# Reverse Mathematics on Lattice Ordered Groups

Alexander S. Rogalski, Ph.D.

University of Connecticut, 2007

Several theorems about lattice-ordered groups are analyzed. $\mathsf{RCA}_0$ is sufficient to prove the induced order on a quotient of $\ell$-groups and the Riesz Decomposition Theorem. $\mathsf{WKL}_0$ is equivalent to the statement "An abelian group $G$ is torsion free if and only if it is lattice-orderable." $\mathsf{ACA}_0$ is equivalent to the existence of various substructures: the join of two convex $\ell$-subgroups, the convex closure of an $\ell$-subgroup, the polar subgroup $X^\perp$ of an $\ell$-subgroup $X$, and a sequence of values $\{V(g) : g \neq e\}$. The standard proof of Holland's Embedding Theorem uses $\mathsf{ACA}_0$. Holland's Theorem is equivalent to the existence of a sequence of excluding prime subgroups $\{P(g) : g \neq e\}$, and the existence of such a sequence is provable in $\mathsf{WKL}_0$ when $G$ is abelian.

# Reverse Mathematics on Lattice Ordered Groups

Alexander S. Rogalski

B.S., Marlboro College, Marlboro, VT, 2002

M.S., University of Connecticut, Storrs, CT, 2004

A Dissertation

Submitted in Partial Fullfilment of the

Requirements for the Degree of

Doctor of Philosophy

at the

University of Connecticut

2007

# APPROVAL PAGE

Doctor of Philosophy Dissertation

# Reverse Mathematics on Lattice Ordered Groups

Presented by

Alexander S. Rogalski, B.S., M.S.

Major Advisor

David Reed Solomon

Associate Advisor

Manuel Lerman

Associate Advisor

Joseph Miller

University of Connecticut

2007

# ACKNOWLEDGEMENTS

First, I wish to acknowledge Old Joe, my banjo. I brought Old Joe to the annual Math Department picnic, where Reed excitedly introduced himself and suggested that we play music sometime. We managed to accomplish this a few times, despite the pressing obligations of academia and graduate studies. Reed truly deserves my thanks for being a superb advisor. Tricia, you are wonderful, and I thank you for believing in me when I feared it would take another year to finish. I also thank our daughter, Georgia, for being born and giving me, among other numerous joys, a *considerable* motivation to graduate. Last but not least, I wish to thank my family for their considerable and constant support.

# TABLE OF CONTENTS

# LIST OF FIGURES

# Chapter 1

# Introduction

## 1.1 Background

It is a relatively common occurrence for a student of mathematics to read or write a proof which, at a key step, uses Zorn's Lemma or an equivalent principle to prove the existence of a set with certain desired properties. Until one is used to doing so, it can seem odd to call on a result from set theory in the middle of a proof which otherwise only requires results in Algebra. One might wonder, "Does one really *need* something as strong as Zorn's Lemma to build this set, or could it be done directly?"

Reverse Mathematics is a subfield of logic which tries to answer questions like this by finding exactly which set-theoretic axioms are truly necessary to prove a theorem. The usual axioms of set theory, ZFC or ZF, are quite strong. We can make finer distinctions by restricting ourselves to "countable" mathematics and axiom systems which, though weaker, are still able to prove many classical theorems of mathematics. More formally, the setting for Reverse Math is the language of second order arithmetic $Z_2$. In this language, we have symbols $+, \cdot$, $<, 0$, and 1, and the usual axioms defining them in the natural numbers $\mathbb{N}$, set membership $\in$, and two types of variables: number variables which are intended to range over $\mathbb{N}$ and set variables which are intended to range over subsets $X \subset \mathbb{N}$.

A typical investigation in Reverse Math goes like this:

1. Pick a theorem $Thm$ to study.

2. Look at a textbook proof of $Thm$ and find a set $S$ of axioms for $Z_2$ that are suitable for the proof of $Thm$.

3. See if it is possible to prove the axioms of $S$ using $Thm$. (This is why it's called Reverse Math.)

We need some amount of set theory to do such a proof as in step 3, and we typically work in a weak base system called $\mathsf{RCA}_0$, which strikes a balance between being strong enough to allow basic proofs and weak enough to keep the set-theoretic impact reasonably minimal. Generally, one of two things happens. If we are able to prove $S$ from $Thm$, this tells us that $S$ is the weakest axiom system capable of proving $Thm$. (If a strictly weaker system $S'$ proved $Thm$, $S'$ would then imply $S$, an impossibility!) In this case we have a proof of $Thm$ from $S$ and a *reversal* of $Thm$ to $S$, and we say the two are equivalent over $\mathsf{RCA}_0$. If, on the other hand, attempts to prove $S$ from $Thm$ aren't working out, we look for a new proof of $Thm$ that uses weaker axioms $\hat{S}$ and repeat the process, trying to prove $\hat{S}$ using $Thm$.

The "full-blown" set existence axiom scheme for $Z_2$ consists of axioms $\exists X \forall n (n \in X \leftrightarrow \varphi(n))$, where $\varphi$ is any formula in the language $Z_2$ not mentioning $X$. This scheme basically says: if we have a formula in $Z_2$, the set of numbers which satisfy it exists. This full collection is too strong to be interesting for Reverse Math, but it contains five particular subsystems (subcollections of axioms) and most theorems successfully analyzed are equivalent to one of them. In order of increasing strength, they are: $\mathsf{RCA}_0$, $\mathsf{WKL}_0$, $\mathsf{ACA}_0$, $\mathsf{ATR}_0$, and $\Pi^1_1$-$\mathsf{CA}_0$. In this dissertation, only the first three come into play.

$\mathsf{RCA}_0$ is the usual base system over which we prove equivalences, and its set comprehension scheme is limited to $\Delta^0_1$ formulas. (We also include axioms allowing $\Sigma^0_1$ induction.) The next strongest, $\mathsf{WKL}_0$, consists of all the axioms of $\mathsf{RCA}_0$ plus the Weak König's Lemma axiom saying "If $T$ is an infinite binary tree, then $T$ has an infinite path". $\mathsf{WKL}_0$ is sometimes sufficient where a standard proof uses Zorn's Lemma, though there are notable cases where it does not suffice. For example, in the theory of commutative rings, the existence of a nontrivial prime ideal is equivalent to $\mathsf{WKL}_0$. The existence of a prime ideal is usually proved as a corollary to the existence of a maximal ideal. Since the existence of a maximal ideal requires $\mathsf{ACA}_0$, this is a case where a set-theoretically "simpler" existence proof for a prime ideal needed to be found. $\mathsf{ACA}_0$, or Arithmetical Comprehension, is the strongest subsystem used in this study, obtained by allowing set comprehension using arithmetical formulas – those which may have any number of number quantifiers in its definition but no set quantifiers.

The subsystem of axioms to which a given theorem is equivalent is a measure of the set-theoretic complexity of the theorem. A theorem which requires only weak set existence axioms is considered less complex than one which requires a lot of complicated assumptions, i.e., a very strong axiom system. Knowing which axioms are necessary is particularly of interest to those working on related problems in Computable Algebra or Combinatorics.

For instance, an effective analogue of a theorem is likely true if the theorem is provable in $\mathsf{RCA}_0$. As an example, $\mathsf{RCA}_0$ suffices to prove that the quotient of a commutative ring by a maximal ideal is a field. Thus, given such a ring and a maximal ideal in a computable presentation, one can effectively form the quotient field. In contrast, maximal ideals generally require $\mathsf{ACA}_0$ and it is not the case that, given a computable commutative ring, one can always effectively find a maximal ideal. Knowing that maximal and prime ideals respectively require $\mathsf{ACA}_0$ and $\mathsf{WKL}_0$ also enables one to make distinctions between the computational "difficulty" of obtaining a maximal or prime ideal in a computable ring. That is, it is both set-theoretically easier and computationally easier to obtain a prime ideal than a maximal one.

This particular project in Reverse Math concerns theorems about lattice-ordered groups. These groups are not necessarily exotic. For example: an abelian group $G$ is lattice-orderable if and only if it is torsion-free. In Chapter 3, we see that this statement is equivalent to $\mathsf{WKL}_0$. Taking a step back, there are three main types of ordered groups, so called because they have both an algebraic group structure and a partial order structure which respects the group operations. The most general kind is a partially-ordered group, or p.o.-group. If the partial order is a lattice order, $G$ is a lattice-ordered group, or $\ell$-group. If the order is a total (linear) order, $G$ is a totally ordered group, or $o$-group. We have the following class containments:

$$o\text{-groups} \subsetneq \ell\text{-groups} \subsetneq p.o.\text{-groups}$$

In [6], Solomon investigated theorems about p.o.-groups and $o$-groups. With $\ell$-groups in intermediate position between the other two, an immediate interest was what connections there were between the theory of lattice-ordered groups and the theories of the other two types, and whether or not there was a stronger resemblance to either side. There seem to be relatively few places where the theories of the three types of ordered groups can be compared directly, but these few are enough to suggest that $\ell$-groups are no more like $o$-groups than $p.o.$-groups. For example, Theorem 3.7 is an instance of $\ell$-groups being like $o$-groups and unlike $p.o.$-groups, whereas in Corollary 4.10, the relationship is reversed.

The results presented follow an exploratory trend, beginning with an investigation of how best to formalize $\ell$-groups in $Z_2$, then moving on to the existence of the various types of subobjects which occur in the classical study of $\ell$-groups, and culminating with an analysis of the more substantial Holland's Embedding Theorem.

**Holland's Embedding Theorem 1.** *Any $\ell$-group is $\ell$-isomorphic to an $\ell$-subgroup of the $\ell$-group of order-preserving permutations of a totally ordered set.*

The standard proof of Holland's Theorem makes use of a sequence of values: convex subgroups which are maximal with respect to excluding a specific element. As shown in Chapter 5, the existence of such a sequence is equivalent to $\mathsf{ACA}_0$. However, in Chapter 6, we show that Holland's theorem is equivalent to an alternative assumption and, when $G$ is abelian, is provable in the weaker subsystem $\mathsf{WKL}_0$.

## 1.2 Notation

We will use the symbols $\wedge, \vee$ for lattice meet and join, and use the symbol "&" and the word "or" in formulas for conjunction and disjunction, respectively.

We fix an enumeration $\Phi_0, \Phi_1, \ldots$ of all partial computable functions.

## 1.3 Reverse Math

With the Reverse Math scope limited to $\mathsf{RCA}_0, \mathsf{WKL}_0$, and $\mathsf{ACA}_0$, we routinely use the following lemmas when proving equivalences over $\mathsf{RCA}_0$.

**Lemma 1.1.** *The following are pairwise equivalent over* $\mathsf{RCA}_0$ *[5].*

1. $\mathsf{WKL}_0$

2. ($\Sigma^0_1$ *separation) Let* $\phi_i(n), i = 0, 1$ *be* $\Sigma^0_1$ *formulas in which* $X$ *does not occur freely. If* $\neg\exists n(\phi_0(n)\ \&\ \phi_1(n))$ *then*

$$\exists X \forall n((\phi_0(n) \to n \in X)\ \&\ (\phi_1(n) \to n \notin X)).$$

3. *If* $f, g : \mathbb{N} \to \mathbb{N}$ *are one-to-one with* $\forall m \forall n(f(m) \neq g(n))$ *then*

$$\exists X \forall m(f(m) \in X\ \&\ g(m) \notin X).$$

**Lemma 1.2.** *The following are pairwise equivalent over* $\mathsf{RCA}_0$ *[5].*

1. $\mathsf{ACA}_0$

2. $\Sigma^0_1$ *comprehension, i.e.,* $\exists X \forall n(n \in X \leftrightarrow \phi(n))$ *restricted to* $\Sigma^0_1$ *formulas* $\phi(n)$ *in which* $X$ *does not occur freely.*

3. *For all one-to-one functions* $f : \mathbb{N} \to \mathbb{N}$ *there exists a set* $X \subseteq \mathbb{N}$ *such that* $\forall n(n \in X \leftrightarrow \exists m(f(m) = n))$*, i.e.,* $X$ *is the range of* $f$*.*

### 1.4 Lattices, Lattice-ordered groups

**Definition 1.3.** *A* ***lattice*** *is a partially ordered set such that every pair of elements has a least upper bound (join) and greatest lower bound (meet). The meet and join of elements* $a, b$ *are denoted* $a \wedge b$ *and* $a \vee b$*, respectively.*

**Definition 1.4.** *A **partially-ordered group** or p.o.**-group** is a group $G$ that is also a partial order and satisfies a condition that the group operation preserves the order on $G$, that is*

$$a \leq b \rightarrow \forall g(ag \leq bg \ \&\ ga \leq gb).$$

*If the partial order on $G$ is a lattice order, then $G$ is a lattice-ordered group or $\ell$-group. If the order on $G$ is a total (linear) order, then $G$ is a totally-ordered group or o-group.*

### 1.5 Fundamental Examples

**Example 1.5.** *Continuous functions on a topological space*

From [1]: let $X$ be a topological space and $C(X)$ the additive group of real-valued continuous functions. We make $C(X)$ an $\ell$-group by providing it with its usual pointwise order: $f \leq g$ if and only if $f(x) \leq g(x)$, for all $x \in X$.

**Example 1.6.** *(Restricted) Hahn groups*

From [1]: let $\Gamma$ be a *root system.* That is, $\Gamma$ is a partially ordered set for which $\{\alpha : \alpha \geq \gamma\}$ is totally ordered, for any $\gamma \in \Gamma$. Let $\{H_\gamma : \gamma \in \Gamma\}$ be a collection of $o$-groups indexed by $\Gamma$. Consider functions $v$ on $\Gamma$ for which $v(\gamma) \in H_\gamma$, for all $\gamma \in \Gamma$. Given such a function $v$, the subset of $\Gamma$ where $v$ is not zero is called its *support*. Let $\Sigma(\Gamma, H_\gamma)$ be the set of all such functions whose support is finite. This is a group under addition. Furthermore, if we define an element to be positive if it is positive at each maximal element of its support, then $\Sigma(\Gamma, H_\gamma)$ is an $\ell$-group, called a *restricted Hahn group* on $\Gamma$. (The general Hahn group on a root system does not require finite support. Rather, the support of each element must have the ascending chain condition.)

**Example 1.7.** *The group of finite sequences of integers*

Let $G$ be the group $\bigoplus_\omega \mathbb{Z}$. That is, $G$ is the group of finite sequences of integers, with the group operation of componentwise addition. (If two strings differ in length, we append zeros to the shorter one until the lengths match.) We say an element of $G$ is positive if each component is greater than or equal to zero. Thus, the meet and join of two elements $f, g$ is computed by taking the componentwise minimum (maximum, resp.) of the two. $G$ may be viewed as a restricted Hahn group on the root system $\Gamma$ consisting solely of a countably infinite antichain, with each $H_\gamma = \mathbb{Z}$ equipped with its usual order as an $o$-group. Of course, $G$ may also be viewed as the additive group of finite-support functions from $\mathbb{N}$ to $\mathbb{Z}$ equipped with the pointwise order.

**Example 1.8.** *Permutations of a Linear Order (and conventions)*

From [4]: let $L$ be a totally ordered set, and let $Aut(L)$ be the set of order-preserving bijections from $L$ to $L$. Then $Aut(L)$ is an $\ell$-group under composition, and lattice operations $\vee, \wedge$ are defined by the rules:

$$\begin{aligned} [f \vee g]\,(l) &= max\{f(l), g(l)\} \\ [f \wedge g]\,(l) &= min\{f(l), g(l)\} \end{aligned}$$

In terms of the induced $\leq$ relation, we have $f \leq g \iff f(l) \leq g(l)$ for all $l$.

**Example 1.9.** *Torsion-Free abelian group generated by* $\{x_i, y_i\}_{i\in\mathbb{N}}$.

The formal presentation for this group is from Solomon as in [6], which is summarized below for reference.

Let $G$ be the free abelian group on the generators $\{x_i, y_j\}_{i\in\mathbb{N}}$. Formally, elements of $G$ are quadruples $\langle I, q, J, p\rangle$ where $I$ and $J$ are finite subsets of $\mathbb{N}$ and $p$ and $q$ represent functions

$$q : I \to \mathbb{Z}\backslash 0 \qquad \text{and} \qquad p : J \to \mathbb{Z}\backslash 0$$

The element $\langle I, q, J, p\rangle$ is denoted $\sum_{i\in I} c_i x_i + \sum_{j\in J} d_j y_j$. The elements represented by $\langle I, q, J, p\rangle$ and $\langle I', q', J', p'\rangle$ are equal if and only if the four components are equal. The sum

$$\left(\sum_{i\in I} q_i x_i + \sum_{j\in J} p_j y_j\right) + \left(\sum_{k\in K} r_k x_k + \sum_{l\in L} s_l y_l\right)$$

is $\sum_{m \in M} t_m x_m + \sum_{n \in N} u_n y_n$ where $M = (I \cup K) \backslash \{z \in I \cap K \mid q_z + r_z = 0\}$ and

$$t_m = \begin{cases} q_m & \text{if } m \in I \backslash K \\ r_m & \text{if } m \in K \backslash I \\ q_m + r_m & \text{if } m \in I \cap K. \end{cases}$$

$N$ and $u_n$ are defined similarly. The identity $1_G$ is represented by $\langle \emptyset, \emptyset, \emptyset, \emptyset \rangle$, and if $g$ is represented by $\langle I, q, J, p \rangle$ then $g^{-1}$ is the sum $\sum_{i \in I} -q_i x_i + \sum_{j \in J} -p_j y_j$.

**Example 1.10.** *The group* $Fin^*_{\mathbb{Z}}$

$Fin^*_{\mathbb{Z}}$ is a formalization of Example 1.7 in $\mathsf{RCA}_0$. With $Fin_{\mathbb{Z}}$ as the formalization of the set of all finite integer sequences in $\mathsf{RCA}_0$, we let $Fin^*_{\mathbb{Z}} = \{\alpha \in Fin_{\mathbb{Z}} : \alpha(|\alpha| - 1) \neq 0\}$, i.e., the set of finite integer sequences which do not end in 0. The group operation $+_{Fin^*_{\mathbb{Z}}}$ consists of componentwise addition with the removal of any trailing zeros afterwards. If the strings are of different lengths, we pad the shorter one with zeros on the end until the lengths match, then add. The identity is the empty string, and the inverse of $\alpha \in Fin^*_{\mathbb{Z}}$, denoted $\alpha^{-1}$ or $-\alpha$, is obtained by changing the sign of every nonzero entry occurring in $\alpha$.

