdots$$
$$\cdots (-1)^{j-i}\big(f(i,i+1)f(i+1,i+2)\cdots f(j-1,j)\big).$$

For any subscripted k appearing in this sum we have $i < k < j$ and we can set $s = k - i$. It follows that $i + s = k < j$ and so by the assumptions on f

$$f(i,k) = f(i,i+s) = 0.$$

All terms in $g(i,j)$ vanish except for the first one. This computation shows that $g(i,j) = -f(i,j) < 0$. It remains to show that $g(k,k+s) = 0$ for k and s such that $s > 0$ and either $i + s < j$ or $i + s = j$ and $k < i$. Using the formula for inverses again and the fact that $f(i,i) = 1$ we have

$$g(k,k+s) = -f(k,k+s) + \sum_{0<n_1<s} f(k,k+n_1)f(k+n_1,k+s) - \cdots$$
$$\cdots + (-1)^{j-i}(f(k,k+1)\cdots f(k+s-1,k+s)).$$

Again, by the restrictions on f, this sum is 0. Hence, the pair $\langle i,j\rangle$ is the witness for $g \notin P(\mathrm{Tri}_K)$.

To verify the third statement of the lemma, let $f \in P(\mathrm{Tri}_K)$ and $g \in \mathrm{Tri}_K$. For notational simplicity, let $h = gfg^{-1}$. We need to show that $h \in P(\mathrm{Tri}_K)$. Again, there are two cases to consider.

Case. $\exists i(f(i,i) > 1)$

In this case we have:

$$h(i,i) = g(i,i)f(i,i)g(i,i)^{-1} = f(i,i).$$

Thus, $h(i,i) > 1$ and for all $j < i$, $h(j,j) = 1$ as required.

Case. $\forall i(f(i,i) = 1)$

Let $\langle i,j\rangle$ be the witness for $f \in P(\mathrm{Tri}_K)$. It is clear that $h(i,i) = 1$ for all i. We need to show that the pair $\langle i,j\rangle$ is a witness for $h \in P(\mathrm{Tri}_K)$. First, we show that $h(i,j) > 0$. We have

$$h(i,j) = \sum_{n=i}^{j}(g\cdot f)(i,n)g^{-1}(n,j)$$
$$(g\cdot f)(i,n) = \sum_{m=i}^{n} g(i,m)f(m,n).$$

Consider $f(m,n)$ as it appears in $(g\cdot f)(i,n)$ for $n < j$. When $i \le m < n < j$, we have by the assumptions on f and $\langle i,j\rangle$ that $f(m,n) = 0$. Also, $f(n,n) = 1$. Hence, we have

$$n < j \Rightarrow (g\cdot f)(i,n) = g(i,n)f(n,n) = g(i,n)$$
$$n = j \Rightarrow (g\cdot f)(i,n) = g(i,i)f(i,j) + g(i,j).$$

Putting this back into the formula for $h(i,j)$ we have:

$$\begin{aligned} h(i,j) &= \sum_{n=i}^{j} (g \cdot f)(i,n) g^{-1}(n,j) \\ &= \sum_{n=i}^{j-1} (g \cdot f)(i,n) g^{-1}(n,j) \;+ (g \cdot f)(i,j) g^{-1}(j,j) \\ &= \sum_{n=i}^{j-1} g(i,n) g^{-1}(n,j) \;+ \big(g(i,i) f(i,j) + g(i,j)\big) g^{-1}(j,j) \\ &= \sum_{n=i}^{j-1} g(i,n) g^{-1}(n,j) \;+ g(i,i) f(i,j) g^{-1}(j,j) + g(i,j) g^{-1}(j,j). \end{aligned}$$

Using the facts that $I = g \cdot g^{-1}$ and $I(i,j) = 0$ we have

$$\begin{aligned} I(i,j) &= \sum_{n=i}^{j} g(i,n) g^{-1}(n,j) \\ 0 &= \sum_{n=i}^{j-1} g(i,n) g^{-1}(n,j) \;+ g(i,j) g^{-1}(j,j) \\ -\sum_{n=i}^{j-1} g(i,n) g^{-1}(n,j) &= g(i,j) g^{-1}(j,j). \end{aligned}$$