$Fin^*_{\mathbb{Z}}$ is an $\ell$-group under the pointwise order, and the meet and join can be calculated directly by (after appending zeros on the right until the lengths match) taking the minimum and maximum, respectively, in each component.

# Chapter 2

# Preliminary Results

An important step in working with a class of objects in $Z_2$ is to choose a workable definition, especially when the object's axioms involve quantifiers. We begin with the definitions of partially and linearly ordered groups, which have fairly straightforward axioms.

**Definition 2.1.** ($\mathsf{RCA}_0$) *A* **group** *is a set $G \subseteq \mathbb{N}$ along with a constant, $1_G$ (or $0_G$ or $e$), 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.** ($\mathsf{RCA}_0$) *A* **partial order** *is a set $X$ with a binary relation $\leq_X$*

*satisfying the following axioms.*

$$\forall x \in X(x \leq_X x)$$

$$\forall x, y \in X(x \leq_X y \ \& \ y \leq_X x \rightarrow x = y)$$

$$\forall x, y, z \in X(x \leq_X y \ \& \ y \leq_X z \rightarrow x \leq_X z)$$

**Definition 2.3.** ($\mathsf{RCA}_0$) *A* **partially ordered group** *is a pair* $(G, \leq_G)$ *where* $G$ *is a group,* $\leq_G$ *is a partial order on* $G$ *and, the group operation preserves the partial order on* $G$*. That is, for any* $a, b, c \in G$*, if* $a \leq_G b$ *then*

$$(a \cdot_G c \leq_G b \cdot_G c) \ \& \ (c \cdot_G a \leq_G c \cdot_G b).$$

*If the order on* $G$ *is a linear order, then* $G$ *is an* **ordered group** *or* **o-group***.*

## 2.1 Definition of $\ell$-group

Classically, a **lattice-ordered group** or **$\ell$-group** is defined as a partially ordered group $(G, \leq)$ where each pair of elements has unique greatest lower bound (meet) and least upper bound (join), i.e., the partial order is a lattice order.

Syntactically, the meet of $a$ and $b$ can be defined by a $\Pi^0_1$ formula:

$$x = (a \wedge b) \leftrightarrow \forall z([z \leq a \ \& \ z \leq b] \rightarrow z \leq x).$$

So can the join:

$$x = (a \vee b) \leftrightarrow \forall z([z \geq a \ \& \ z \geq b] \rightarrow z \geq x).$$

To say that the meet and join exist for every pair $a, b$ is then a $\Pi^0_3$ statement:

$$\forall a, b \exists x \forall z([z \leq a \;\&\; z \leq b] \rightarrow z \leq x)$$

$$\forall a, b \exists y \forall z[z \geq a \;\&\; z \geq b] \rightarrow z \geq y).$$

The obvious concern, then, when deciding on a definition for $\ell$-groups in $\mathsf{RCA}_0$, is whether or not these usual axioms for meet and join will be useful in actually calculating meet and join. Will knowing that every pair of elements has a meet, say, enable us to calculate it by a $\Delta^0_1$ function? Or is it necessary to explicitly require functions for meet and join as part of the definition in $\mathsf{RCA}_0$? Considering $(\mathbb{N}, REC)$, the standard model of $\mathsf{RCA}_0$, the following theorem shows that it is not possible in general to define meet and join by $\Delta^0_1$ functions.

**Theorem 2.4.** *There is a computable p.o.-group $(G, \leq)$ which is a lattice-ordered group, but for which the meet $\wedge$ and join $\vee$ operations are not computable. Furthermore, they are as complicated as the halting problem.*

*Proof.* Imitating a construction by Downey and Kurtz in [2], we construct our computable group $G = \cup_s G_s$ in stages. Each $G_s$ will be a finite set of integers with an associated representation function $\sigma_s$. For all elements $n \in G_s, \sigma_s(n)$ will be an element of $Fin^*_{\mathbb{Z}}$, a finite string of integers with no trailing zeros. We will define $n \circ_s m = k$ if $\sigma_s(n) +_{Fin_{\mathbb{Z}}} \sigma_s(m) = \sigma_s(k)$. The operation $\circ$ will be $\cup_{s\in\omega} \circ_s$, that is, once $n \circ_s m = k$ is defined, we will have $n \circ_t m = k$ for all $t \geq s$. Similarly, we define the partial order $\leq_s$, whose union will be the partial order on $G$. The partial order will satisfy the property $n \leq_G m \iff \sigma_s(n) \leq_s \sigma_s(m)$. That is, once $\sigma_s(n), \sigma_s(m)$ are defined, the partial order is defined and will be preserved throughout the construction.

The construction of $G$ will be done accomplishing the following:

- For some $m(s) \in \omega$ we will assign to all $p \leq m(s)$ a string $\sigma_s(p)$.

- If $t > s$, then $m(t) \geq m(s)$.

- If $p, q, r \leq m(s)$ and $\sigma_s(p) +_{Fin_{\mathbb{Z}}} \sigma_s(q) = \sigma_s(r)$, then for all $t > s$, we ensure that $\sigma_t(p) +_{Fin_{\mathbb{Z}}} \sigma_t(q) = \sigma_t(r)$.

- If $p, q \leq m(s)$ and $\sigma_s(p) \leq \sigma_s(q)$, then for all $t > s$, we ensure that $\sigma_t(p) \leq \sigma_t(q)$. We do the same for $\not\leq$.

- For all $p, \lim_{s \in \omega} \sigma_s(p)$ exists and is a finite string.

Additionally, $G$ will have a computable sequence of pairs $\langle a_e, b_e \rangle$, such that $a_e \wedge b_e \neq 0_G \iff \Phi_e(e) \downarrow$. We will meet the following requirements:

- **Group Closure**

  $C_e$: If $e = \langle p, q \rangle$, then $p \circ q$ is defined.

- **Group Inverses**

  $I_p$: There exists a $q$ such that $p \circ q = 0$ (0 denotes the zero of $\omega$ and the identity of $G$.)

- **Coding Requirements**

  $N_e$: $a_e \wedge b_e$ can compute whether $\Phi_e(e)$ halts.

  We order the requirements as follows: $N_0 \geq C_0 \geq I_0 \geq N_1 \geq \cdots$

**Definition 2.5.** *We say*

1. $C_e$ requires attention *at stage* $s+1$ *if* $e = \langle p, q\rangle$ *for some* $p, q \leq m(s)$ *and there is no* $r \leq m(s)$ *such that* $\sigma_s(p) +_{Fin_{\mathbb{Z}}} \sigma_s(q) = \sigma_s(r)$.

2. $I_p$ requires attention *at stage* $s+1$ *if* $p \leq m(s)$ *and there is no* $q \leq m(s)$ *such that* $\sigma_s(p) +_{Fin_{\mathbb{Z}}} \sigma_s(q) = 0$.

3. $N_e$ requires attention *at stage* $s+1$ *if* $N_e$ *is* unrealized *and either*

   (a) *for no* $t \leq s$ *are there a* $p, q$ *such that* $\sigma_s(p) = 0^{3e}1, \sigma_s(q) = 0^{3e}01$ *(in which case* $N_e$ *is* inactive*); or*

   (b) *there exists* $p, q$ *as above and* $\Phi_{e,s}(e)\downarrow$. *(we say* $N_e$ *is* active*)*

   *These* $p, q$ *are the pair* $\langle a_e, b_e\rangle$.

The requirements $N_e$ will achieve their goal as follows. When $N_e$ is active and unrealized, we have introduced elements $a_e, b_e$ whose meet corresponds to the identity $0 \in Fin^*_{\mathbb{Z}}$. Once $\Phi_e(e)$ halts, we change the mapping on $a_e$ and $b_e$ in a way that's compatible with all the p.o.-group requirements so that $a_e \wedge b_e$ becomes a new nonidentity element.

**Construction.**

*Stage* 0. Set $p(0) = 0$ and $\sigma_0(0) = 0 \in Fin^*_{\mathbb{Z}}$. The zero of $\mathbb{N}$ is to be the identity of $\langle G, \circ \rangle$.

*Stage* $s+1$. Let $R$ be the requirement of highest priority that requires attention.

*Case* 1: $R$ is $C_e$ with $e = \langle p, q \rangle$. Define $m(s+1) = m(s)+1$. Define $\sigma_{s+1}(r)$ for $r \leq m(s+1)$ via:

$$\sigma_{s+1}(r) = \begin{cases} \sigma_s(r) & \text{if } r < m(s+1), \\ \sigma_s(p) +_{Fin_{\mathbb{Z}}} \sigma_s(q) & \text{if } r = m(s+1). \end{cases}$$

*Case* 2: $R$ is $I_p$. Let $m(s+1) = m(s)+1$. Define $\sigma_s(r)$ for $r \leq m(s+1)$ via:

$$\sigma_{s+1}(r) = \begin{cases} \sigma_s(r) & \text{if } r < m(s+1), \\ -\sigma_s(p) & \text{if } r = m(s+1). \end{cases}$$

*Case* 3: $R$ is $N_e$ and $N_e$ is inactive. Let $m(s+1) = m(s)+2$ and define $\sigma_{s+1}$ for $r \leq m(s+1)$ via:

$$\sigma_{s+1}(r) = \begin{cases} \sigma_s(r) & \text{if } r < m(s), \\ 0^{3e}1 & \text{if } r = m(s+1), \\ 0^{3e}01 & \text{if } r = m(s+2). \end{cases}$$

At this point, $N_e$ becomes active.

*Case* 4: $R$ is $N_e$ and $N_e$ is active. Thus, there are $p, q \leq m(s)$ such that $\sigma_s(p) = 0^{3e}1, \sigma_s(q) = 0^{3e}01$ and $\Phi_{e,s}(e) \downarrow$. Let $m(s+1) = m(s)+1$, and define $\sigma_{s+1}$ for $r < m(s+1)$ via:

$$\sigma_{s+1}(r)(x) = \begin{cases} \sigma_s(r)(x) & \text{if } x \neq 3e+2 \\ \\ \sigma_s(r)(3e) + \sigma_s(r)(3e+1) & \text{if } x = 3e+2 \end{cases}$$

and define $\sigma_{s+1}$ for $r = m(s+1)$ by

$$\sigma_{s+1}(r) = 0^{3e}001.$$

$N_e$ is now realized.

This has the effect of re-mapping the generators $0^{3e}1 \to 0^{3e}101$ and $0^{3e}01 \to 0^{3e}011$, and defining an element mapped to the new meet, $0^{3e}001$. This of course means that the lengths of strings may change at some stage, but each string can only get at most two digits longer.

For example, suppose we have $\sigma_s(r) = 0^{3e}23$, where $\Phi_{e,s} \uparrow$. If there is a $t > s$ such that $\Phi_{e,t} \downarrow$, then for some stage $t' \geq t$ we will have $\sigma_{t'}(r) = 0^{3e}235$, as a linear combination of the redefined generators.

This will allow us to compute $0'$ from a meet function, since $a_e \wedge b_e \neq 0_G \iff \Phi_e(e) \downarrow$.

**Verification.**

The limit of $\sigma_s$ exists, because the map will change at most $\lceil \frac{k}{3} \rceil$ times for a string of length $k$. The partial order and group operations are preserved by the redefinition in Case 4, because it is a linear mapping. The injectivity of $\lim_s \sigma_s$ follows by construction and is preserved by the redefinition in Case 4.

Thus we have an injection of $G$ into the finite sequences of integers as a p.o. group. $G$ is a computable p.o-group by the construction. Nonuniformly, we see that $G$ is isomorphic to the subgroup of $Fin^*_{\mathbb{Z}}$ generated by the strings

$$\{0^{3e}1, 0^{3e}01 : e \notin HALT\} \cup \{0^{3e}1, 0^{3e}01, 0^{3e}001 : e \in HALT\}.$$

This is also an $\ell$-subgroup of $Fin^*_{\mathbb{Z}}$, so the order $\leq$ on $G$ ends up being a lattice order in the classical sense. Because of the way that $G$ is constructed, no steps need to be taken to ensure that meets and joins exist, although requirements to that effect could be easily added. □

## 2.2 Definition of an $\ell$-group for Reverse Math

Because of the connection between $\mathsf{RCA}_0$ and computable mathematics, the above result means that in order to work with meet and join in $\ell$-groups in $\mathsf{RCA}_0$, we need to explicitly include them in the formal definition. Thus, we consider an $\ell$-group to be given by a group $G$ together with a lattice order $\leq$ and functions $\wedge$ and $\vee$ giving the meet and join operations.

**Definition 2.6.** *An $\ell$-group is a tuple $(G, e, \cdot, \wedge, \vee)$ such that under the partial order defined by $x \leq y \Leftrightarrow x \vee y = y$, $(G, e, \cdot, \leq)$ satisfies the axioms of a p.o.-group* *and the following identities:*

| | | |
|---|---|---|
| *L.1.* | $x \vee x = x$ | $x \wedge x = x$ |
| *L.2.* | $x \vee y = y \vee x$ | $x \wedge y = y \wedge x$ |
| *L.3.* | $(x \vee y) \vee z = x \vee (y \vee z)$ | $(x \wedge y) \wedge z = x \wedge (y \wedge z)$ |
| *L.4.* | $(x \vee y) \wedge x = x$ | $(x \wedge y) \vee x = x$ |

We sometimes take the partial (lattice) order $\leq$ as included, though it is computed directly from $\vee$. It is easy to give direct proofs that the lattice axioms imply the poset axioms of reflexivity, antisymmetry, and transitivity via the equivalence $x \leq_L y \Leftrightarrow x \vee_L y = y$ using the lattice axioms L.1, L.2, and L.3, respectively. Verifying that the join is the least upper bound uses L.3. Verifying the meet requires using L.4. to redefine the above equivalence using $\wedge$, then uses L.3 as in the join. Thus, it is possible to prove in $\mathsf{RCA}_0$ that if $(G, \vee, \wedge)$ satisfies L.1 through L.4, then it is a lattice under the induced partial order.

## 2.3 Basic computation in $\ell$-groups

The following theorems have proofs that can be easily formalized in $\mathsf{RCA}_0$. (See pages 15–18 of [4].)

**Theorem 2.7.** ($\mathsf{RCA}_0$) *[Multiplication Across Meet and Join] Let* $(G, \cdot, e, \wedge, \vee)$ *be such that* $(G, \cdot, e)$ *is a group,* $(G, \wedge, \vee)$ *is a lattice, and in* $G$ *the identities*

$$u(x \vee y)v = uxv \vee uyv \quad , \quad u(x \wedge y)v = uxv \wedge uyv$$

*hold. Then $G$ is a lattice-ordered group under the partial order of the lattice $(G, \wedge, \vee)$. If $G$ is a lattice-ordered group, then the above identities hold.*

*Proof.* See proof of Theorem 2 on pages 14–15 of [4]. □

**Definition 2.8.** *An element $g$ of an $\ell$-group is said to be* positive *if $e \leq g$, or equivalently, $g \wedge e = e$. Negative elements are defined similarly.*

**Theorem 2.9.** ($\mathsf{RCA}_0$) *In any $\ell$-group $G$ the inequality $a \wedge bc \leq (a \wedge b)(a \wedge c)$ is satisfied for any positive elements $a, b, c$. Furthermore, if $a \wedge b = e$ then $a \wedge bc = a \wedge c$.*

*Proof.* From page 15 of [4]. If $a, b, c \geq e$ then $a \leq a^2, a \leq ac, a \leq ba$ and $(a \wedge b)(a \wedge c) = a^2 \wedge ba \wedge ac \wedge bc \geq a \wedge bc$. The second statement then follows from the first. □

**Corollary 2.10.** ($\mathsf{RCA}_0$) *For all $m, n \in \mathbb{N}, a \wedge b = e \rightarrow a^n \wedge b^m = e$*

*Proof.* We use the special cases where $c = a$ or $c = b$ to build up by induction. □

**Theorem 2.11.** ($\mathsf{RCA}_0$) *In any $\ell$-group, the following hold:*

$$(x \vee y)^{-1} = x^{-1} \wedge y^{-1} \quad , \quad (x \wedge y)^{-1} = x^{-1} \vee y^{-1}$$

$$x(x \wedge y)^{-1}y = x \vee y \quad , \quad x(x \vee y)^{-1}y = x \wedge y$$

*Proof.* See proof of Proposition 1 on page 16 of [4]. □

**Theorem 2.12.** ($\mathsf{RCA}_0$) *In an $\ell$-group $G$, the following holds: $\forall n \geq 1(x^n \geq e \rightarrow x \geq e)$.*

To prove this universal statement in $\mathsf{RCA}_0$ requires several lemmas formalizing the standard proof. We define, by primitive recursion, a function $f(x,n) = x^n$, which we will use transparently by writing exponents, and two functions $m$, and $m^+$ with the following inductive definitions.

$$m(x,1) = x \wedge e, \qquad m(x,n+1) = x^{n+1} \wedge m(x,n) \text{ for } n \geq 1$$

$$m^+(x,1) = x, \qquad m^+(x,n+1) = x^{n+1} \wedge m^+(x,n) \text{ for } n \geq 1$$

Intuitively, $m(x,n) = x^n \wedge x^{n-1} \wedge \cdots \wedge x \wedge e$, and $m^+(x,n) = x^n \wedge x^{n-1} \wedge \cdots \wedge x$.

**Lemma 2.13.** $(\mathsf{RCA}_0)$ $\forall x \forall n \geq 1 (m(x,n) = m^+(x,n) \wedge e)$

*Proof.* The proof is by induction on $n$. When $n = 1$, $m(x,1) = m^+(x,1) \wedge e$ by definition. Suppose the lemma holds for $n$.

$$\begin{aligned} m(x,n+1) &= x^{n+1} \wedge m(x,n) \\ &= x^{n+1} \wedge m^+(x,n) \wedge e \text{ (by induction hypothesis)} \\ &= m^+(x,n+1) \wedge e \text{ (by definition of } m^+) \end{aligned}$$

□

**Lemma 2.14.** $(\mathsf{RCA}_0)$ $\forall x \forall n \geq 1 (x \cdot m(x,n) = m^+(x,n+1))$

*Proof.* Again, proof by induction on $n$. When $n = 1$,

$$\begin{aligned} x \cdot m(x,1) &= x \cdot (x \wedge e) \\ &= x^2 \wedge x \\ &= x^2 \wedge m^+(x,1) \\ &= m^+(x,2). \end{aligned}$$

Supposing the lemma for $n$,

$$\begin{aligned} x \cdot m(x,n+1) &= x(x^{n+1} \wedge m(x,n)) \\ &= x^{n+2} \wedge x \cdot m(x,n) \\ &= x^{n+2} \wedge m^+(x,n+1) \text{ (by induction hypothesis)} \\ &= m^+(x,n+2). \end{aligned}$$

□

**Lemma 2.15.** ($\mathsf{RCA}_0$) $\forall x \forall n \geq 1((x \wedge e)^n = m(x,n))$

*Proof.* Again, a proof by induction on $n$. The case $n = 1$ is trivial.

Suppose we have the lemma for $n$.

$$
\begin{aligned}
(x \wedge e)^{n+1} &= (x \wedge e)(x \wedge e)^n \\
&= (x \wedge e) \cdot m(x,n) \text{ (by induction hypothesis)} \\
&= (x \cdot m(x,n)) \wedge (e \cdot m(x,n)) \\
&= (m^+(x,n+1) \wedge m(x,n) \text{ (by Lemma 2.14)} \\
&= x^{n+1} \wedge m^+(x,n) \wedge m(x,n) \\
&= x^{n+1} \wedge m^+(x,n) \wedge m^+(x,n) \wedge e \text{ (by Lemma 2.13)} \\
&= x^{n+1} \wedge m^+(x,n) \wedge e \\
&= x^{n+1} \wedge m(x,n) \text{ (by Lemma 2.13)} \\
&= m(x,n+1)
\end{aligned}
$$

□

Now we return to proof of the theorem: $\forall x \forall n \geq 1(x^n \geq e \rightarrow x \geq e)$

*Proof.* The proof is now direct, and the case $n = 1$ is trivial. Otherwise, suppose $x^{n+1} \geq e$.

$$
\begin{aligned}
(x \wedge e)^{n+1} &= m(x, n+1) \text{ (by Lemma 2.15)} \\
&= x^{n+1} \wedge m(x, n) \\
&= x^{n+1} \wedge m^{+}(x, n) \wedge e \\
&= (x^{n+1} \wedge e) \wedge m^{+}(x, n) \\
&= m^{+}(x, n) \wedge e \text{ (By hypothesis, } x^{n+1} \geq e \text{, so } x^{n+1} \wedge e = e.) \\
&= m(x, n) = (x \wedge e)^{n}
\end{aligned}
$$

Thus, if we suppose $(x \wedge e)^{n+1} \geq e$, then the above calculation shows that $(x \wedge e)^{n+1} = (x \wedge e)^{n}$. Multiplying both sides by $(x \wedge e)^{-n}$, we obtain $x \wedge e = e$, so $x \geq e$.

□

**Definition 2.16.** *For $x \in G$, we define $x^{+} = (x \vee e)$, $x^{-} = (x \wedge e)$, and $|x| = (x \vee x^{-1})$.*

**Theorem 2.17.** ($\mathsf{RCA}_0$) *In an $\ell$-group $G$, $x = x^{+}x^{-}$, $x^{+} \wedge (x^{-})^{-1} = e$, $x^{+}(x^{-})^{-1} = (x^{-})^{-1}x^{+}$.*

*Proof.* See proof of Proposition 5 on page 17 of [4]. □

**Theorem 2.18.** ($\mathsf{RCA}_0$) *In an $\ell$-group $G$, the following hold:*

$$(xy)^{+} \leq x^{+}y^{+} \quad , \quad (xy)^{+} = x(x \wedge y^{-1})^{-1}$$

$$\forall n((x^{n})^{+} = (x^{+})^{n}) \quad , \quad \forall n((x^{n})^{-} = (x^{-})^{n})$$

*Proof.* See proof of Proposition 6 on page 18 of [4]. □

**Theorem 2.19.** ($\mathsf{RCA}_0$) *In an $\ell$-group $G$, the following hold:*

$$|x| = x^+(x^-)^{-1}$$

$$\forall n(|x^n| = |x|^n)$$

*Proof.* See proof of Proposition 7 on page 18 of [4]. □

Note that since $x^+$ is positive and $x^-$ is negative, Theorem 2.19 implies that absolute values are positive.

**Theorem 2.20.** ($\mathsf{RCA}_0$) *In an $\ell$-group, $|xy| \leq |x||y||x|$, and $|x \vee y| \leq |x||y|$.*

*Proof.* From page 18 of [4]. Both are brief. First, $|x|^{-1}|y|^{-1}|x|^{-1} \leq |x|^{-1}|y|^{-1} \leq xy \leq |x||y| \leq |x||y||x|$. This shows that $xy$ and $(xy)^{-1}$ are both bounded above by $|x||y||x|$. Then $|xy| = (xy) \vee (xy)^{-1} \leq |x||y||x|$. Second, $|x \vee y| = (x \vee y) \vee (x \vee y)^{-1} = (x \vee y) \vee (x^{-1} \wedge y^{-1}) \leq x \vee y \vee x^{-1} \vee y^{-1} = |x| \vee |y| \leq |x||y|$. (To see this last inequality, just consider the fact that $|x| \leq |x||y|$ and $|y| \leq |x||y|$.) □

## 2.4 The Riesz Decomposition Theorem

**Riesz Decomposition Theorem 1.** *Suppose $h_1, \ldots, h_n$ are positive elements of the $\ell$-group $G$. If $e \leq g \leq h_1 h_2 \cdots h_n$, then $g = g_1 g_2 \cdots g_n$, where $e \leq g_i \leq h_i$.*

*Proof.* A proof of this Theorem (see page 3 of [1]) goes by induction on $n$. The base case $n = 1$ is trivial. For the induction step, suppose $e \leq g \leq h_1 h_2 \cdots h_n$.

Let $g_1 = g \wedge h_1$ and note that $e \leq g_1 \leq h_1$. Then

$$k = g_1^{-1}g = (g^{-1} \vee h_1^{-1})g = e \vee (h_1^{-1}g) \leq h_2 \cdots h_n,$$

Now, by induction $k = g_2 \cdots g_n$ with $e \leq g_i \leq h_i$. But $g = g_1 k$, and $e \leq g_1 \leq h_1$. □

**Theorem 2.21.** *The Riesz Decomposition Theorem is provable in* $\mathsf{RCA}_0$

*Proof.* We formalize the proof given above in $\mathsf{RCA}_0$. Suppose we are given an $\ell$-group $G$. Let $R = \{\langle n, g, x\rangle : x$ is the code for an $n$-tuple $\langle h_1, \ldots, h_n\rangle$ s.t. each $h_i \geq e$ and $g \leq h_1 \cdot h_2 \cdots h_n\}$. Let $Q = \{\langle n, g, x, y\rangle : \langle n, g, x\rangle \in R$ & $y$ codes an $n$-tuple $\langle g_1, \ldots, g_n\rangle$ s.t. $e \leq g_i \leq h_i$ for each $i$ and $g = g_1 g_2 \cdots g_n\}$.

By primitive recursion on $n$, we define a function $f : R \to \mathbb{N}$ such that for all $\langle n, g, x\rangle \in R$, $\langle n, g, x, f(n, g, x)\rangle \in Q$.

Case $n = 1$. If $\langle 1, g, x\rangle \in R$, then $x = \langle g\rangle$ and $e \leq g$ so $\langle 1, g, x, g\rangle \in Q$. So we define $f(\langle 1, g, x\rangle) = g$.

Case $n > 1$. We define $f(\langle n, g, x\rangle) = \langle (g \wedge h_1)\rangle \star f(n-1, (g \wedge h_1)^{-1}g, \langle h_2, \ldots, h_n\rangle)$, where $x = \langle h_1, \ldots, h_n\rangle$ and $\star$ denotes concatenation and subsequent coding of lists of elements.

By the induction hypothesis, $f(n-1, (g \wedge h_1)^{-1}g, \langle h_2, \ldots, h_n\rangle)$ returns a $\hat{y}$ such that $(g \wedge h_1)^{-1}g = g_2 g_3 \cdots g_n$ where $\hat{y} = \langle g_2, \ldots, g_n\rangle$. Then $g = (g \wedge h_1)g_2 \cdots g_n\rangle$, so the code $\langle (g \wedge h_1), g_2, \ldots, g_n\rangle$ returned by this process is correct.

Let $\Pi(x)$ be the product of the elements coded by $x$, and let $P(n)$ be the formula $\forall g \forall x(\langle n, g, x\rangle \in R \to g = \Pi(f(n, g, x)))$ By our definition of $f$, and by calculations similar to those in the first proof, we have $\forall n(P(n) \to P(n+1))$, so by $\Pi^0_1$ induction:

$$\forall n \forall g \forall x(\langle n, g, x\rangle \in R \to g = \Pi(f(n, g, x)))$$

□

The following criterion for an $\ell$-subgroup will be convenient for later verifications.

**Theorem 2.22.** ($\mathsf{RCA}_0$) *A subgroup $H$ of the $\ell$-group $G$ is an $\ell$-subgroup iff $\forall a \in H(a \vee e \in H)$.*

*Proof.* From [4]: The first implication is obvious. Conversely, let $H$ be a subgroup of $G$ and suppose $\forall a \in H(a \vee e \in H)$. Then $x^{-1}y \vee e \in H$ for any $x, y \in H$ and $x(x^{-1}y \vee e) = y \vee x \in H$. Now that we have joins, $x \wedge y = (x^{-1} \vee y^{-1})^{-1} \in H$. □

The following Lemma will be referred to in Chapter 5, and we put it here with the other results about basic computations.

**Lemma 2.23.** ($\mathsf{RCA}_0$) $|a| \wedge |b| \leq |a \wedge b|$

*Proof.* By writing out the absolute values and distributing, we obtain the equalities

$$\begin{aligned} |a| \wedge |b| &= (a \wedge b) \vee (a \wedge b^{-1}) \vee (a^{-1} \wedge b) \vee (a^{-1} \wedge b^{-1}) \\ |a \wedge b| &= (a \wedge b) \vee (a^{-1} \vee b^{-1}). \end{aligned}$$

Note that each is a join of $(a \wedge b)$ with another element. Furthermore,

$$\begin{aligned} (a \wedge b^{-1}) &\leq (a^{-1} \vee b^{-1}) \\ (a^{-1} \wedge b) &\leq (a^{-1} \vee b^{-1}) \\ (a^{-1} \wedge b^{-1}) &\leq (a^{-1} \vee b^{-1}) \end{aligned}$$

where the first is justified by noting that $(a^{-1} \vee b^{-1}) \geq b^{-1} \geq (a \wedge b^{-1})$, and the rest are similarly justified. The conclusion then follows by the principle $x \leq y \rightarrow a \vee x \leq a \vee y$.

□

# Chapter 3

# More Results

## 3.1 Identifying groups which are lattice-orderable

Since an $\ell$-group is first and foremost a group, it is worth asking the question "Can I tell if a given group $G$ can be made into an $\ell$-group?" This question is partially answered by the following theorem about $o$-groups from [1].

**Theorem 3.1.** *For an abelian group $G$, the following are equivalent:*

1. *$G$ is totally orderable*

2. *$G$ is lattice orderable*

3. *$G$ is torsion-free*

In the context of Reverse Math, the equivalences of the orderability statements with the torsion-free statement are somewhat unbalanced in that one direction can be done in $\mathsf{RCA}_0$ and the other cannot.

**Lemma 3.2.** ($\mathsf{RCA}_0$) *If $G$ is a (potentially non-abelian) group, then "lattice-orderable $\rightarrow$ torsion free"*

*Proof.* This follows from Theorem 2.12. Suppose we have some torsion element $x$ with $x^n = e$ Then, in particular $x^n \geq e$, so by Theorem 2.12, $x \geq e$. On the other hand, we must also have $x^{-n} = e$, and a similar argument shows that $x^{-1} \geq e$, and thus $x = e$. □

The equivalence of "t.f. abelian → totally orderable" and $\mathsf{WKL}_0$ was shown in a paper by Hatzikiriakou and Simpson [3]. Since totally ordered groups are automatically lattice ordered groups, we have $\mathsf{WKL}_0 \vdash$ "t.f. abelian → lattice orderable." Since we already know that the implication for totally-orderable groups is equivalent to $\mathsf{WKL}_0$, the remaining question is then: Does the *weaker* statement "t.f. abelian → lattice orderable" imply $\mathsf{WKL}_0$? As it turns out, this is the case.

**Theorem 3.3.** ($\mathsf{RCA}_0$) *The following are equivalent.*

1. *Every torsion-free abelian group is lattice-orderable.*

2. $\mathsf{WKL}_0$

*Proof.* By the comments above, we have 2 → 1. Now, we prove 1 → 2.

Let $u, v$ be one-to-one functions with disjoint ranges. We will form a separating set. Let $G$ be the free abelian group on generators $a_i, b_i$ modulo the relations $(2k+3) \cdot a_{u(k)} = b_{u(k)}$ and $(2k+3) \cdot b_{v(k)} = a_{v(k)}$. (We use $2k+3$ so that we do not have equality when $k = 0$.) Since torsion free and abelian implies lattice-orderable, there is some lattice order with $\wedge, \vee, \leq$ defined on $G$. We modify the formal definition from Example 1.9 to get a formal representation of $G$. The technique of introducing relations is adapted from [3]. Any $g \in G$ has a unique normal form

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

where the coefficients are reduced according to the relations above. In terms of the quadruple $\langle I, q, J, p \rangle$ which formally represents $g$, we require that

$$\forall i \in I \neg \exists k \leq (|q_i| - 2)(i = u(k))$$

$$\&$$

$$\forall j \in J \neg \exists k \leq (|p_j| - 2)(j = v(k))$$

Since these are bounded-quantifier formulas, set of these normal forms exists in $\mathsf{RCA}_0$. To see why these requirements give us a unique normal form, suppose that $u(k) = i$. Then we can start generating normal forms like

$$a_i, 2a_i, \ldots, ka_i, (k+1)a_i$$

$$-a_i, -2a_i, \ldots, -ka_i, -(k+1)a_i.$$

With positive coefficients, once we get to $(k+2)a_i$, we have the relation $(2k+3)a_i = b_i$ which gives us the equality $(k+2)a_i = b_i - (k+1)a_i$. The bounds on the coefficients appearing in the requirements above force us to use the latter representation for the normal form.

We formally work with $G'$, defined as the set of all elements of $G$ that are in normal form. Then, for the $G'$ group sum on normal forms $g' +_{G'} h'$, we take the $G$-sum $g' +_G h'$ and, if necessary, search for the normal form in $G'$ obtained by reducing $g' +_G h'$ according to the relations. Since $g'$ and $h'$ were in normal form before adding, this process may only change a given $q_i$ by 2k+3, where $u(i) = k$, and change the corresponding $p_i$ by one, and similarly for the relations involving the function $v$.

That is, after adding the normal-form elements $g' +_G h'$ to get $\sum_{i \in I} q_i a_i + \sum_{j \in J} p_j b_j$, the associated normal form has components $\langle I', q', J', p' \rangle$, where each component can be calculated as demonstrated below.

If, for example, $\exists k \leq (|q_i| - 2)(i = u(k))$, then we reduce to a normal form by cases.

Case 1: $q_i > 0$. Then we take $q_i a_i + \overbrace{(b_i - (2k+3)a_i)}^{0_G}$ to get $(q_i - 2k - 3)a_i + (p_i + 1)b_i$. Since the two summands were in normal form, we have $q_i \leq 2k + 2$. Thus $k + 3 \leq q_i \leq 2k + 2$, so $-k \leq q_i - 2k - 3 \leq -1$, and the result is in normal form. Coincidental cancellation may result in differences between $I, J$ and $I', J'$.

Case 2: $q_i < 0$ is handled similarly.

Because this process uses only bounded quantification, including quantifying over (codes for) finite sets, the function taking $\langle I, q, J, p \rangle$ to the normal form $\langle I', q', J', p' \rangle$ may be defined by a $\Delta^0_1$ formula, so $G'$ exists as a group in $\mathsf{RCA}_0$. Having done this, we refer to $G'$ as $G$.

**Claim.** *$G$ is torsion free.*

The claim follows from the fact that $u$ and $v$ have disjoint ranges. Essentially, a reduction of $m \cdot a_i$ to $b_i$ may only happen if $i \in ran(u)$ and a reduction of $m \cdot b_i$ to $a_i$ may only happen if $i \in ran(v)$.

Now, we return to the proof of a reversal. The theorem asserts that there is a lattice order on $G$, which implies there are meet and join functions $\vee, \wedge$. This, in turn, lets us work with the absolute value $|x| = x \vee x^{-1}$. Then the set $\{n : |a_n| \leq |b_n|\}$ separates the ranges of $u, v$. Suppose $u(k) = n$. Then we have $a_n^{2k+3} = b_n$ and $|a_n|^{2k+3} = |b_n|$. Since $|x| \geq e$ for all $x$, it follows that $|a_n| \leq |b_n|$. It is easy to show that for every $n, |a_n| \neq |b_n|$, so the complement of the separating set contains $\{n : |a_n| > |b_n|\}$, which is the range of $v$. Note that $|a_n|$ and $|b_n|$ are only related by $<$ or $>$ if $n$ is in the range of $u$ or $v$. By Lemma 1.1, the existence of a separating set implies $\mathsf{WKL}_0$.

□

## 3.2 Convex $\ell$-subgroups and Right Cosets

In the context of $\ell$-groups, a type of $\ell$-subgroup called a *convex* $\ell$-subgroup plays an important role, analogous to that of normal subgroups in the context of general group theory. Cosets of a normal subgroup inherit the group structure in a natural way and, similarly, cosets of a convex $\ell$-subgroup inherit the lattice structure in a natural way.

**Definition 3.4.** *An $\ell$-subgroup $C$ is* convex *if for every $c_1, c_2 \in C$ and every $x$, $c_1 \leq x \leq c_2 \to x \in C$.*

**Theorem 3.5.** ($\mathsf{RCA}_0$) *The subgroup $C$ is a convex $\ell$-subgroup iff $\forall c \in C(|x| \leq |c| \to x \in C)$.*

*Proof.* On page 23 of [4] there is a quick proof which can be done in $\mathsf{RCA}_0$. □

**Theorem 3.6.** *If $C$ is a convex $\ell$-subgroup of the $\ell$-group $G$, then the right cosets of $C$ in $G$ form a lattice under the partial order given by $Cg \leq Ch \leftrightarrow \exists c \in C(g \leq hc)$.*

This same condition gives us the induced order in the context of cosets of a convex subgroup of a *p.o.*-group or an *o*-group. As shown in [6], the existence of the induced order on $G/C$ is equivalent to $\mathsf{ACA}_0$ when $G$ is a *p.o.*-group, and provable in $\mathsf{RCA}_0$ when $G$ is an *o*-group. In this regard, it turns out that $\ell$-groups are closer to *o*-groups than *p.o.*-groups.