Plugging this into the formula above, we obtain

$$\begin{aligned} h(i,j) &= \sum_{n=i}^{j-1} g(i,n) g^{-1}(n,j) + g(i,i) f(i,j) g^{-1}(j,j) - \sum_{n=i}^{j-1} g(i,n) g^{-1}(n,j) \\ &= g(i,i) f(i,j) g^{-1}(j,j). \end{aligned}$$

Since each of $g(i,i)$, $f(i,j)$, and $g^{-1}(j,j)$ are strictly positive, we have that $h(i,j) > 0$. It remains to show that $h(k, k+s)$ for the appropriate k and s.

$$h(k, k+s) = \sum_{n=0}^{s} (g \cdot f)(k, k+n) g^{-1}(k+n, k+s)$$

$$(g \cdot f)(k, k+n) = \sum_{m=0}^{n} g(k, k+m) f(k+m, k+n)$$

Recall that the conditions on k and s are that $s > 0$ and either $s + i < j$ or $s + i = j$ and $k < i$. To examine the bottom equation, let $t = n - m$. From the ranges of the indices on the sums, it follows that $t \leq s$ and $t = s$ only if $n = s$ and $m = 0$. We can use t to write

$f(k+m, k+n)$ as $f(k+m, k+m+t)$. Since $\langle i, j\rangle$ is the witness for $f \in P(\mathrm{Tri}_K)$, we know that if $t > 0$, then $f(k+m, k+m+t) = 0$ if $t+i < j$ or $t+i = j$ and $k+m < i$. We now look at lots of cases. We first split into the cases when $t > 0$ and $t = 0$ and then subdivide further from there.

If $t > 0$ and $s+i < j$ then, since $t \leq s$, we have that $t+i < j$ and so $f(k+m, k+m+t) = f(k+m, k+n) = 0$. Still assuming $t > 0$, suppose that $s+i = j$ and $m+t = n < s$. It follows from $n \neq s$ that $t < s$. Hence, $t+i < j$ and $f(k+m, k+m+t) = 0$. This still leaves the case when $s+i = j$ and $n = s$. We will consider this case last.

Next assume that $t = 0$. This implies that $m = n$ and hence $f(k+m, k+n) = f(k+n, k+n) = 1$. Our calculations so far show that if $n < s$, then all the terms in the sum for $(g \cdot f)(k, k+n)$ drop out except for the $g(k, k+n)f(k+n, k+n)$ term which is just $g(k, k+n)$.

We return to the case when $s+i = j$ and $n = s$. The sum looks like

$$(g \cdot f)(k, k+s) = \sum_{m=0}^{s} g(k, k+m) f(k+m, k+s).$$

If $0 < m < s$ then $f(k+m, k+s) = 0$ since $i+s = j$ and so $i+s-m < j$. Also, $f(k, k+s) = 0$ and $f(k+s, k+s) = 1$. Thus

$$\begin{aligned}(g \cdot f)(k, k+s) &= g(k,k)f(k, k+s) + g(k, k+s)f(k+s, k+s) \\ &= g(k, k+s).\end{aligned}$$

Altogether, we now have that for $0 \leq n \leq s$, $g \cdot f(k, k+n) = g(k, k+n)$. Putting this back into the formula for $h(k, k+s)$ we obtain

$$\begin{aligned}h(k, k+s) &= \sum_{n=0}^{s} (g \cdot f)(k, k+n) g^{-1}(k+n, k+s) \\ &= \sum_{n=0}^{s} g(k, k+n) g^{-1}(k+n, k+s).\end{aligned}$$

As above, we apply the facts that $I = g \cdot g^{-1}$ and $I(k, k+s) = 0$ for $s > 0$ to get

$$0 = \sum_{n=0}^{s} g(k, k+n) g^{-1}(k+n, k+s).$$

Thus, $h(k, k+s) = 0$ as required. $\square$

A.3 Proofs for Free Product Embedding

In this section, we prove the properties of the embedding of $A * B$ into $\mathrm{Tri}_{\mathbb{Q}[C]}$. Recall that A and B are f.o. groups and C is the restricted direct product

$$C = A \times B \times \prod_{i,j=1}^{\infty} \langle x_{ij} \rangle \times \prod_{i,j=1}^{\infty} \langle y_{ij} \rangle \times \prod_{i=1}^{\infty} \langle u_i \rangle \times \prod_{i=1}^{\infty} \langle v_i \rangle$$