**Theorem 3.7.** ($\mathsf{RCA}_0$) *Let $G$ be an $\ell$-group. Let $H$ be a convex $\ell$-subgroup of $G$. The induced order on the set of right cosets $G/H$ exists.*

*Proof.* Let $a, b$ be elements of $G$. The induced order on $G/H$ as originally given is: $Ha \leq Hb \leftrightarrow (\exists h \in H)a \leq hb$. Note that by choosing $h = e$, it is apparent that $a \leq b \to Ha \leq Hb$. Also note the following identity, which holds for all elements $x, y$.

$$x = (e \vee xy^{-1})(x \wedge y)$$

To verify this identity, we distribute. First,

$$\begin{aligned}(e \vee xy^{-1})(x \wedge y) &= [(e \vee xy^{-1})x] \wedge [(e \vee xy^{-1})y] \\ &= (x \vee xy^{-1}x) \wedge (y \vee x) \\ &\geq x\end{aligned}$$

Then, distributing the other way,

$$\begin{aligned}(e \vee xy^{-1})(x \wedge y) &= [e(x \wedge y)] \vee [xy^{-1}(x \wedge y)] \\ &= (x \wedge y) \vee (xy^{-1}x \wedge x) \\ &\leq x\end{aligned}$$

**Claim.** $(e \vee ab^{-1}) \in H \rightarrow Ha \leq Hb$

*Proof.* Let $(e \vee ab^{-1}) \in H$. Then $a = (e \vee ab^{-1})(a \wedge b)$, by the identity above. Therefore, $Ha = H(a \wedge b) \leq Hb$. □

**Claim.** $Ha \leq Hb \rightarrow (e \vee ab^{-1}) \in H$

*Proof.* Fix $h \in H$ s.t. $a \leq hb$. Then we have

$$(a \wedge b) \leq a \leq hb$$

$$(a \wedge b)b^{-1} \leq ab^{-1} \leq h$$

$$(ab^{-1} \wedge e) \leq ab^{-1} \leq h$$

$$e \vee (ab^{-1} \wedge e) \leq (e \vee ab^{-1}) \leq e \vee h$$

$$e \leq (ab^{-1} \vee e) \leq e \vee h$$

Since $e, h \vee e$ belong to $H$ and $H$ is convex, we have $ab^{-1} \vee e \in H$. □

By these two claims, we can decide the induced order on cosets by the quantifier free condition $aH \leq bH \leftrightarrow (e \vee ab^{-1}) \in H$. □

If $C$ is normal then $G/C$ has the familiar quotient group structure described by $Ca \cdot Cb = C(ab)$. Even when $C$ is not normal, by convexity alone, we have the induced order on the right cosets, as defined above, and this gives us the properties $Ca \vee Cb = C(a \vee b)$ and $Ca \wedge Cb = C(a \wedge b)$ as discussed in the following theorem from [4].

**Theorem 3.8.** ($\mathsf{RCA}_0$) *Let $C$ be a convex subgroup of $G$. Then $C(x \wedge y) = Cx \wedge Cy$ and $C(x \vee y) = Cx \vee Cy$ under the induced order.*

*Proof.* We prove the case for joins, and the case for meets is similar.

By definition of the induced order, it follows that $Cx \leq C(x \vee y)$ and $Cy \leq C(x \vee y)$. Let $Cz \geq Cx$, $Cz \geq Cy$. for some $z \in G$. Then there exist $c_1, c_2 \in C$ such that $c_1 z \geq x, c_2 z \geq y$. Let $c = c_1 \vee c_2 \in C$. Then $cz \geq c_1 z \geq x$ and $cz \geq c_2 z \geq y$, so $cz \geq x \vee y$. Thus $Cz \geq C(x \vee y)$ and $C(x \vee y)$ is the least upper bound of $Cx, Cy$ in $G/C$. □

# Chapter 4

# Convexity Results and Reversals for Substructure Existences

## 4.1 Closure Operations

To each kind of subgroup we associate a closure operation.

**Definition 4.1.** *Let $A$ be a subset of the $\ell$-group $G$. Let*

- *$\langle A \rangle$ denote the subgroup of $G$ generated by $A$,*
- *$\langle A \rangle_\ell$ denote the $\ell$-subgroup of $G$ generated by $A$,*
- *and $CL(A)$ denote the convex $\ell$-subgroup of $G$ generated by $A$.*

To form $\langle A \rangle$, one must close under inverses and group composition. To form $\langle A \rangle_\ell$, it is sufficient to further close under join, since $x \wedge y = (x^{-1} \vee y^{-1})^{-1}$. From this, one may form $CL(A)$ by adding all elements bounded above and below by elements of $\langle A \rangle_\ell$.

To work with these closures in $\mathsf{RCA}_0$, we define a mechanism of generation by primitive recursion. First we define a $\Sigma^0_1(A)$ mechanism for generating $\langle A \rangle$. Let

$A$ be a subset of the $\ell$-group $G$, and suppose $G$ is enumerated as $\{g_0 = e, g_1, \ldots\}$. Let

- $\langle A \rangle_0 = \{0\}$
- $\langle A \rangle_{t+1} = \{g_k \in G : g_k \leq_{\mathbb{N}} t \ \& \ \exists g_i, g_j \in \langle A \rangle_t$ s.t.

$$\begin{aligned} &( \ g_k \in \langle A \rangle_t \\ \mathit{or} \quad & g_k \in A \\ \mathit{or} \quad & g_i^{-1} = g_k \\ \mathit{or} \quad & g_k = g_i g_j)\} \end{aligned}$$

Then we define $\langle A \rangle$ as the set $\{g \in G : \exists n(g \in \langle A \rangle_n)\}$, which is $\Sigma^0_1(A)$. Thus, given an $\ell$-group $G$ and a subset $A \subset G$, $\mathsf{ACA}_0$ is sufficient to prove the existence of $\langle A \rangle$.

By adding the disjunction "or $g_k = g_i \vee g_j$", one defines $\langle A \rangle_\ell$. By further adding the disjunction "or $g_i \leq g_k \leq g_j$", one defines $CL(A)$.

Note that the definition of the closure is $\Sigma^0_1$ in all three cases. While $\mathsf{ACA}_0$ is equivalent to the existences of $\langle A \rangle, \langle A \rangle_\ell$, and $CL(A)$, given $A$, many of the interesting properties of these sets can be verified in $\mathsf{RCA}_0$ if they exist. For the next lemma, we will use the following notation which generalizes to the other forms of closure.

- $g \in \langle A \rangle$ means $\exists n(g \in \langle A \rangle_n)$

- $\langle A\rangle \subseteq \langle B\rangle$ means $\forall g(\exists n(g \in \langle A\rangle_n) \to \exists n(g \in \langle B\rangle_n))$.

- $\langle A\rangle$ is a subgroup of $G$ means $\forall g, h(g, h \in \langle A\rangle \to (g^{-1} \in \langle A\rangle \;\&\; g \cdot h \in \langle A\rangle))$.

**Lemma 4.2.** ($\mathsf{RCA}_0$) *Using the abbreviations above, for all $A, B \subseteq G$,*

1. *$\langle A\rangle$ is a subgroup of $G$.*

2. *If $A$ is a subgroup of $G$ then $\langle A\rangle = A$.*

3. *If $A \subseteq B$ then $\langle A\rangle \subseteq \langle B\rangle$.*

4. *If $A \subseteq B$ and $B$ is a subgroup of $G$ then $\langle A\rangle \subseteq B$.*

*Moreover, the Lemma is also true if one replaces all instances of the word "subgroup" with "$\ell$-subgroup" or "convex $\ell$-subgroup" and uses the appropriate closure operation.*

*Proof.* Statement (1) is clear by the construction of $\langle A\rangle$. For (2), the containment $A \subseteq \langle A\rangle$ follows from the construction. The reverse containment is shown by the statement $\forall n(\langle A\rangle_n \subseteq A)$ which is proved by $\Sigma^0_0$ induction. There are three cases to consider for an element added at the $(n+1)^{th}$ step. If $g_k$ is added because it belongs to $A$, then it is obviously in $A$ already. If $g_k$ is added because it is the inverse of an element in $\langle A\rangle_n$, then that element, by the induction hypothesis, belonged to $A$, and thus so did $g_k$ since $A$ is a subgroup. The third case, that $g_k$ is a product of elements in $\langle A\rangle_n$, is similar.

Similarly, to prove (3) one uses the statement "$A \subseteq B \to \forall n(\langle A \rangle_n \subseteq \langle B \rangle_n)$" which is proved by $\Sigma_0^0$ induction. Finally, (4) follows from (2) and (3).

The generalizations to $\ell$-subgroup closure and convex closure are proved in the same way. □

We also state the following lemma using the abbreviations described above.

**Lemma 4.3.** ($\mathsf{RCA}_0$) *Let $S$ be a subset of the $\ell$-group $G$. Then we have the following:*

- $y \in S \to \langle S \rangle = \langle S \cup \{y^{-1}\} \rangle$
- $x, y \in S \to \langle S \rangle = \langle S \cup \{xy\} \rangle$
- $x, y \in S \to \langle S \rangle_\ell = \langle S \cup \{x \vee y\} \rangle_\ell$
- $x, y \in S \ \& \ x \leq_G z \leq_G y \to CL(S) = CL(S \cup \{z\})$

*Furthermore, the first three implications are also valid for the more specific closure operations.*

*Proof.* We prove only the first statement. The rest are similar. First, suppose $y \in S$. Then we have the containments $S \subseteq S \cup y^{-1} \subseteq \langle S \rangle$. To be explicit about the second containment, suppose $y^{-1}$ is not already in $S$. If $y = g_a$ and $y^{-1} = g_b$, with $a < b$, then the latter will be a member of $\langle S \rangle_b$ by construction. If the inequality is reversed, then the latter will be a member of $\langle S \rangle_{a+1}$. By arguments like those in Lemma 4.2, we want to show that $\langle S \rangle \subseteq \langle S \cup y^{-1} \rangle \subseteq \langle \langle S \rangle \rangle = \langle S \rangle$.

Formally, the containments can be stated as $\exists n(x \in \langle S \rangle) \rightarrow \exists n(x \in \langle S \cup y^{-1} \rangle_n)$ and $\exists n(x \in \langle S \cup y^{-1} \rangle_n) \rightarrow \exists m \exists n(x \in \langle \langle S \rangle_n \rangle_m)$, while the equality can be stated $\exists m \exists n(x \in \langle \langle S \rangle_n \rangle_m) \leftrightarrow \exists n(x \in \langle S \rangle_n)$.

$\square$

**Lemma 4.4.** ($\mathsf{RCA}_0$) *Let $g$ be an element of the $\ell$-group $G$. Then* $CL(\{g\}) = \{h \in G : \exists n > 0(|h| \leq |g|^n)\}$, *i.e.* $\forall h[\exists n(h \in CL(\{g\})_n \leftrightarrow \exists n > 0(|h| \leq |g|^n))]$.

*Proof.* Fix $h \in G$. The statement $\exists n > 0(|h| \leq |g|^n) \rightarrow \exists n(h \in CL(\{g\})_n)$ follows from the definition of $CL(\{g\})$.

For the other direction, instead of proving the implication $\exists n > 0(|h| \leq |g|^n) \rightarrow \exists n(h \in CL(\{g\})_n)$, which is neither $\Sigma^0_1$ nor $\Pi^0_1$, we use a bounded quantifier in the second part. Let $f(n) = 3^n$, so that $f(n+1) = 3 \cdot f(n)$. As in a classic "$\frac{\epsilon}{3}$" argument, this choice will make sense in the future. We show by $\Pi^0_1$ induction on $n$ that $\exists n(h \in CL(\{g\})_n) \rightarrow |h| \leq |g|^{f(n)})$. For $n = 0$, we have $CL(\{g\})_0 = \{0\}$, $|0| = 0 \leq |g|^1$, and $0 < 1 \leq f(0) = 1$. For the induction step, suppose $h \in CL(\{g\}_{n+1}$. Then we have several cases, corresponding to the ways an element can enter the convex closure.

- If $h = g$ then $|h| \leq |g|^1$ and $1 \leq f(n+1)$.
- If $h \in CL(\{g\})_n$, then $|h| \leq |g|^k$ for some $0 < k \leq f(n) < f(n+1)$.
- If $\exists g_i \in CL(\{g\})_n$ with $h = g_i^{-1}$, then $|h| = |g_i^{-1}| = |g_i| \leq |g|^k$ for some $0 < k \leq f(n) < f(n+1)$.

- If $\exists g_i, g_j \in CL(\{g\})_n$ such that either $h = g_i g_j, h = g_i \vee g_j$, or $g_i < h < g_j$, then we have 3 subcases.
  - If $h = g_i g_j$ then, by Theorem 2.20, $|h| \leq |g_i| \cdot |g_j| \cdot |g_i| \leq |g|^{f(n)} \cdot |g|^{f(n)} \cdot |g|^{f(n)} = |g|^{3f(n)} = |g|^{f(n+1)}$.
  - If $h = g_i \vee g_j$ then $|h| \leq |g_i| \cdot |g_j| \leq |g|^{2f(n)} < |g|^{f(n+1)}$.
  - Suppose $g_i < h < g_j$. Then $|h| = (h \vee h^{-1}) \leq (g_j \vee h^{-1}) \leq (g_j \vee g_i^{-1}) \leq (|g_i| \vee |g_j|)$. Since $g_i, g_j \in CL(\{g\})_n$, $|g_i| \vee |g_j| \leq |g|^{f(n)}$. Thus, $|h| \leq |g|^{f(n)} < |g|^{f(n+1)}$.

□

**Lemma 4.5.** ($\mathsf{RCA}_0$). *Let $g_1, \ldots g_n$ be positive elements of the $\ell$-group $G$. Then $CL(\{g_1, \ldots, g_n\}) = CL(\{\prod_{1 \leq j \leq n} g_j\})$.*

*Proof.* Both containments are proved using an $n$-fold application of Lemma 4.3. First, since each $g_j$ is positive, $e \leq g_i \leq \prod_j g_j$. This proves the "$\subseteq$" containment. For the other direction, observe that the product $\prod_{1 \leq j \leq n} g_j$ must be contained in $CL(\{g_1, \ldots, g_n\})$, since the latter is a subgroup containing each factor. □

**Theorem 4.6.** ($\mathsf{RCA}_0$) *If $A, B$ are convex $\ell$-subgroups and $\langle A, B \rangle$ exists, then $CL(A \cup B) = \langle A, B \rangle$.*

*Proof.* The method of proof on page 8 of [1] uses the Riesz Decomposition Theorem and Theorem 2.20, and can be adapted to work in $\mathsf{RCA}_0$. We sketch the proof. Let $C = \langle A, B\rangle := \langle A \cup B\rangle$. By Lemma 4.2, $C$ is a subgroup. We use the criterion in Theorem 3.5 to show $C$ is a convex $\ell$-subgroup. Let $c \in C, g \in G$, and $|g| \leq |c|$. Then there is a finite collection of elements $c_i, i \leq n$ which belong to either $A$ or $B$ such that

$$c = c_0 c_1 \cdots c_n.$$

Then $g^+ \vee (g^-)^{-1} = |g| \leq |c_0 c_1 \cdots c_n|$, and by repeated use of Theorem 2.20 one obtains the inequality

$$|c_0 c_1 \cdots c_n| \leq |c_0||c_1| \cdots |c_n||c_{n-1}| \cdots |c_1| \cdots |c_0|.$$

Then, by the Riesz Decomposition Theorem, $g^+$ and $(g^-)^{-1}$ (and hence $g^-$) can be expressed as products of elements which belong to $A$ or $B$ by convexity. Since $g = g^+ g^-$, $g \in C$. □

## 4.2 Existence of the subgroup generated by $A, B$.

**Theorem 4.7.** ($\mathsf{RCA}_0$) *The following are equivalent.*

1. *For any group $G$ and subgroups $A, B \subseteq G$, the subgroup $\langle A, B\rangle$ exists.*
2. $\mathsf{ACA}_0$

*Proof.* $\langle A, B\rangle$ can be formed in $\mathsf{ACA}_0$ since it has a $\Sigma^0_1$ definition. To show the reversal, let $f$ be a one-to-one function. Let $G$ be the torsion free abelian group generated by $\{x_i, y_i\}_{i\in\mathbb{N}}$. The formal presentation for this group as sums

$\sum_{i\in I} q_i a_i + \sum_{j\in J} p_j b_j$ was defined in Example 1.9 and we subsequently refer to that notation below.

Let $A$ be the set of elements of the form $\sum_{i\in I} q_i x_i + 0$, i.e., those for which $J = p = \emptyset$. Clearly, $A$ is a subgroup of $G$. Then let $B$ be the subgroup of $G$ generated by all elements of the form $x_i + y_{f(i)}$. The exact condition for a formal sum to belong in $B$ can be stated as the following conjunction:

$$\forall i \in I \exists j \in J(j = f(i) \;\&\; p_i = q_j)$$

$$\&$$

$$\forall j \in J \exists i \in I(j = f(i) \;\&\; p_i = q_j).$$

Since $I$ and $J$ are finite, the quantifiers are bounded, so both $A$ and $B$ may be formed in $\mathsf{RCA}_0$.

Clearly, if $\exists i(f(i) = n)$ then the elements $x_i$ and $x_i + y_n$ belong to $A$ and $B$, respectively. In particular, the group sum $-1x_i + (x_i + y_n) = y_n$ belongs to $\langle A, B\rangle$. On the other hand, assume that $y_n = a + b$ for some $a \in A, b \in B$. Then $y_n = \sum_{i'\in I'} p_{i'} x_{i'} + (\sum_{i\in I} p_i x_i + \sum_{i\in I} p_i y_{f(i)})$. The parts involving $x$ terms must cancel, leaving $I' = I$. Since only $y_n$ appears in the left hand side, we must have $I = \{m\}$ where $f(m) = n$ and $p_n = 1$.

Then $y_n \in \langle A, B\rangle \leftrightarrow \exists i(f(i) = n)$, and $ran(f) = \{n : y_n \in \langle A, B\rangle\}$. □

## 4.3 Existence of the convex closure of an $\ell$-subgroup $H$

**Theorem 4.8.** ($\mathsf{RCA}_0$)

*1. For any $\ell$-group $G$ and $\ell$-subgroup $H \subseteq G$, $CL(H)$ exists.*

*2.* $\mathsf{ACA}_0$.

*Proof.* Since $CL(H)$ has $\Sigma^0_1$ definition with $H$ as a parameter, it is clear that $2 \to 1$. For the other direction, let $G$ be $Fin^*_{\mathbb{Z}}$, the $\ell$-group of finite-support functions from $\mathbb{N}$ to $\mathbb{Z}$ in the pointwise order. Let $f$ be a one-to-one function. The set $A$ of all strings $\sigma$ such that all three of the following hold

1. $\forall x < |\sigma|(\sigma(x) = 0 \text{ or } 1 \text{ or } 2)$

2. $\forall x < |\sigma|(\sigma(x) = 1 \to \exists i \le x[x = 2i \;\&\; 2f(i) + 1 < |\sigma| \;\&\; \sigma(2f(i) + 1) = 2])$

3. $\forall x < |\sigma|(\sigma(x) = 2 \to \exists i[2i < |\sigma| \;\&\; x = 2f(i) + 1 \;\&\; \sigma(2i) = 1])$

is definable by a bounded-quantifier formula, so exists in $\mathsf{RCA}_0$.

In other words, if $a_i = 0^{2i-1}1$ and $b_n = 0^{2n}1$, then the generators in A are all strings of the form $a_i + 2b_{f(i)}$. The subgroup $H = \langle A \rangle$ may also be described as all elements of the form $\sum_{i \in I} c_i \cdot a_i + \sum_{i \in I} 2c_i \cdot b_{f(i)}$ for some finite set $I$, and the set $A$ represents elements for which $c_i = 1$. Thus $H$ exists in $\mathsf{RCA}_0$. Clearly, if $f(i) = n$ then $0 < b_n < 2b_n < a_i + 2b_{f(i)}$, so $b_n$ must belong to $CL(H)$. On the other hand, suppose $b_n \in CL(H)$. Then there is some finite set $I$ such that $0 \le b_n \le \sum_{i \in I} c_i \cdot a_i + \sum_{i \in I} 2c_i \cdot b_{f(i)}$. Since $Fin^*_{\mathbb{Z}}$ has the pointwise order and $b_n$ has the form $0^{2n}1$, the sum bounding $b_n$ must have a positive number in the $(2n+1)^{th}$ place. This can't come from the $\sum c_i \cdot a_i$ part, so must come from the

the $\sum 2c_i \cdot b_{f(i)}$ part. This means $\exists i(f(i) = n)$. Then $b_n \in CL(H)$ if and only if $n \in ran(f)$. □

## 4.4 Existence of the convex $\ell$-subgroup generated by convex $\ell$-subgroups $A, B$.

In the setting of totally ordered groups, the question is trivial, since $CL(A, B)$ is simply the larger of the two or, equivalently, their union.

The first version of this proof uses computable algebra, and is followed by a more direct proof typical of Reverse Math. In all but the easiest reversals, it seems easier to work in the computable setting, and build an computable encoding object by a step-by-step construction, and to then use the process of the construction to help define the object in more general terms using $\Delta^0_1$ formulas. Theorem 4.6 allows us to simplify both versions of the proof by looking at $\langle A, B\rangle$ instead of $CL(A, B)$.

**Theorem 4.9.** *There is a computable abelian $\ell$-group $G$ with computable convex $\ell$-subgroups $A, B$ such that $A + B \geq_1 0'$.*

**Corollary 4.10.** ($\mathsf{RCA}_0$) *The following are equivalent.*

1. *For any convex $\ell$-subgroups $A, B$ of the $\ell$-group $G$, the subgroup $\langle A, B\rangle$ exists.*

2. $\mathsf{ACA}_0$.

*Proof.* As in the proof of Theorem 2.4, we construct an injection from a computable $\ell$-group $G$ into the $\ell$-group $D = \bigoplus_\omega \mathbb{Z}$, equipped with the pointwise order. Elements of $D$ are finite sequences of integers with the last entry nonzero. The image of $G$ in $D$ will be a (nonconvex) $\ell$-subgroup of $D$, yet classically isomorphic to the full group. $G$ will contain computable convex $\ell$-subgroups $A, B$ such that $A + B = \langle A, B \rangle$ is $\geq_1 0'$.

We construct our computable group $G = \cup_s G_s$ in stages. Each $G_s$ will be a finite set of integers, and representation function $\sigma_s : G_s \to D$. For all elements $n \in G_s, \sigma_s(n)$ will be a finite string of integers with no trailing zeros. We will define $n \circ_s m = k$ if $\sigma_s(n) + \sigma_s(m) = \sigma_s(k)$. The operation $\circ$ will be $\cup_{s \in \omega} \circ_s$. Similarly, we define $\wedge_s, \vee_s$ whose union will be the usual meet and join on $G$. The partial order on $G$ can be recovered from $\vee$ and $\wedge$ since $a \wedge b = b \leftrightarrow b \leq a$.

The construction of $G$ will be done accomplishing the following:

- For some $m(s) \in \omega$ we will assign to all $p \leq m(s)$ a string $\sigma_s(p)$.
- If $t > s$, then $m(t) \geq m(s)$.
- If $p \leq m(s)$, then $\sigma_s(p) = \sigma_t(p)$ for all $t \geq s$.

Additionally, $G$ will have computable convex $\ell$-subgroups $A, B$. Once $\sigma_s(p)$ is defined, the membership of $p$ in $A$ or $B$ will be computable from $\sigma_s(p)$. We will have $p \in A \iff \sigma_s(p)(n) = 0$ for each odd $n$ up to $|\sigma_s(p)|$, and $p \in$

$B \iff \sigma_s(p)(n) = 0$ for each even $n$ up to $|\sigma_s(p)|$. We will meet the following requirements:

- **Group Closure**

  $C_e$: If $e = \langle p, q\rangle$, then $p \circ q$ is defined.

- **Group Inverses**

  $I_p$: There exists a $q$ such that $p \circ q = 0$ (0 denotes the zero of $\omega$ and the identity of $G$.)

- **Meet and Join**

  $M_e, J_e$: If $e = \langle p, q\rangle$, then $p \wedge q$, $p \vee q$ are defined.

- **A∨B non-computability requirements**

  $N_e$: $\langle A, B\rangle$ can compute whether $\phi_e(e)$ halts.

We order the requirements as follows: $N_0 \geq C_0 \geq M_0 \geq J_0 \geq I_0 \geq N_1 \geq \cdots$

**Definition 4.11.** *We say*

1. $C_e$ requires attention *at stage* $s+1$ *if* $e = \langle p, q\rangle$ *for some* $p, q \leq m(s)$ *and there is no* $r \leq m(s)$ *such that* $\sigma_s(p) + \sigma_s(q) = \sigma_s(r)$.

2. $M_e$ requires attention *at stage* $s+1$ *if* $e = \langle p, q\rangle$ *for some* $p, q \leq m(s)$ *and there is no* $r \leq m(s)$ *such that* $\sigma_s(p) \wedge \sigma_s(q) = \sigma_s(r)$, *and similarly for* $J_e$.

*3.* $I_p$ requires attention *at stage* $s+1$ *if* $p \leq m(s)$ *and there is no* $q \leq m(s)$ *such that* $\sigma_s(p) + \sigma_s(q) = 0$

*4.* $N_e$ requires attention *at stage* $s+1$ *if* $N_e$ *is* unrealized *and either*

*(a) for no* $t \leq s$ *is there a* $p$ *such that* $\sigma_s(p) = 0^{2e}11$ *(in which case we say* $N_e$ *is* inactive*); or*

*(b) there exists* $p$ *as above and* $\phi_{e,s}(e)\downarrow$ *(in which case we say* $N_e$ *is* active*).*

### 4.4.1 Construction

*Stage* 0. Set $p(0) = 0$ and $\sigma_0(0) = 0$. The zero of $\omega$ is to be the identity of $\langle G, \circ \rangle$.

*Stage* $s+1$. Let $R$ be the requirement of highest priority that requires attention.

*Case* 1: $R$ is $C_e$ with $e = \langle p, q \rangle$. Define $m(s+1) = m(s)+1$. Define $\sigma_{s+1}(r)$ for $r \leq m(s+1)$ via:

$$\sigma_{s+1}(r) = \begin{cases} \sigma_s(r) & \text{if } r < m(s+1), \\ \sigma_s(p) + \sigma_s(q) & \text{if } r = m(s+1). \end{cases}$$

*Case* 2: $R$ is $I_p$. Let $m(s+1) = m(s)+1$. Define $\sigma_s(r)$ for $r \leq m(s+1)$ via:

$$\sigma_{s+1}(r) = \begin{cases} \sigma_s(r) & \text{if } r < m(s+1), \\ -\sigma_s(p) & \text{if } r = m(s+1). \end{cases}$$

*Case* 3: $R$ is $M_e$ with $e = \langle p, q \rangle$. Define $m(s+1) = m(s)+1$. Define $\sigma_{s+1}(r)$ for $r \leq m(s+1)$ via:

$$\sigma_{s+1}(r) = \begin{cases} \sigma_s(r) & \text{if } r < m(s+1), \\ \sigma_s(p) \wedge \sigma_s(q) & \text{if } r = m(s+1). \end{cases}$$

*Case* 4: $R$ is $J_e$. Similar to case 3.

*Case* 5: $R$ is $N_e$ and $N_e$ is inactive. Let $m(s+1) = m(s)+1$ and define $\sigma_{s+1}$ for $r \leq m(s+1)$ via:

$$\sigma_{s+1}(r) = \begin{cases} \sigma_s(r) & \text{if } r < m(s+1), \\ 0^{2e}11 & \text{if } r = m(s+1). \end{cases}$$

At this point, $N_e$ becomes active.

*Case* 6: $R$ is $N_e$ and $N_e$ is active. Thus, there is a $p \leq m(s)$ such that $\sigma_s(p) = 0^{2e}11$ and $\phi_{e,s}(e) \downarrow$. Let $m(s+1) = m(s)+2$, and define $\sigma_{s+1}$ for $r \leq m(s+1)$ via:

$$\sigma_{s+1}(r) = \begin{cases} \sigma_s(r) & \text{if } r \leq m(s) \\ 0^{2e}1 & \text{if } r = m(s)+1 \\ 0^{2e+1}1 & \text{if } r = m(s)+2 \end{cases}$$

This creates elements of $G$ in $A$ and $B$, respectively, whose group sum is $p$, thereby putting $p \in \langle A, B \rangle$. $N_e$ is now realized. Notice that this will ensure $\langle A, B \rangle \geq_1 0'$: To determine if $e \in 0'$, find $p$ such that $\sigma(p) = 0^{2e}11$. Then $e \in 0' \iff p \in \langle A, B \rangle$.

### 4.4.2 Verification

$G$ is clearly a computable $\ell$-group by the construction. $A, B$, and $\langle A, B\rangle$ are easily verified as convex $\ell$-subgroups. For example, $A$ contains the elements $p$ such that $\sigma(p)$ is zero in all odd-numbered components. The operations of group sum, meet and join on two elements of $A$ cannot introduce a nonzero entry into an odd-numbered component with respect to the map $\sigma$, so $A$ is an $\ell$-subgroup. As for the convexity of $A$: suppose $a \in A$ and $0 \leq |g| \leq |a|$. It follows that $\sigma(g)$ is zero in all odd-numbered components, and so $g \in A$.

The verification for $B, \langle A, B\rangle$ is very similar, except that in the case of $\langle A, B\rangle$, we say $p \in \langle A, B\rangle \iff \sigma(p)$ has nonzero entries only in components numbered $2e$ or $2e+1$ where $\phi_e(e)\downarrow$. □

Now, we give a formal proof of the reverse math corollary.

**Theorem 4.12.** ($\mathsf{RCA}_0$) *The following are equivalent.*

1. $\mathsf{ACA}_0$
2. *If $A, B$ are convex $\ell$-subgroups of $G$, then*

$$\exists X \forall t (t \in X \leftrightarrow \exists n (t \in \langle A \cup B\rangle_n)).$$

*Proof.* Since $X$ has a $\Sigma^0_1$ definition, $1 \to 2$. Now we show $2 \to 1$. Fix a one-to-one function $f$. We define an injection $\sigma : \mathbb{N} \to Fin^*_{\mathbb{Z}}$ by primitive recursion. The group $G$ will be $\mathbb{N}$ with $+_G$ given by $g +_G h = k \leftrightarrow \sigma(g) +_{Fin^*_{\mathbb{Z}}} \sigma(h) = \sigma(k)$, and we define $\alpha_e = 0^{2e}11, \beta_e = 0^{2e}1$, and$\gamma_e = 0^{2e+1}1$.

- Let $\sigma(0) = 0$ (as a string)

- For $r = 5m+1$, set $\sigma(r) = \alpha_e$ where $e$ is least such that $\forall k < r(\sigma(r) \neq \alpha_e)$.

(This will be the default action, if the test condition fails in other stages.)

- For $r = 5m + 2$, let $\langle i, j\rangle$ be $\mathbb{N}$-least such that $i, j < r$ and $\forall k < r(\sigma(i) + \sigma(j) \neq \sigma(k))$. If such a pair exists, define $\sigma(r) = \sigma(i) +_{Fin^*_{\mathbb{Z}}} \sigma(j)$, otherwise perform the default action.

- For $r = 5m + 3$, let $\langle i, j\rangle$ be $\mathbb{N}$-least such that $i, j < r$ and $\forall k < r(\sigma(i) \wedge \sigma(j) \neq \sigma(k))$. If such a pair exists, define $\sigma(r) = \sigma(i) \wedge \sigma(j)$, otherwise perform the default action.

- For $r = 5m+4$, let $i$ be $\mathbb{N}$-least such that $i < r$ and $\forall k < r(\sigma(i)+_{Fin^*_{\mathbb{Z}}}\sigma(k) \neq 0$. If such $i$ exists, define $\sigma(r) = \sigma(i)^{-1}$, otherwise perform the default action.

- For $r = 5m + 5$ look for $\mathbb{N}$-least $e < r$ s.t. $\exists k < r(\sigma(k) = \alpha_e)$ & $\neg\exists k < r(\sigma(k) = \beta_e$ or $\sigma(k) = \gamma_e)$ & $\exists k < r(f(k) = e)$. Then we define $\sigma(r) = \beta_e$.

Then we define the sets

$$\begin{aligned} A &= \{n : \forall s(2s + 1 \leq |\sigma(n)| \to \sigma(n)[2s + 1] = 0)\} \\ B &= \{n : \forall s(2s \leq |\sigma(n)| \to \sigma(n)[2s] = 0)\} \end{aligned}$$

It is easy to verify that $A, B$ are both convex $\ell$-subgroups. Let $e \in \mathbb{N}$. By definition of $\sigma$, there is some $k$ s.t. $\sigma(k) = \alpha_e$. If $e \in ran(f)$, then by definition of $\sigma$, there are $m, n$ s.t. $\sigma(n) = \beta_e, \sigma(m) = \gamma_e$. Then $m \in A$ and $n \in B$. Then $\sigma(n)+\sigma(m) =$

$\alpha_e = \sigma(k)$, so $k \in \langle A, B\rangle$. On the other hand, suppose $k \in \langle A, B\rangle = A + B$. Then there exist $m \in A, n \in B$ s.t. $m + n = k$ i.e., $\sigma(m) + \sigma(n) = \alpha_e$. But, by the definitions of $\alpha_e$ and $A, B$, this means that all entries of $\sigma(m), \sigma(n)$ must be zero except at $2e+2$ and $2e+1$, respectively. This implies that $\sigma(n) = \beta_e$, which can only happen if $\exists j < r(f(j) = e)$, by definition of $\sigma$. Thus we define a function $\phi(e)$ by $\phi(e) = k \leftrightarrow k \leq 5e + 1$ & $\sigma(k) = \alpha_e$. By the construction, $\phi$ is total and definable in $\mathsf{RCA}_0$. By the verification, $ran(f) = \{e : \phi(e) \in \langle A \cup B\rangle\}$.

□

### 4.5 Existence of the Polar $X^\perp$.

**Definition 4.13.** *Two elements $a, b$ of an $\ell$-group are said to be* orthogonal *if $a \wedge b = e$.*

**Definition 4.14.** *Let $M$ be a subset of the $\ell$-group $G$. The polar of $M$, denoted $M^\perp$, is defined as the set $\{g \in G : \forall x \in M(|x| \wedge |g| = e)\}$.*

**Theorem 4.15.** ($\mathsf{RCA}_0$) *If it exists, $M^\perp$ is a convex subgroup of $G$.*

*Proof.* Adapted from [1]. We verify that $M^\perp$ is a subgroup and is convex. Suppose $g, h$ are positive elements of $M^\perp$. Let $m \in M$. Then

$$e = |m| \wedge g = |m| \wedge (|m| \wedge h)g = |m| \wedge (|m|g) \wedge (hg) = |m| \wedge hg.$$

Since the definition of $M^\perp$ uses absolute value, inverses are automatically included, and the identity satisfies the definition. Thus, checking composition is enough to show that $M$ is a subgroup. For convexity, suppose $b \in M^\perp$ and $|a| \leq |b|$. Then

$$|a| \leq |b| \rightarrow e \leq |m| \wedge |a| \leq |m| \wedge |b|.$$

Since $b \in M^\perp$, $|m| \wedge |b| = e$, and therefore $|m| \wedge |a| = e$. So $a \in M^\perp$. □

Note that if $M$ is finite, $M^\perp$ has a $\Pi^0_0$ definition, so exists in $\mathsf{RCA}_0$. In particular, for each $g \in G$, $g^\perp = \langle g \rangle^\perp$ exists in $\mathsf{RCA}_0$. Such polar subgroups are called principal polars. In general, though, $M^\perp$ is $\Pi^0_1(M)$ and can be complicated.

When seeking a reversal for the existence of $M^\perp$, it is worth considering how much structure $M$ should have – when $M$ is finite, the case is simple. When $M$ is infinite, is proving the existence of $M^\perp$ any simpler if $M$ is already, say, a subgroup, $\ell$-subgroup, or even convex $\ell$-subgroup? The following shows that, in general, it is not.