$\mathbb{Q}[C]$ is the group ring of C over $\mathbb{Q}$. The elements are the finite formal sums $\sum \alpha_i c_i$ with $\alpha_i \in \mathbb{Q} \setminus \{0\}$, $c_i \in C$ and all the c_i distinct. Addition is defined by

$$\sum_{i \in I} \alpha_i c_i \; + \; \sum_{j \in J} \beta_j c_j \; = \; \sum_{i \in I \setminus J} \alpha_i c_i \; + \; \sum_{j \in J \setminus I} \beta_j c_j \; + \; \sum_{i \in I \cap J} (\alpha_i + \beta_i) c_i$$

with the stipulation that any terms in the third sum with $\alpha_i + \beta_i = 0$ are removed. Multiplication is defined by

$$\left(\sum_{i \in I} \alpha_i c_i \right) \left(\sum_{j \in J} \beta_j c_j \right) \; = \; \sum_{i \in I} \sum_{j \in J} (\alpha_i \beta_j) c_i c_j$$

where the terms with the same value from C in this finite sum are collected and any term with coefficient 0 is dropped. The additive identity here is the empty sum $I = \emptyset$, and the multiplicative identity is the sum with one element $1_{\mathbb{Q}} 1_C$. The sum $\sum_{i \in I} \alpha_i c_i$ is in $P(\mathbb{Q}[C])$ if and only if $I = \emptyset$ or $\alpha_j >_{\mathbb{Q}} 0$ where j is such that c_j is the $\leq_C$-least element among the c_i with $i \in I$.

See Chapter 5 for the definitions of the elements $X, Y, U, V \in \text{Tri}_{\mathbb{Q}[C]}$ and the maps

$$\alpha, \alpha', \alpha'' : A \to \text{Tri}_{\mathbb{Q}[C]}$$
$$\beta, \beta', \beta'' : B \to \text{Tri}_{\mathbb{Q}[C]}$$
$$\gamma : A * B \to \text{Tri}_{\mathbb{Q}[C]}.$$

In Chapter 5, we proved that γ satisfies the properties of a group homomorphism. The proof that γ is one-to-one required the explicit formulas for $\alpha'(a)(i,j)$ and $\beta'(b)(i,j)$ which are proved below.

Lemma A.20. *(RCA_0)*

$$\alpha'(a)(i,i) = \begin{cases} 1 & i \text{ is odd} \\ a & i \text{ is even} \end{cases}$$

Proof. This comes directly from the formulas for f and g. □

Lemma A.21. *(RCA_0) If $i < j$ and i, j are both even, then*

$$\alpha'(a)(i,j) \; = \; (1-a) \sum_{\substack{n=i+1 \\ n \text{ odd}}}^{j-1} \Bigg(-x_{in} x_{nj} \; + \sum_{i < k_1 < n} (x_{ik_1} x_{k_1 n} x_{nj}) \; - \; - \sum_{i < k_1 < k_2 < n} (x_{ik_1} x_{k_1 k_2} x_{k_2 n} x_{nj}) \; + \cdots + (-1)^{n-i} x_{i(i+1)} \cdots x_{(n-1)n} x_{nj} \Bigg)$$

Proof. The proof consists of grinding through the calculations one step at a time, and breaking the sum up into pieces.

$$\begin{aligned}\alpha'(a)(i,j) &= \sum_{n=i}^{j} g(i,n)f(n,j) \\ &= \underbrace{g(i,i)f(i,j)}_{(I)} + \underbrace{g(i,j)f(j,j)}_{(II)} + \underbrace{\sum_{n=i+1}^{j-1} g(i,n)f(n,j)}_{(III)}\end{aligned}$$

Since i is even, (I) is ax_{ij}. Since j is even, $f(j,j) = a$, and so (II) equals

$$a\left(-x_{ij} + \sum_{i<k_1<j}(x_{ik_1}x_{k_1j}) - \cdots + (-1)^{j-i}(x_{i(i+1)}\cdots x_{(j-1)j})\right)$$

(III) breaks into two cases: when n is even and when n is odd.