**Theorem 4.16.** ($\mathsf{RCA}_0$) *Let $G$ be an $\ell$-group. The following are equivalent.*

1. *For every $M \subseteq G$, $M^\perp$ exists.*

2. *For every convex $\ell$-subgroup $M \subseteq G$, $M^\perp$ exists.*

3. $\mathsf{ACA}_0$

*Proof.* 1 $\Rightarrow$ 2 is trivial, and 3 $\Rightarrow$ 1 by the arithmetical definition of $M^\perp$. It remains to show 2 $\Rightarrow$ 3. We will construct an abelian $\ell$-group $G$ with a convex $\ell$-subgroup $M$ such that $M^\perp$ computes the range of a given one-to-one function. Group theoretically, $G$ is a restricted Hahn group on the root system $\Gamma$ which may be described as $\omega$ incomparable copies of an $\omega^*$ ordering.

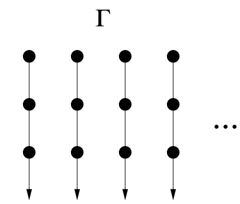

**Fig. 4.1:** The Root System $\Gamma$

We formalize this group in $\mathsf{RCA}_0$: let $G$ be the free abelian group on generators $a_{ij}$. That is, an element of $G$ is a reduced finite sum $\sum_{1\le i\le m, 1\le j\le n} c_{ij}a_{ij}$, where $c_{ij} \in \mathbb{Z}$ and $\exists i \exists j (c_{mj} \neq 0 \ \&\ c_{in} \neq 0.)$ That is, the normal form for an element has coefficients indexed by an $m \times n$ array, where $m, n$ are as small as possible in the sense that the last column and last row must each contain some nonzero coefficient. We may think of each $a_{ij}$ as representing the $j^{th}$ element of the $i^{th}$ column of $\Gamma$. The underlying formal representation uses triples $\langle m, n, c\rangle$ where $c$ is a function from $\{\langle i, j\rangle : 1 \le i \le m, 1 \le j \le n\}$ to $\mathbb{Z}$. As with Example 1.9, the group operation is componentwise addition, with cancellation. (If adding elements of different sizes, one may perform the operation with oversized arrays (using extra 0s) and then put the result in normal form by eliminating unnecessary rows and columns.) Thus, the inverse of the element $\sum_{i\le m, j\le n} c_{ij}a_{ij}$ is given by $\sum_{i\le m, j\le n} -c_{ij}a_{ij}$, and the group identity is represented by $\langle \emptyset, \emptyset, \emptyset\rangle$.

Let $g = \langle m, n, c\rangle$ be an element of $G$ and let $S_g = \{i \le m : \exists j \le n(c_{ij} \neq 0)\}$, that is, $S_g$ is the set of indices $i$ such that $g$ has a nonzero coefficient in the $i^{th}$ column. An element in a Hahn group is positive if it is so at each maximal element of its support. Thus $g = \langle m, n, c\rangle$ is positive iff the set

$$S_g^{max} = \{c_{ij} : i \in S_g, j \leq n \ \& \ c_{ij} \neq 0 \ \& \ \forall k < j(c_{ik} = 0)\}$$

contains only positive numbers. This allows us determine the partial order $\leq_G$. For example, $a \leq b \leftrightarrow e \leq ba^{-1}$, i.e., $S_{ba^{-1}}^{max}$ only contains positive numbers. Equivalently, suppose we have two elements $c, d$ with coefficients $c_{ij}, d_{ij}$ defined on an $x \times y$ array. Then

$$c \leq d \leftrightarrow \forall i \leq x[\exists j \leq y(c_{ij} \neq d_{ij}) \rightarrow [d_{ik} > c_{ik} \text{ where } k = \mu s(c_{is} \neq d_{is})]].$$

This reasoning behind this is that when attempting to compare the two elements $c, d$ by testing to see if $cd^{-1}$ is positive, the maximal elements of the support of $cd^{-1}$ correspond to the least-numbered row in each column such that differing entries can be found.

So far, $G$ is a *p.o.*-group in $\mathsf{RCA}_0$. Classically, we know it to be an $\ell$-group. To verify that it is an $\ell$-group in $\mathsf{RCA}_0$, we need to be able to calculate the join of elements $a = \langle m, n, c\rangle$ and $b = \langle p, q, d\rangle$. Putting some formality aside, we describe an algorithm which can be used to calculate $a \vee b$ and claim that a function that uses said algorithm to calculate joins is $\Sigma_0^0$ definable.

First, letting $x = max(m, p), y = max(n, q)$ we work with the "improper" representations $a^* = \langle x, y, c^* \rangle$ and $b^* = \langle x, y, d^* \rangle$ where

$$c^*_{ij} := \begin{cases} c_{ij} & \text{if } 1 \leq i \leq m \;\&\; 1 \leq j \leq n \\ \\ 0 & \text{if } m < i \leq x \text{ or } n < j \leq y \end{cases}$$

and $d^*$ is defined similarly.

We build the join $a \vee b$ by using $c^*$ and $d^*$ to construct a coefficient function $h$ for an $x \times y$ array, and then, if necessary, we reduce the array size to eliminate unnecessary rows or columns of zeros. For each $i \leq x$, one compares the $i^{th}$ columns of $c^*$ and $d^*$, and defines the $i^{th}$ coefficient column of $h$ according to three cases.

1. If $\forall j \leq y(c^*_{ij} = d^*_{ij})$, then $\forall j \leq y$ we define $h^*_{ij} := c^*_{ij}$.

2. If, at the least $j$ such that $c^*_{ij} \neq d^*_{ij}, c^*_{ij} > d^*_{ij}$, then $\forall j \leq y$ we define $h^*_{ij} := c^*_{ij}$.

3. If, at the least $j$ such that $c^*_{ij} \neq d^*_{ij}, c^*_{ij} < d^*_{ij}$, then $\forall j \leq y$ we define $h^*_{ij} := d^*_{ij}$.

Essentially, this procedure compares the $i^{th}$ columns as if they were elements of the lexicographically ordered direct sum $\bigoplus_\omega \mathbb{Z}$, and takes the larger of the two for the $i^{th}$ column of the join. This follows from the Hahn order on the root system $\Gamma$, which in this case ends up being a "pointwise" order on the columns of $\Gamma$, where each column is given a lexicographic ordering.

To see that the resulting $h$ gives us a join for $\langle x, y, c^* \rangle$ and $\langle x, y, d^* \rangle$, we consider each column. Fix some $i$, and consider the $i^{th}$ column. If $c^* = d^*$ in the $i^{th}$ column, then any "larger" column would be unsuitable for a least upper bound, and any "smaller" column wouldn't work for an upper bound.

If $c^* > d^*$ at the first disagreement in the $i^{th}$ column, then the $i^{th}$ column of $c^* - d^*$ will be positive at the maximal element of its support. Since we use $c^*$ to define $h$ in this case, we have $h = c^*$ and $h > d^*$ in the $i^{th}$ column. Any "larger" column would not contribute to a *least* upper bound, and any "smaller" column would result in an element that was no longer an upper bound of $\langle x, y, c^* \rangle$.

The remaining case is similar. Thus, after reducing, one gets the join of $a \vee b$ in normal form with no extraneous rows or columns of zeros. This algorithm gives rise to a $\Sigma^0_0$ definition for the join function, so $\mathsf{RCA}_0$ proves that $G$ exists and is an $\ell$-group.

Now, on to the reversal. Let $f$ be a one-to-one function. Let $M = \{\langle m, n, c \rangle \in G : \forall i \leq m \forall j \leq n (c_{ij} \neq 0 \to \exists k \leq j (f(k) = i))\}$.

**Claim.** *$M$ is a convex $\ell$-subgroup of $G$.*

*Proof.* The question of inverses is easy, since the support of the coefficient function is identical for an element and its inverse. The support of the coefficient function for a group sum is contained in the union of the supports of its summands' coefficient functions, all of which must satisfy the condition in the definition of $M$. Thus, we have that $M$ is at least a subgroup. Suppose that $x, y \in M$. Since the columns of $x \vee y$ are columns from either $x$ or $y$, all of which satisfy the condition of $M$, the coefficients of $x \vee y$ must satisfy the conditions of $M$. So $M$ is closed under meet (and join), and is an $\ell$-subgroup.

To verify convexity, suppose that $|x| \leq |m|$ and $m \in M$. Suppose, for a contradiction, that $x \notin M$. Then $\exists i, j(|x|_{ij} \neq 0 \ \& \ \forall k \leq j(f(k) \neq i))$. Without loss of generality, take $j$ to be the least so that this is true for the given $i$, that is, $\forall k < j(|x|_{ik} = 0)$. Since $|x|$ is positive, $|x|_{ij}$, as the maximal element of the support of the $i^{th}$ column, must be positive. Then, since $|m| \geq |x|$, either $\forall s(|m|_{is} = |x|_{is})$, (which is impossible, since it implies that $m \notin M$) or, at the first place they differ in the $i^{th}$ column, $|m|_{is} > |x|_{is}$. This would imply that either $|m|_{ij} > |x|_{ij} > 0$, or for some $k < j(|m|_{ik} > 0)$. However, $\forall k \leq j(f(k) \neq i) \rightarrow \forall k \leq j(|m|_{ik} = 0)$, so neither case is possible, and we have our contradiction. □

Then the convex $\ell$-subgroup $M$ is definable by a bounded-quantifier formula, so exists in $\mathsf{RCA}_0$.

Let $\alpha_{uv}$ denote the element $\langle u, v, c \rangle$, where

$$c_{ij} = \begin{cases} 1 & \text{if } i = u \ \& \ j = v \\ 0 & \text{otherwise.} \end{cases}$$

Suppose $f(j) = i$. Then $\alpha_{ij} \in M$, so $|\alpha_{i0}| \wedge |\alpha_{ij}| = |\alpha_{ij}| \neq e$ and $\alpha_{i0} \notin M^{\perp}$. On the other hand, suppose $\alpha_{i0} \in M^{\perp}$. Then, for all $m \in M$, $|\alpha_{i0}| \wedge |m| = e$. In particular, no $\alpha_{ij}$ is in $M$, since $|\alpha_{i0}| \wedge |\alpha_{ij}| = |\alpha_{ij}|$. But $[(\forall j)\alpha_{ij} \notin M] \rightarrow i \notin ran(f)$. Thus we have $i \in ran(f) \iff \alpha_{i0} \notin M^{\perp}$. □

The reversals of this chapter can be summarized as follows:

**Theorem 4.17.** ($\mathsf{RCA}_0$) *Let $G$ be an $\ell$-group. The following are equivalent:*

1. $\mathsf{ACA}_0$
2. *The existence of the subgroup generated by two subgroups $A, B$.*
3. *The existence of the convex $\ell$-subgroup generated by two convex $\ell$-subgroups $A, B$.*
4. *The existence of the convex $\ell$-subgroup generated by a (nonconvex) $\ell$-subgroup $A$.*
5. *The existence of the polar subgroup $A^{\perp} = \{g \in G : (\forall a \in A)|g| \wedge |a| = 1_G\}$*

# Chapter 5

# Prime Subgroups and Values

## 5.1 Prime Subgroups

**Definition 5.1.** *The convex $\ell$-subgroup $P$ is prime if*

$$\forall x \forall y [x \wedge y \in P \rightarrow x \in P \text{ or } y \in P].$$

The following lemma from [4] will be useful.

**Lemma 5.2.** ($\mathsf{RCA}_0$) *Let $g$ be an element of the $\ell$-group $G$ and $P$ be a convex $\ell$-subgroup of $G$. Then the set $C = \{x \in G : |g| \wedge |x| \in P\}$ is a convex $\ell$-subgroup of $G$.*

*Proof.* Let $x, y \in C$. Then $e \leq |x| \wedge |g| = h_1 \in P$ and $e \leq |y| \wedge |g| = h_2 \in P$.

$$\begin{aligned}
|xy^{-1}| \wedge |g| &\leq |x||y||x| \wedge |g| \text{ (by Thm. 2.20)} \\
&= |x||y||x| \wedge |x||y||g| \wedge |g| (\text{ since } |x||y||g| \geq |g|) \\
&= |x||y|(|x| \wedge |g|) \wedge |g| \\
&= |x||y|h_1 \wedge |g| \\
&\leq |x||y|h_1 \wedge |g|h_1 \\
&= (|x||y| \wedge |g|)h_1 \\
&= (|x||y| \wedge |x||g| \wedge |g|)h_1 (\text{ since } |x||g| \geq |g|\}) \\
&= (|x|(|y| \wedge |g|) \wedge |g|)h_1 \\
&= (|x|h_2 \wedge |g|)h_1 \\
&\leq (|x|h_2 \wedge |g|h_2)h_1 \\
&= (|x| \wedge |g|)h_2h_1 = h_1h_2h_1 \in P.
\end{aligned}$$

Thus, we have $e \leq |xy^{-1}| \wedge |g| \leq h_1h_2h_1$, so $|xy^{-1}| \wedge |g| \in P$ and $xy^{-1} \in C$. $C$ is therefore a subgroup of $G$. According to Theorem 2.22, the subgroup $C$ is an $\ell$-subgroup iff $\forall x \in C(x \vee e \in C)$. By Theorem 2.20 $|x \vee e| \leq |x|$. Thus $e \leq |x \vee e| \wedge |g| \leq |x| \wedge |g| \in P$, so $x \vee e \in C$ and $C$ is an $\ell$-subgroup. To show $C$ is convex, let $e \leq x \leq h$ where $h \in C$. Thus $|x| \leq |h|$ so $e \leq |x| \wedge |g| \leq |h| \wedge |g| \in P$, so $|x| \wedge |g| \in P$ and $x \in C$. $\square$

**Theorem 5.3.** ($\mathsf{RCA}_0$) *For a convex subgroup $P$ of the $\ell$-group $G$, the following are equivalent:*

1. *$P$ is prime.*

2. *$x \wedge y = 0 \rightarrow x \in P$ or $y \in P$.*

3. *$G/P$ is totally ordered under the induced order.*

4. *If $A, B$ are convex $\ell$-subgroups containing $P$ then $A \subseteq B$ or $B \subseteq A$.*

Note that $\mathsf{RCA}_0$ is sufficient to form the quotient group from (3). The proofs of $1 \rightarrow 2, 2 \rightarrow 3, 3 \rightarrow 4$ are in [1], whereas $4 \rightarrow 1$ is from [4].

*Proof.*

$1 \rightarrow 2$: Trivial.

$2 \rightarrow 3$: Given $g, h \in G$, we have

$$((g \vee h)g^{-1}) \wedge ((g \vee h)h^{-1}) = (g \vee h)(g^{-1} \wedge h^{-1}) = (g \vee h)(g \vee h)^{-1} = e.$$

WLOG, by 2, $(g \vee h)h^{-1} \in P$. Then $Ph = P(g \vee h) \geq Pg$.

$3 \rightarrow 4$: Suppose $A, B$ are convex $\ell$-subgroups containing $P$ s.t. $A \not\subseteq B$ and $B \not\subseteq A$. By taking absolute values if necessary, choose positive $a \in A \backslash B$ and positive

$b \in B \backslash A$. Then, WLOG, $Pa \geq Pb$, so there exists $p \in P$ s.t. $pa \geq b$. Since $P \subset A$, $pa \in A$ and by convexity we have $b \in A$, a contradiction.

$4 \rightarrow 1$: We prove $\neg 1 \rightarrow \neg 4$. Suppose $P$ is not prime, so there exists $a, b$ not in $P$ with $a \wedge b \in P$. Form the $\Sigma_0$ sets $A = \{x \in G : |x| \wedge |b| \in P\}, B = \{x \in G : |x| \wedge |a| \in P\}$. Let $x = a$. By Lemma 2.23, $|a| \wedge |b| \leq |a \wedge b|$. Since $a \wedge b \in P$, $|a \wedge b| \in P$, and $|a| \wedge |b| \in P$ by convexity, and we have $x \in A$. On the other hand, if $x = a$ then $x \notin B$. Thus we have $A \nsubseteq B$ and the proof of $B \nsubseteq A$ is similar. By the definitions of $A$ and $B$ and the convexity of $P$, it follows that $P \subseteq A$ and $P \subseteq B$. By Lemma 5.2, $A$ and $B$ are convex $\ell$-subgroups. Since $A$ and $B$ contain $P$ and are incomparable under inclusion, we have shown the contrapositive, $\neg 1 \rightarrow \neg 4$. □

### 5.2 Values

**Definition 5.4.** *Let $g$ be a nonidentity element of an $\ell$-group $G$. A value of $g$, denoted $V(g)$, is a convex $\ell$-subgroup maximal w.r.t not containing $g$.*

In general, values are not unique. The notation $V(g)$ serves mainly to denote that $V$ is maximal with respect to excluding $g$.

The most natural way to describe the maximality of a value would be to say $V$ is a value of $g$ if it is a convex subgroup not containing $g$ such that for every convex $\ell$-subgroup $W \supsetneq V, g \in W$. Unfortunately, this statement is $\Pi^1_1(V)$.

We can describe the maximality, however, in terms of convex closure, which is arithmetical.

**Definition 5.5.** *Let $g$ be a nonidentity element of the $\ell$-group $G$. A value of $g$ is a set $V$ such that*

- *$V$ is a convex $\ell$-subgroup (which is an arithmetical condition).*
- *$g \notin V$.*
- *$\forall x \notin V \exists n (g \in CL(V \cup \{x\})_n)$, that is, the convex $\ell$-subgroup generated by $V \cup \{x\}$ contains $g$.*

Thus, whether or not a set $V$ is a value of $g$ is decidable in $\mathsf{ACA}_0$.

**Theorem 5.6.** ($\mathsf{RCA}_0$) *Values are prime.*

*Proof.* The proof is adapted from [4] : Let $V$ be a value of $g$. Suppose there are elements $a, b > e$ such that $a \wedge b = e$ and $a \notin V$. Form the set $C = \{x \in G : |x| \wedge |g| \in V\}$. By Lemma 5.2, $C$ is a convex $\ell$-subgroup. Since $|x| \wedge |g| \leq |x|$ and $V$ is convex, every element of $V$ belongs to $C$.

Suppose, for a contradiction, that there exists an element $y \in C \backslash V$. By the definition of $V$ as a value, $g \in CL(V \cup \{y\})$. By Lemma 4.2, $CL(V \cup \{y\}) \subset CL(C) = C$. Then $g \in C$ so, by definition of $C$, $|g| \wedge |g| = |g| \in V$, a contradiction. So, $V = C$.