$$\underbrace{\sum_{\substack{n=i+1\\ \text{n odd}}}^{j-1}\big(g(i,n)\cdot x_{nj}\big)}_{(IV)} + \underbrace{\sum_{\substack{n=i+1\\ \text{n even}}}^{j-1}\big(g(i,n)\cdot ax_{nj}\big)}_{(V)} =$$

$$\sum_{\substack{n=i+1\\ \text{n odd}}}^{j-1}\left(-x_{in}x_{nj} + \sum_{i<k_1<n}(x_{ik_1}x_{k_1n}x_{nj}) - \cdots + (-1)^{n-i}(x_{i(i+1)}\cdots x_{nj})\right) +$$
$$a\cdot\sum_{\substack{n=i+1\\ \text{n even}}}^{j-1}\left(-x_{in}x_{nj} + \sum_{i<k_1<n}(x_{ik_1}x_{k_1n}x_{nj}) - \cdots + (-1)^{n-i}(x_{i(i+1)}\cdots x_{nj})\right)$$

There are a couple of important observations. First, (I) cancels with the first term in (II). Second, all of the terms in (V) appear in and cancel with terms in (II). Third, since j is even, it follows that $j-1$ is odd and so the last term in (II) does not cancel. Performing the cancelations, we are left with

$$\begin{aligned}&a\cdot\left(\sum_{\substack{i<k_1<j\\ k_1 \text{ odd}}}(x_{ik_1}x_{k_1j}) - \sum_{\substack{i<k_1<k_2<j\\ k_2 \text{ odd}}}(x_{ik_1}x_{k_1k_2}x_{k_2j}) + \right.\\ &\qquad\qquad \left. + \cdots + (-1)^{j-i}(x_{i(i+1)}\cdots x_{(j-1)j})\right) + \\ &\qquad + \sum_{\substack{n=i+1\\ \text{n odd}}}^{j-1}\left(-x_{in}x_{nj} + \sum_{i<k_1<n}(x_{ik_1}x_{k_1n}x_{nj}) - \cdots + (-1)^{n-i}(x_{i(i+1)}\cdots x_{nj})\right).\end{aligned}$$

This equation yields the formula in the statement of the lemma once the following general rewriting principles are applied.

$$\sum_{\substack{i<k_1<j \\ k_1 \text{ odd}}} x_{ik_1}x_{k_1j} \quad \Rightarrow \quad - \sum_{\substack{n=i+1 \\ \text{n odd}}}^{j-1} -x_{in}x_{nj}$$

$$- \sum_{\substack{i<k_1<k_2<j \\ k_2 \text{ odd}}} x_{ik_1}x_{k_1k_2}x_{k_2j} \quad \Rightarrow \quad - \sum_{\substack{n=i+1 \\ \text{n odd}}}^{j-1} \left(\sum_{i<k_1<n} x_{ik_1}x_{k_1n}x_{nj} \right)$$

These principles continue for longer linear sequences of subscripted k's. For example, a similar rewriting rule can be applied to the sum over $i < k_1 < k_2 < k_3 < j$ with k_3 odd. □

Lemma A.22. *(RCA_0) If $i < j$, i is even, and j is odd then*

$$\alpha'(a)(i,j) = (1-a)(-x_{ij}) + (1-a) \sum_{\substack{n=i+1 \\ n \text{ even}}}^{j-1} \Bigg(x_{in}x_{nj} - \sum_{i<k_1<n} (x_{ik_1}x_{k_1n}x_{nj}) + $$
$$+ \sum_{i<k_1<k_2<n} x_{ik_1}x_{k_1k_2}x_{k_nn}x_{nj} \;- \cdots + (-1)^{n-i} x_{ii+1} \cdots x_{n-1n}x_{nj} \Bigg).$$

Proof. This proof proceeds as the last one. I will outline it and point out what needs to be changed from the last proof. As before we have

$$\alpha'(a)(i,j) \;=\; \sum_{n=i}^{j} g(i,n)f(n,j)$$
$$= \underbrace{g(i,i)f(i,j)}_{(I)} + \underbrace{g(i,j)f(j,j)}_{(II)} + \underbrace{\sum_{n=i+1}^{j-1} g(i,n)f(n,j)}_{(III)}.$$

Since i is still even, (I) remains ax_{ij}. However, since j is odd, $f(j,j) = 1$ and so (II) is

$$-x_{ij} \;+ \sum_{i<k_1<j} (x_{ik_1}x_{k_1j}) \;- \cdots + (-1)^{j-i}(x_{i(i+1)} \cdots x_{(j-1)j}).$$

(III) still breaks into two pieces.

$$\underbrace{\sum_{\substack{n=i+1 \\ \text{n odd}}}^{j-1} (g(i,n) \cdot x_{nj})}_{(IV)} \;+\; \underbrace{\sum_{\substack{n=i+1 \\ \text{n even}}}^{j-1} (g(i,n) \cdot ax_{nj})}_{(V)}$$

This time, (I) does not cancel with the first term of (II), and instead of the terms of (V) appearing in (II), the terms in (IV) appear there. Since j is odd, it follows that $j-1$ is even, and so the last term in (II) does not cancel. The lemma follows after cancelling and rewriting as above. □

Using similar methods, we can prove the next two lemmas as well.

Lemma A.23. *(RCA_0) If $i < j$ and both i, j are odd then*

$$\alpha'(a)(i,j) = (1-a)\sum_{\substack{n=i+1\\ n\ even}}^{j-1}\Bigg(x_{in}x_{nj} - \sum_{i<k_1<n}(x_{ik_1}x_{k_1n}x_{nj}) + \\ + \sum_{i<k_1<k_2<n}(x_{ik_1}x_{k_1k_2}x_{k_2n}x_{nj}) + \cdots + (-1)^{n-i}x_{i(i+1)}\cdots x_{(n-1)n}x_{nj}\Bigg).$$

Lemma A.24. *(RCA_0) If $i < j$, i is odd, and j is even then*

$$\alpha'(a)(i,j) = (1-a)(x_{ij}) + (1-a)\sum_{\substack{n=i+1\\ n\ odd}}^{j-1}\Bigg(-x_{in}x_{nj} + \sum_{i<k_1<n}(x_{ik_1}x_{k_1n}x_{nj}) - \\ - \sum_{i<k_1<k_2<n}x_{ik_1}x_{k_1k_2}x_{k_nn}x_{nj} + \cdots + (-1)^{n-i}x_{i(i+1)}\cdots x_{(n-1)n}x_{nj}\Bigg).$$

Bibliography

Baumslag, G., F. Cannonito, D. Robinson and D. Segal (1991): "The Algorithmic Theory of Polycyclic-by-finite Groups," *J. Algebra*, 141: pp. 118–149.

Buttsworth, R. (1971): "A Family of Groups With a Countable Infinity of Full Orders," *Bull. Austral. Math. Soc.*, 4: pp. 97–104.

Dobritsa, V. (1983): "Some Constructivizations of Abelian Groups," *Siberian Math. J.*, 24, no. 2: pp. 167–173.

Downey, R. (1995): "On Presentations of Algebraic Systems," Unpublished lecture notes from COLORET II conference.

Downey, R. and S. A. Kurtz (1986): "Recursion Theory and Ordered Groups," *Ann. Pure Appl. Logic*, 32: pp. 137–151.

Drake, F. R. (1989): "On the Foundations of Mathematics in 1987," in *Logic Colloquium 87*, vol. 129 of *Studies in Logic*, pp. 11–25, North–Holland.

Feferman, S. (1988): "Hilbert's Program Relativized: Proof Theoretical and Foundational Reductions," *J. Symbolic Logic*, 53, no. 2: pp. 364–384.

Friedman, H. M., S. G. Simpson and R. L. Smith (1983): "Countable Algebra and Set Existence Axioms," *Ann. Pure Appl. Logic*, 25: pp. 141–181.

Fuchs, L. (1958): "Note On Ordered Groups and Rings," *Fund. Math.*, 46: pp. 167–174.

Fuchs, L. (1963): *Partially Ordered Algebraic Systems*, Pergamon Press.

Hatzikiriakou, K. (1989): "Algebraic Disguises of Σ^0_1 Induction," *Arch. Math. Logic*, 29, no. 4: pp. 47–51.

Hatzikiriakou, K. and S. G. Simpson (1990): "WKL_0 and Orderings of Countable Abelian Groups," *Contemporary Mathematics*, 106: pp. 177–180.

Hirst, J. L. (1994): "Reverse Mathematics and Ordinal Exponentiation," *Ann. Pure Appl. Logic*, 66: pp. 1–18.