Now form the set $A = \{x \in G : |x| \wedge b \in V\}$. By Lemma 5.2, $A$ is a convex $\ell$-subgroup. Since $|x| \wedge b \leq |x|$ and $V$ is convex, every element of $V$ belongs to

$A$. Furthermore, we have assumed $a \notin V$, but $a \in A$. So $A$ strictly contains $V$, and since $V$ is a value, there is an $n$ s.t. $g \in CL(V \cup \{a\})_n$, the $n^{th}$-stage approximation to $CL(V \cup \{a\})$. As above, by properties of the convex closure, $A$ must contain $g$, so $|g| \wedge b \in V$. This implies that $b \in C$, and since $C = V$, we have $b \in V$. To recap, we have shown that $(a \vee b = e \;\&\; a \notin V) \rightarrow b \in V$, which implies $V$ is prime. □

## 5.3 Existence of a Sequence of Values

As mentioned above, values are not generally unique. However, in an *o*-group, the convex subgroups form a chain, so there is only one value for each element. Furthermore, in an *o*-group, any two elements are comparable.

**Definition 5.7.** *We say* $x \ll y$ *if* $\forall n(|x|^n < |y|)$, *and say* $x \approx y \leftrightarrow \neg(x \ll y$ *or* $y \ll x)$. *Equivalently,* $x \approx y \leftrightarrow \exists n([|x|^n \geq |y| \& |y|^n \geq |x|])$.

**Lemma 5.8.** ($\mathsf{RCA}_0$) *If* $a, b$ *are elements of an o-group, then exactly one of the three relations* $a \ll b, a \gg b, a \approx b$ *must hold.*

We will need the following:

**Lemma 5.9.** ($\mathsf{RCA}_0$) *Let* $A$ *be a subset of an o-group* $G$ *such that* $\forall x \in A(x \ll y)$. *Then* $\forall x \in G \forall n \in \mathbb{N}(x \in CL(A)_n \rightarrow x \ll y)$.

*Proof.* In the context of *o*-groups, join is trivial to compute since $a \vee b = max_{\leq_G}(a, b)$. The result follows by an induction on the definition of $CL(A)$. Since join is trivial, the only interesting case is the group operation, which is also resolved easily. □

**Lemma 5.10.** ($\mathsf{RCA}_0$) *Let $G$ be an o-group. Suppose $V$ is a value of $g$. Then $x \in V$ iff $x \ll g$.*

*Proof.* Let $x \in V$. Suppose $\neg(x \ll g)$. Then $x \approx g$ or $x \gg g$. Then, since $V$ is a convex $\ell$-subgroup, $x$ generates $g \in V$, a contradiction. For the other direction, suppose $x \ll g$ and $x \notin V$. By Lemma 5.9, $\forall h \forall n (h \in CL(V \cup \{x\})_n \rightarrow h \ll g)$. In particular, $\forall n (g \notin CL(V \cup \{x\}))$. Along with the fact that $x \notin V$, this violates the third condition of Definition 5.5, so $V$ is not a value and we have our contradiction.

□

**Corollary 5.11.** ($\mathsf{RCA}_0$) *Let $G$ be an o-group. Let $x, y$ be distinct elements of $G$, and $V(x), V(y)$ be values of $x, y$, respectively. Then $x \approx y \leftrightarrow x \notin V(y)$ & $y \notin V(x)$.*

Now, suppose one had a set $K$ coding a sequence of values $V_i$ for each nonidentity $g_i \in G$. By the corollary above, $K$ can compute the set of pairs $R = \{\langle i, j \rangle : g_i \approx g_j\}$ and thus also compute a set of archimedean class representatives $C = \{i : (\forall s <_{\mathbb{N}} i) \langle i, s \rangle \notin R\}$. In [7], Solomon & Downey proved that the existence of a set of archimedean class representatives for an abelian $o$-group is equivalent to $\mathsf{ACA}_0$. Thus, the existence of a sequence of values implies $\mathsf{ACA}_0$.

**Theorem 5.12.** ($\mathsf{RCA}_0$) *The following are equivalent.*

1. *For every o-group $G$ the sequence of values $V_i = V(g_i)$ exists.*

*2.* $\mathsf{ACA}_0$

**Corollary 5.13.** ($\mathsf{RCA}_0$) *The existence of a sequence of values for an $\ell$-group implies* $\mathsf{ACA}_0$.

Together with this corollary, the following theorem constitutes an equivalence of the existence of a sequence of values to $\mathsf{ACA}_0$.

**Theorem 5.14.** ($\mathsf{RCA}_0$) $\mathsf{ACA}_0$ *implies the existence of a sequence of values for an $\ell$-group.*

*Proof.* Let $G$ be enumerated as $g_0, g_1 \dots$. Let $A$ be (the code for) a finite subset of $G$. Using the mechanism of convex closure defined earlier, we define a bounded-quantifier relation $\Psi(A, i, s)$ such that $g_i \in CL(A) \leftrightarrow \exists s \Psi(A, i, s)$. Informally, $s$ represents a stage of the construction of $CL(A)$ such that $g_i \in CL(A)_s$. In $\mathsf{ACA}_0$, we may form the set $S$ of pairs $\langle A, i \rangle$ such that $A$ is a (code for a) finite set, and $\forall s \neg \Psi(A, i, s)$. We then define a function $f(j, n) : \mathbb{N}^2 \to \{0, 1\}$. We define by primitive recursion on $n$:

*Case n=0:* $$f(j,0) = \begin{cases} 1 & \text{if } \langle \{g_0\}, j \rangle \in S \\ 0 & \text{if } \langle \{g_0\}, j \rangle \notin S. \end{cases}$$

*Case n+1:* $$f(j,n+1) = \begin{cases} 1 & \text{if } \langle (\{g_k : k \leq n \ \& \ f(j,k) = 1\} \cup \{g_{n+1}\}, j \rangle \in S \\ 0 & \text{if } \langle (\{g_k : k \leq n \ \& \ f(j,k) = 1\} \cup \{g_{n+1}\}, j \rangle \notin S. \end{cases}$$

**Claim.** *For each $j$, the set $W = \{g_k : f(j,k) = 1\}$ is a value of $g_j$.*

*Proof.* Each successive element $g_k$ is included or excluded by $f$ based solely on whether its inclusion would eventually cause $g_j$ to be generated. By Lemma 4.3, the convex closure of a set of elements is unaffected by adding group inverses, compositions, joins, and positive elements bounded above by a member of that set. For example, if $f(j,5) = 1$, and $g_6 = g_5^{-1}$, then $f(j,6) = 1$ because including inverses will not cause any new elements (particularly $g_j$) to enter the convex closure. The other criteria for a convex $\ell$-subgroup are satisfied similarly. Thus $W$ is a convex $\ell$-subgroup. By the definition of $f$, $g_j \notin W$. Also by the definition of $f$, any element not in $W$ is excluded specifically because including it would generate $g_j$. □

□

## 5.4 Existence of a Sequence of Excluding Primes

**Definition 5.15.** *An excluding prime for $g$, denoted $P(g)$, is a prime convex $\ell$-subgroup not containing $g$.*

Since values are prime, a value $V(g)$ is a maximal excluding prime for $g$. However, it is easy to show that there are, in general, non-maximal excluding primes. Take the $o$-group obtained by lexicographically ordering $\mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}$. The element $(1,0,0)$ is excluded by the convex $\ell$-subgroups generated by $(0,1,0)$ and $(0,0,1)$, both of which are prime, as are all convex subgroups of an $o$-group. However, the latter is a proper subgroup of the former.

**Lemma 5.16.** ($\mathsf{RCA}_0$). *Let $G$ be an abelian $\ell$-group, with $G = \{g_0 = e, g_1, \ldots\}$. Then there is a uniform sequence of infinite trees $\langle T_1, T_2, \ldots\rangle$ such that $\forall m \geq 1, f \in [T_m] \leftrightarrow f$ is the characteristic function of a prime subgroup not containing $g_m$.*

*Proof.* For each $\sigma \in 2^{<\omega}$ we write $g_i \in \sigma \leftrightarrow \sigma(i) = 1$ and abuse this notation by writing things like $|g_i| \in \sigma$ to mean $\sigma(k) = 1$, where $g_k = |g_i|$. For each $\sigma \in 2^{<\omega}$, define

$$\begin{aligned} S_\sigma \;=\; & \{k < |\sigma| : g_k \in \sigma \text{ or} \\ & \exists i < |\sigma|(g_i \in \sigma \;\&\; (g_i \cdot g_k = e \text{ or } |g_k| \leq |g_i|)) \text{ or} \\ & \exists i, j < |\sigma|(g_i, g_j \in \sigma \;\&\; (g_k = g_i \cdot g_j \text{ or } g_k = g_i \wedge g_j))\}. \end{aligned}$$

Note that $\tau \subseteq \sigma \to S_\tau \subseteq S_\sigma$. We define the relations $R, Q$ :

$$\begin{aligned} R(\sigma) &:= \forall i, j[(i < j < |\sigma| \;\&\; g_i \wedge g_j = e) \to (g_i \in \sigma \text{ or } g_j \in \sigma)]. \\ Q(\sigma) &:= \forall k < |\sigma|(g_k \in S_\sigma \to k \in \sigma). \end{aligned}$$

Note that $\tau \subseteq \sigma \to (R(\sigma) \to R(\tau) \;\&\; Q(\sigma) \to Q(\tau))$.We say $\sigma$ is $m$-acceptable if and only if $R(\sigma)$ & $Q(\sigma)$ & $|g_m| \notin \sigma$. Then $\tau \subseteq \sigma$ & $\sigma$ is $m$-acceptable $\to$ $\tau$ is $m$-acceptable. For $m \geq 1$, we define $T_m = \{\sigma \in 2^{<\omega} : \sigma \text{ is } m\text{-acceptable}\}$.

**Claim.** *If $f \in [T_m]$ then $f$ is the characteristic function of a prime subgroup not containing $g_m$.*

Let $f \in [T_m]$. Then $f(|g_m|) = 0$, since $f \restriction n$ is $m$-acceptable for all $n$. Since $Q(f \restriction n)$ for each $n$, $f$ codes a convex $\ell$-subgroup and since $R(f \restriction n)$ for each $n$, this convex $\ell$-subgroup is prime. □

If I can prove in $RCA_0$ that $T_m$ is infinite, $WKL_0$ will prove that there is a path, and hence a prime subgroup not containing $g_m$.

**Lemma 5.17.** ($\mathsf{RCA}_0$) *Every tree* $T_x, x \geq 1$, *is infinite. Formally,* $\forall n(T_x$ *has a node of length* $n)$.

*Proof.* Suppose not. Fix $x \geq 1$ and let $n$ be $\mathbb{N}$-least such that $T_x$ has no node of length $n$. If $n$ is less than the index of $|g_x|$, then we are done, since the string $1^n$ satisfies $Q, R$ and is $x$-acceptable, hence belongs to $T_x$. So assume $n \geq$ the index of $|g_x|$. Let $Y = \{\langle i, j\rangle : i < j < n \ \& \ g_i \wedge g_j = e\}$. We will construct a node $\sigma$ of length $n$ that is $x$-acceptable, so belongs to $T_x$. To satisfy $R$, $\sigma$ must contain at least one element from every pair in $Y$. Intuitively, it is easy to find a convex $\ell$-subgroup excluding a nonidentity element – one may choose the identity subgroup or consider a principal polar. The difficulty arises when we try to also require it to be prime. Thus, our first priority is to choose one element from each pair in $Y$. The next priority is to make sure that $Q$ is satisfied.

**Claim.** ($\mathsf{RCA}_0$) *If* $Y$ *contains* $m$ *pairs, there is a way to choose one element from each pair so that our choices do not generate* $|g_x|$*, in the sense of satisfying* $Q$*.*

Suppose the $m$ pairs of $Y$ are written as $\langle a_{i,0}, a_{i,1}\rangle$, with $0 \leq i \leq m-1$. A binary string of length $m$ can then represent a choice of one element from each pair. Given $\tau \in 2^m$, we form $\sigma_\tau$ with $|\sigma_\tau| = n$ by bounded $\Sigma^0_1$ comprehension: define

$$S_{\sigma_\tau} = \{k : k < n \ \& \ g_k \in CL(\{a_{i,\tau(i)} : i < m)\}\}$$

and then let $\sigma_\tau(k) = 1 \iff k \in S_{\sigma_\tau}$.

To prove the claim, we need to show that there is a $\tau \in 2^m$ such that $\sigma_\tau \in 2^n$ is $x$-acceptable. For $\tau$ with $|\tau| \leq m$, let $g_\tau = \prod_{i=0}^{|\tau|-1} a_{i,\tau(i)}$. Then the meet of all possible products with one factor from the first $k$ pairs in $Y$ is $\bigwedge_{\tau \in 2^k} g_\tau$. First we prove by induction that, for $k \leq m$, $\bigwedge_{\tau \in 2^k} g_\tau = e$. Case $k = 1$. We have one pair $a_{0,0}, a_{0,1}$ such that $a_{0,0} \wedge a_{0,1} = e$. In this case, the only possibilies for $g_\tau$ are $a_{0,0}$ and $a_{0,1}$, which clearly meet to the identity.

Suppose we have proved the result for $k < m$, and consider the case $k + 1$.

By the distributive law,

$$[(\bigwedge_{\tau \in 2^k} g_\tau) \cdot a_{k,0}] = \bigwedge_{\tau \in 2^k} (g_\tau \cdot a_{k,0}) = (\bigwedge_{\tau \in 2^{k+1} : \tau(k)=0} g_\tau).$$

Similarly,

$$[(\bigwedge_{\tau \in 2^k} g_\tau) \cdot a_{k,1}] = (\bigwedge_{\tau \in 2^{k+1} : \tau(k)=1} g_\tau).$$

Thus,

$$\bigwedge_{\tau \in 2^{k+1}} g_\tau = [(\bigwedge_{\tau \in 2^k} g_\tau) \cdot a_{k,0}] \wedge [(\bigwedge_{\tau \in 2^k} g_\tau) \cdot a_{k,1}].$$

By distribution again, this equals $(\bigwedge_{\tau \in 2^k} g_\tau) \cdot (a_{k,0} \wedge a_{k,1})$. The first factor is equal to $e$ by induction, and the second is equal to $e$ by definition of $Y$. This proves that $\bigwedge_{\tau \in 2^{k+1}} g_\tau = e$. By induction, $\bigwedge_{\tau \in 2^m} g_\tau = e$.

Since $G$ is abelian, it follows that $(g_\tau)^p = \Pi_{i=0}^{m-1}(a_{i,\tau(i)})^p$. By repeated application of Corollary 2.10, we have $\bigwedge_{\tau \in 2^m} (g_\tau)^p = e$.

Suppose, for a contradiction, that every way of choosing one element from each pair in $Y$ forced the generation of $|g_x|$, that is, for all $\tau \in 2^m, |g_x| \in S_{\sigma_\tau}$. By Lemmas 4.4 and 4.5, there is a $p \geq 0$ such that $\forall \tau \in 2^m(|g_x| \leq (g_\tau)^p)$. Thus $|g_x| \leq \bigwedge_{\tau \in 2^m}(g_\tau)^p = e$, a contradiction since $g_x \neq e$. Therefore, there is at least one $\tau$ which does not generate $|g_x|$. This completes the proof of the claim. To finish the proof of the lemma, fix any $\tau \in 2^m$ such that $|g_x| \notin S_{\sigma_\tau}$. Clearly $\sigma_\tau$ is $x$-acceptable, and $|\sigma_\tau| = n$, a contradiction. Therefore, each tree is infinite. □

So, we have a uniform sequence of infinite trees such that a path through $T_m$ codes a prime convex $\ell$-subgroup not containing $g_m$. What we really want, however, is a set uniformly coding a sequence of excluding prime subgroups. We accomplish this by coding all the trees $T_m$ into a single tree $T^*$ such that a path through $T^*$ uniformly computes a path through each $T_m$.

**Theorem 5.18.** $(\mathsf{WKL}_0)$ *Let $e = g_0, g_1, \ldots$ be an enumeration of the $\ell$-group $G$. Then there is a set $K$ such that $\forall x \geq 1$, $K_x$ is a prime subgroup of $G$ not containing $g_x$.*

**Lemma 5.19.** $(\mathsf{RCA}_0)$ *If $\langle T_1, \ldots \rangle$ is a sequence of infinite trees, then there is an infinite tree $T^*$ and a $\Sigma^0_0$ function $\phi(f,i)$ s.t.$\forall f \in [T^*](\phi(f,i)$ is a path in $T_i)$.*

We define, by induction, the tree $T^*$ and a labeling function $l : T^* \to \mathbb{N}\times 2^{<\omega}$. The root node $\lambda$ of $T^*$ is labeled $l(\lambda) = \langle 1, \lambda\rangle$. Induction step: If $\sigma \in T^*$ and $l(\sigma) = \langle i, \tau\rangle$, then $\sigma * j \in T^* \leftrightarrow \tau * j \in T_i$. Furthermore, we define

$$l(\sigma * j) = \begin{cases} \langle n+1, \lambda\rangle & \text{if } i = 1 \\ \langle i-1, \hat{\tau} * k\rangle & \text{if } i > 1 \end{cases}$$

where $n = max\{j : (\exists \hat{\sigma} \subsetneq \sigma)\pi_1(l(\hat{\sigma})) = j\}$ and $\hat{\tau}, k$ have the property that if $\hat{\sigma}$ is the longest proper substring of $\sigma$ such that $\pi_1(l(\hat{\sigma})) = i-1$, then $l(\hat{\sigma}) = \langle i-1, \hat{\tau}\rangle$, and $\hat{\sigma} * k \subseteq \sigma$. Here, $\pi_1$ denotes the projection function on the first component. (See Figure 5.1.) To prove that $T^*$ is infinite, we describe a method of producing nodes longer than a specified height. Let $m > 1$ be fixed. Since each $T_i$ is infinite, there exist $\sigma_i \in T_i$ for $i = 1, \ldots, m$ such that $|\sigma_i| = m$. If we run through the construction substituting $\sigma_i$ for $T_i$, we will be able to produce a node in $T^*$ of length greater than $m$.

Given $\{\sigma_i : 1 \leq i \leq m\}$, let $f$ be the function which on input $\langle \sigma, l(\sigma)\rangle$ returns the pair $\langle \sigma * j, l(\sigma * j)\rangle$ as defined in the construction above, replacing $T_i$ with $\sigma_i$, or more precisely, the tree consisting of all strings contained in $\sigma_i$.