Hungerford, T. W. (1974): *Algebra*, vol. 73 of *Graduate Texts in Mathematics*, Springer–Verlag.

Jockusch Jr., C. G. and R. I. Soare (1972): "Π^0_1 Classes and Degrees of Theories," *Trans. Amer. Math. Soc*, 173: pp. 33–56.

Jockusch Jr., C. G. and R. I. Soare (1991): "Degrees of Orderings Not Isomorphic to Recursive Linear Orderings," *Ann. Pure Appl. Logic*, 52: pp. 39–64.

Kargapolov, M., A. Kokorin and V. Kopytov (1965): "On the Theory of Orderable Groups," *Algebra i Logika*, 4, no. 6: pp. 21–27, (Russian).

Kokorin, A. and V. Kopytov (1974): *Fully Ordered Groups*, Halsted Press.

Kunen, K. (1980): *Set Theory An Introduction to Independence Proofs*, North–Holland.

Lorenzen, P. (1949): "Über Halbgeordnete Gruppen," *Arch. Math.*, 2: pp. 66–70, (German).

Łos, J. (1954): "On the Existence of Linear Order In a Group," *Bull. Acad. Polon. Sci. Cl. III*, 2: pp. 21–23.

Magnus, W., A. Karrass and D. Solitar (1965): *Combinatorial Group Theory: Presentations of Groups in Terms of Generators and Relations*, vol. 8 of *Pure and Applied Mathematics*, Interscience Publishers.

Mal'tsev, A. (1949): "On Ordered Groups," *Izv. Akad. Nauk. USSR Sem. Mat.*, 13: pp. 473–482, (Russian).

Metakides, G. and A. Nerode (1979): "Effective Content of Field Thoery," *Ann. Math. Logic*, 17: pp. 289–320.

Mura, R. B. and A. Rhemtulla (1977): *Orderable Groups*, vol. 27 of *Lecture Notes in Pure and Applied Mathematics*, Marcel Dekker, Inc.

Ohnishi, M. (1952): "Linear Order On a Group," *Osaka Math. J.*, 4: pp. 17–18.

Parsons, C. (1970): "On a Number Theoretic Choice Scheme and Its Relation to Induction," in A. Kino et al., eds., *Intuitionism and Proof Theory*, pp. 459–474, North–Holland.

Rabin, M. (1960): "Computable Algebra, General Theory and Theory of Computable Fields," *Trans. Amer. Math. Soc.*, 95: pp. 341–360.

Revesz, G. (1986): "Full Orders on Free Groups," in S. Wolfenstein, ed., *Algebra and Order: Proc. First Int. Symp. Ordered Algebraic Structures Luminy–Marseille 1984*, pp. 105–111.

Revesz, G. (1987): "A Simple Proof of Vinogradov's Theorem on the Orderability of the Free Product of O-Groups," *Czech. Math. J.*, 37(112): pp. 310–312.

Robinson, D. (1982): *A Course in the Theory of Groups*, Springer–Verlag.

Simpson, S. G. (1984): "Which Set Existence Axioms Are Needed to Prove the Cauchy/Peano Theorem For Ordinary Differential Equations?" *J. Symbolic Logic*, 49: pp. 783–802.

Simpson, S. G. (1985): "Reverse Mathematics," *Proceedings of Symposia in Pure Mathematics*, 42: pp. 461–471.

Simpson, S. G. (1988): "Partial Realizations of Hilbert's Program," *J. Symbolic Logic*, 53, no. 2: pp. 349–363.

Simpson, S. G. (Unpublished): "Subsystems of Second Order Arithmetic," (to appear).

Smith, R. L. (1981): "Two Theorems On Autostability In p–Groups," in A. Dold and B. Eckmann, eds., *Logic Year 1979–80*, vol. 859 of *Lecture Notes In Mathematics*, pp. 302–311, Springer–Verlag.

Soare, R. (1980): *Recursively Enumerable Sets and Degrees*, Springer–Verlag.

Soare, R. I. (1987): *Recursively Enumerable Sets and Degrees*, Perspectives in Mathematical Logic, Springer–Verlag.

Teh, H. (1960): "Construction of Orders In Abelain Groups," *Cambridge Philosophical Society Proceedings*, 57: pp. 476–482.