Suppose $f^k(\langle 1, \lambda\rangle) = \langle \mu, \langle i, \tau\rangle\rangle$. Then $f(\langle \mu, \langle i, \tau\rangle\rangle)$ has two components. The first component is found by looking in $\sigma_i$ for the string $\tau$. We extend $\mu$ by the next bit of $\sigma_i$ after $\tau$, resulting in $\mu * \sigma_i(|\tau| + 1)$ The second component has two cases. If $i = 1$, then the second component is $\langle n+1, \lambda \rangle$, where $n = max\{j : (\exists \hat{\sigma} \subsetneq \mu)\pi_1(l(\hat{\sigma})) = j\}$. If $i > 1$, then we look for the longest proper substring $\hat{\sigma} \subsetneq \mu$ whose label has first component $i-1$. Because we are working with the non-branching tree generated from $\sigma_i$ instead of the whole of $T_i$, we know that $l(\hat{\sigma}) = \langle i-1, \sigma_{i-1} \upharpoonright j \rangle$ for some $j$. In this case, the second component is $\langle i-1, \sigma_{i-1} \upharpoonright j+1 \rangle$.

This construction "visits" $T_1$, then $T_2, T_1$, then $T_3, T_2, T_1$, etc. So, just given $\sigma_i \in T_i$ of length $m$ we will be able to define at least $\frac{(m-1)(m)}{2}$ iterates of $f$. Since each iteration produces a longer node of $T^*$, this is enough to produce a node longer than $m$ bits.

**Claim.** *If $f$ is a path in $T^*$, then $f$ computes a path in $T_i$ for each $i$.*

*Proof.* By primitive recursion, we can define a function $g(i,j)$ such that $g(i,j)$ is the level in $T^*$ coding the $j^{th}$ level of $T_i$. For any $f \in [T^*]$, $l(f \upharpoonright g(i,j))$ has the form $\langle i, \tau \rangle$, where $|\tau| = j$. Thus, $f(g(i,j))$ is the $j^{th}$ bit of the path in $T_i$ coded by $f$, and the function $h_i(j) := f(g(i,j))$ gives a path through $T_i$. $\square$

Now, $\mathsf{RCA}_0$ proves that $T^*$ exists and that paths through $T_i$ correspond to prime subgroups of $G$ not containing $g_i$. $WKL_0$ proves that $T^*$ has a path, and we have seen that such a path can uniformly compute paths through each $T_i$. Thus, we have proved Theorem 5.18.

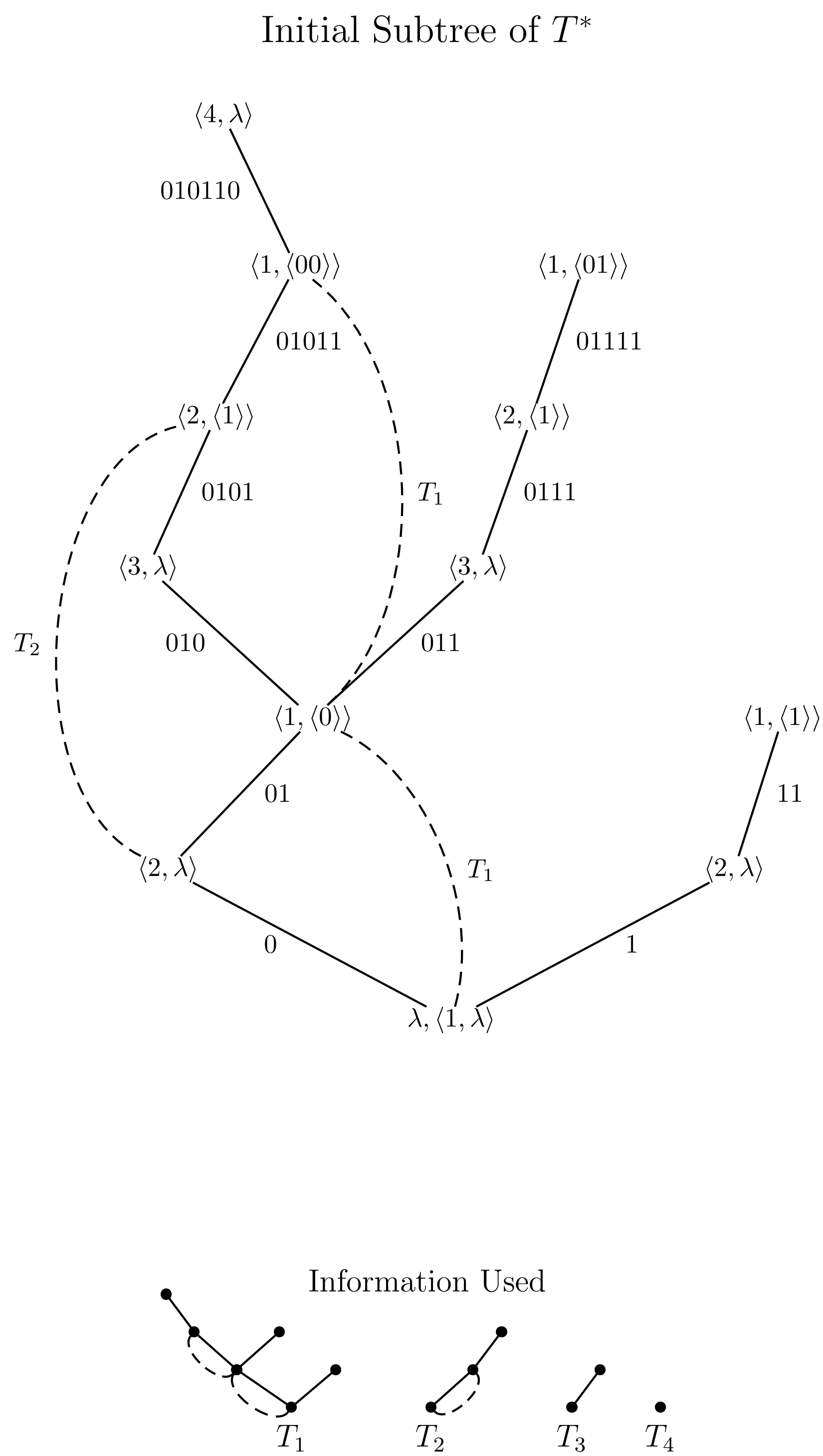


**Fig. 5.1:** Initial Subtree of $T^*$

# Chapter 6

# Holland's Embedding Theorem

The central object of study in this chapter is the following theorem:

**Holland's Embedding Theorem 2.** *Let $G$ be a lattice ordered group. Then there is an embedding of $G$ into the group of order-preserving permutations of some linear order.*

At face value, this theorem purports both the existence of a linear order and the group of order-preserving permutations of that linear order. For this to be non-trivial, the linear order must of course be infinite. Moreover, the permutation group is then a third-order object which we cannot define directly in $Z_2$. We carefully sidestep this obstacle by restating the theorem. Specifically, using the purported linear order $L$, we show that there is a uniform way of obtaining, for each $g \in G$, a specific function $f_g : L \to L$ which is in fact an order-preserving permutation, and verify all the desired properties of the embedding without explicitly forming the *range* of the embedding as a set.

**Holland's Embedding Theorem 3.** *If $G$ is an $\ell$-group, then there exists a linear order $L$ and a function $f(g,l) : G \times L \to L$ such that for each $g \in G$, the function $f(g,l)$, abbreviated $f_g$, is an order preserving bijection on $L$, and satisfies the properties*

- $\forall l \in L(f_e(l) = l)$.
- $[\forall l \in L(f_g(l) = f_h(l))] \leftrightarrow g = h$.
- $\forall g, h \in G, l \in L(f_{g \wedge h}(l) = \min\{f_g(l), f_h(l)\})$.
- $\forall g, h \in G, l \in L(f_{g \vee h}(l) = \max\{f_g(l), f_h(l)\})$.
- $\forall g, h \in G, l \in L(f_{gh}(l) = f_h(f_g(l))\}$.

The first two properties above indicate, respectively, that the group identity induces the identity permutation, and that each element induces a distinct permutation. The last three ensure that the embedding respects the $\ell$-group structure of $G$ – that is, that if one forms the meet, join, or group product of two elements, then one gets the same permutation as though one had taken the meet, join, or composition of the permutations induced by those elements individually.

### 6.1 Summary of Original Proof of Holland's Theorem

1. Fix a sequence of values $\{V_g\}$, one for each $g \neq e$.

2. Since values are prime, the induced order on each collection of right cosets $G/V_g$ is linear.

3. The collections of cosets $G/V_g$ may be ordered lexicographically to form a linear order $L$.

4. Each element of $G$ naturally induces an order-preserving permutation of $L$ by right multiplication.

5. The $\ell$-group structure of $G$ naturally embeds into the $\ell$-group structure of order-preserving permutations of $L$.

6. Proof is relatively constructive and can be done in $\mathsf{RCA}_0$ **except** for obtaining a sequence of values $V_g$ which, as we saw in Chapter 5, is equivalent to $\mathsf{ACA}_0$.

There are two qualities of values that are used in the proof, namely, that they are prime and that each element is excluded from some value – that is, there is no use of values' maximality except for proving that values are prime. This observation motivated the definition of excluding primes in Chapter 5 and led to a couple of questions, namely: *"Is the existence a sequence of excluding primes equivalent to something weaker than* $\mathsf{ACA}_0$*?"* and *"Can Holland's Theorem be proved using excluding primes instead of values?"*

The answer to the first question is "Yes, but so far only for abelian $\ell$-groups", as was shown in Chapter 5. We now address the second question.

## 6.2 Proof of Holland's Theorem using excluding primes

Let $G$ be an $\ell$-group. For $g \neq e$, let $P(g)$ denote a prime subgroup not containing $g$. Suppose we are given a set $K = \{\langle x, y\rangle : y \in P(x)\}$ coding a sequence of excluding primes. (If $G$ is abelian, then by Theorem 5.18, $K$ can be formed in $\mathsf{WKL}_0$.) By Theorem 3.7, $\mathsf{RCA}_0$ is sufficient to establish the induced orders on the sets of right cosets $G/P(g)$ for each nonidentity $g$. Thus, given $K$ we can form $\bar{K} = \{\langle x, y\rangle : y$ is the $\mathbb{N}$-least element of a right coset in $G/P(x)\}$.

Since $P(g)$ is prime for each $g$, each column of $\bar{K}$ (representing cosets $G/P(g)$) is linearly ordered under the induced order $<_{G/P(g)}$, by Theorem 5.3. Thus, we may totally order $\bar{K}$: $\langle a, b\rangle < \langle x, y\rangle$ iff $a <_{\mathbb{N}} x$ or $a = x$ and $b <_{G/P(x)} y$ in $\mathsf{RCA}_0$. The set $\bar{K}$ plays the role of the linear order $L$ in the statement of Holland's Theorem.

**Lemma 6.1.** ($\mathsf{RCA}_0$) *If $P$ is a prime subgroup of an $\ell$-group $G$, then an element $g \in G$ induces an order-preserving permutation $f_g$ of $G/P$, defined by $f_g(Px) = Pxg$.*

*Proof.* Since $P$ is prime, $G/P$ is totally ordered under the induced order. Let the induced order be represented by $\preceq$. Since $f_g(Pyg^{-1}) = Py$, it is clear that the map is surjective. Suppose $f_g(Px) = f_g(Py)$. Then $Pxg = Pyg$. It follows that $\exists p \in P(x = py)$, so $Px = Py$, and we have shown $f_g$ is injective. Now, we show it is order-preserving. Suppose $Px \preceq Py$. By the definition of the induced order, this means $\exists p \in P(x \leq py)$. Then $xg \leq pyg$, so $Pxg \preceq Pyg$.

□

**Lemma 6.2.** ($\mathsf{RCA}_0$) *Given an $\ell$-group $G$ and sequence of excluding primes $K$, there exists a function $f(g, \langle x, y\rangle) : G \times \bar{K} \to \bar{K}$ so that for all $g \in G$, $f(g, k)$ is an order-preserving permutation of $\bar{K}$.*

*Proof.* We define $f(g, \langle x, y\rangle)$ using right multiplication: $f(g, \langle x, y\rangle) = \langle x, z\rangle$, where $z$ is the least coset representative of $yg$ in $\bar{K}_x \cong G/P(x)$. By Lemma 6.1, this mapping is a bijection of each column $\bar{K}_x$ which preserves each induced order $<_{G/P(x)}$. Thus $f_g$ preserves the order on $\bar{K}$. □

**Lemma 6.3.** ($\mathsf{RCA}_0$) *The function $f(g, k)$ respects the $\ell$-group structure of $G$, and the only element which induces the identity permutation of $\bar{K}$ is the identity of $G$.*

*Proof.* We need to establish the following:

1. $\forall g, h \in G(f_g \circ f_h = f_{hg})$.

2. $\forall g \in G(f_g = id_{\bar{K}} \leftrightarrow g = e)$.

3. $\forall g, h \in G(f_{g \wedge h} = f_g \wedge f_h = min\{f_g, f_h\})$.

4. $\forall g, h \in G(f_{g \vee h} = f_g \vee f_h = max\{f_g, f_h\})$.

(1) Follows directly from the definition of $f(g, k)$ by right multiplication.

(2) It is clear that $f_e$ is the identity on $\bar{K}$. On the other hand, suppose $g \neq e$.

Then we have a column in $\bar{K}$ corresponding to $G/P(g)$. Since $g \notin P(g)$, $f_g$ permutes $\bar{K}_g$ nontrivially, so cannot be the identity on $\bar{K}$.

(3) By Theorem 3.8, for any convex subgroup $C$, $C(g \wedge h) = Cg \wedge Ch$. In the case that $C$ is prime, the induced order is linear so the meet is the minimum. Let $k = \langle x, y\rangle \in \bar{K}$. $f_{g\wedge h}(\langle x, y\rangle) = \langle x, y(g \wedge h)^*\rangle = \langle x, (yg \wedge yh)^*\rangle = \langle x, min_{G/P(x)}\{yg, yh\}^*\rangle = min_{\bar{K}}\{f_g(k), f_h(k)\}$. The asterisk $^*$ reminds us that technically these equalities use the least coset representative, e.g., $yg^*$ is the $\mathbb{N}$-least coset representative of $P(x)yg$.

(4) Similar to (3).

Note: the last two criteria feature a consequence of the standard lattice order on the group of automorphisms of a linear order as mentioned in Example 1.8. □

While we do not explicitly form the set of automorphisms of the linear order $\bar{K}$, we produce a function $f(g, k)$ which, practically speaking, provides an $\ell$-embedding of $G$ into $Aut(\bar{K})$. We have:

**Theorem 6.4.** ($\mathsf{RCA}_0$ *+ Existence of a sequence of excluding primes*) $\vdash$ *Holland's Theorem.*

By Theorem 5.18, we then have:

**Corollary 6.5.** $\mathsf{WKL}_0 \vdash$ *Holland's Embedding Theorem for abelian $\ell$-groups.*

This Corollary is certainly a successful result – the standard assumption of a sequence of values requires $\mathsf{ACA}_0$ even for abelian $\ell$-groups and, in that context, the strictly weaker assumption of a sequence of excluding primes suffices for the proof of Holland's Theorem. Without having a reversal, however, this raises another question: *"Might Holland's Theorem be proven by still weaker assumptions?"*

## 6.3 A Reversal

**Theorem 6.6.** ($\mathsf{RCA}_0$) *Let $G$ be an $\ell$-group. The following are equivalent:*

1. *Holland's Theorem*

2. *The existence of a sequence of prime subgroups $P(g)$ s.t. $\forall g \neq e(g \notin P(g))$.*

*Proof.* We have just seen that $2 \to 1$. We now show that $1 \to 2$. If $G$ is an $\ell$-group then by Holland's Theorem there is a linear order $L$ and a function $f(g,l) : L \to L$ satisfying all the properties mentioned in the revised statement of Holland's Embedding Theorem for $Z_2$. Suppose we are given such $G, L, f$. Define $F_l = \{g \in G : f(g,l) = l\}$, the set of $g$ which "fix" $l$. It is easy to check that for each $l$, $F_l$ is a prime subgroup of $G$.

- $e \in F_l$ because $f_e = id_L$.

- $x \in F_l \leftrightarrow x^{-1} \in F_l$.

- $x, y \in F_l \to xy \in F_l$, since $f_{xy}(l) = f_y(f_x(l)) = f_y(l) = l$.

- $x \in F_l \to x \vee e \in F_l$, since $f_{x\vee e}(l) = max\{f_x(l), f_e(l)\} = l$ (here we are using criterion 2.22).

- Suppose $e \leq x \leq g$ and $g \in F_l$. Then $f_e(l) \leq f_x(l) \leq f_g(l)$, so $l \leq f_x(l) \leq l$ and $x \in F_l$. Hence $F_l$ is a convex $\ell$-subgroup.

- Suppose $a \wedge b = e$. Then $f_{a\wedge b}(l) = f_e(l) = l$. But we also have $f_{a\wedge b}(l) = min\{f_a(l), f_b(l)\}$, so either $a \in F_l$ or $b \in F_l$, and therefore $F_l$ is a prime subgroup.

Furthermore, for each $g \neq e$, $f_g$ is nontrivial, so there is an $l$ so that $g \notin F_l$. Let $l$ be the $\mathbb{N}$-least such that $f(g, l) \neq l$. Then $g \notin F_l$.

This is an effective way of finding $l$ s.t. $g \notin F_l$. Since $F_l$ has a quantifier-free definition, given $L$ we can form in $\mathsf{RCA}_0$ a set $K = \{\langle x, y\rangle\}$ such that $K_x$ codes a prime subgroup not containing $g_x$ for $x \geq 1$. □

# Bibliography


[1] Marlow Anderson and Todd Feil. *Lattice-Ordered Groups: an introduction*. D. Reidel Publishing Company, Dordrecht, Holland, 1988.

[2] R.G. Downey and Stuart A. Kurtz. "Recursion Theory and Ordered Groups". *Annals of Pure and Applied Logic*, 32:137–151, 1986.

[3] K. Hatzikiriakou and S.G. Simpson. "$WKL_0$ and Orderings of Countable Abelian Groups". *Contemporary Mathematics*, 106:177–180.

[4] V.M. Kopytov and N.Ya. Medvedev. *The Theory of Lattice-Ordered Groups*, pages 1–55. Kluwer, Dordrecht, The Netherlands, 1994.

[5] Stephen G. Simpson. *Subsystems of Second Order Arithmetic*. Springer-Verlag, Berlin, Germany, 1999.

[6] D.R. Solomon. "Reverse Mathematics and Fully Ordered Groups". *Notre Dame Journal of Formal Logic*, 39(2):157–189, 1998.

[7] D.R. Solomon and Rod Downey. "Reverse Mathematics, Archimedean Classes, and Hahn's Theorem". In Stephen Simpson, editor, *Reverse Mathematics 2001*, pages 147,163. AK Peters, 2005.