

Rigid models of Presburger arithmetic

Emil Jeřábek*

Institute of Mathematics of the Czech Academy of Sciences

Žitná 25, 115 67 Praha 1, Czech Republic, email: jerabek@math.cas.cz

November 8, 2018

Abstract

We present a description of rigid models of Presburger arithmetic (i.e., \mathbb{Z} -groups). In particular, we show that Presburger arithmetic has rigid models of all infinite cardinalities up to the continuum, but no larger.

1 Introduction

Starting with classical Galois theory, it has been a common technique in algebra, logic, and other fields of mathematics to investigate structures by means of their automorphisms. This works well for structures with rich automorphism groups; in first-order logic, such models abound: for example, all structures have homogeneous (and highly saturated) elementary extensions, and by the Ehrenfeucht–Mostowski theorem, we can find structures with arbitrarily complex automorphism groups that in a sense control the structures.

On the opposite side of the spectrum, we have structures with only a few automorphisms, and in particular, *rigid* structures (i.e., having no automorphisms save the identity). Unlike models with many automorphisms, the existence of rigid models is a rather mysterious and whimsical property. On the one hand, many theories have no rigid models at all: this is true of theories as simple as the theory of the infinite set with no further structure, but we can construct arbitrarily complex such theories just by throwing in a new function symbol denoting a nontrivial automorphism. On the other hand, many theories of interest do have rigid models, even arbitrarily large.

For example, there are rigid linear orders (e.g., well orders), and consequently, rigid structures in any class that is “sufficiently universal” so that it can suitably represent all other relational structures (e.g., the theory of graphs). What is more surprising is that there are rigid dense linear orders or Boolean algebras of any uncountable cardinality (cf. [8]).

Interestingly, some theories have a limited amount of certain “trivial” rigid models, but also many other rigid models for non-trivial reasons. For instance, any completion of Peano arithmetic has a unique prime model where each element is definable; these models are clearly rigid. But in fact, Peano arithmetic has many more rigid models: every model of PA has a rigid elementary end-extension of the same cardinality (see Kossak and Schmerl [3, Thm. 3.3.14]). For an example involving a more tame theory: archimedean real-closed fields (or any archimedean ordered fields, for that matter) are rigid for trivial reasons, but as proved by Shelah [7], it also follows from

*The research leading to these results has received funding from the European Research Council under the European Union’s Seventh Framework Programme (FP7/2007–2013) / ERC grant agreement no. 339691. The Institute of Mathematics of the Czech Academy of Sciences is supported by RVO: 67985840.

certain combinatorial principles consistent with set theory that there are large, non-archimedean real-closed fields.

In this note, we will have a look at another tame theory: Presburger arithmetic, or equivalently, the theory of \mathbb{Z} -groups. Models of Presburger arithmetic with rich automorphism groups were studied by Llewellyn-Jones [4]. We will instead have a look at rigid models of the theory; in fact, we will present their complete description. We will see that there are, in a sense, both “trivial” and “non-trivial” rigid models, but the amount of non-triviality is limited, which manifests in a cardinality bound: Presburger arithmetic only has rigid models of sizes up to 2^{\aleph_0} . We also discuss the simpler case of “unordered Presburger arithmetic” $\text{Th}(\langle \mathbb{Z}, +, 1 \rangle)$, which turns out to have only “trivial” rigid models.

We note that the tamest theory of ordered abelian groups, namely of the divisible ones, has no rigid models (e.g., $x \mapsto 2x$ is always an automorphism). The theory of \mathbb{Z} -groups, which are just extensions of \mathbb{Z} by divisible ordered groups, can thus be thought of as the first nontrivial case in these parts.

2 Preliminaries

In this section, we will review the necessary background information about \mathbb{Z} -groups, and ordered groups in general. For references, basic properties of Presburger arithmetic and \mathbb{Z} -groups are discussed in Prestel and Delzell [6, §4.1], Marker [5, §3.1], and Llewellyn-Jones [4, §2–5]; in a more general set-up, model theory of modules and abelian groups is introduced in Hodges [2, §A.1–2].

In this paper, all groups are commutative, and all ordered structures are linearly ordered.

We assume familiarity with basic properties of ordered groups. We specifically mention that a group can be ordered iff it is torsion-free; more generally, if G is a torsion-free group, and $H \subseteq G$ an ordered subgroup, the order on H extends to an order on G . A subgroup H of an ordered group G is *convex* if $-y \leq x \leq y$ and $y \in H$ imply $x \in H$. If H is a convex subgroup of G , the order on G induces an order on G/H . Conversely, if H is a subgroup of G , \leq_H is an order on H , and $\leq_{G/H}$ an order on G/H , then there exists a unique order \leq_G on G that makes $\langle H, \leq_H \rangle$ a convex subgroup of $\langle G, \leq_G \rangle$, and that induces the order $\leq_{G/H}$ on G/H . Since \leq_G is explicitly defined by

$$0 \leq_G g \iff 0 <_{G/H} g + H \text{ or } (g \in H \text{ and } 0 \leq_H g),$$

we will call it the *lexicographic order* induced by \leq_H and $\leq_{G/H}$, even though strictly speaking we should reserve this term for the case where G is a direct sum of H and G/H .

Recall that a subgroup H of G is *pure* if for any integer $n > 0$ (w.l.o.g. prime), and any element $a \in H$, if $a = nb$ for some $b \in G$, then $a = nb$ for some $b \in H$. If G is torsion free, b is defined uniquely, hence we can restate the condition as follows: $b \in H$ whenever $nb \in H$ for some integer $n > 0$. In particular, if H is a subgroup of a torsion-free group G , then $\{a \in G : \exists n \in \mathbb{N}^{>0} na \in H\}$ is the least pure subgroup of G that includes H .

We will use the fact that divisible groups are injective: in particular, a divisible subgroup $H \subseteq G$ is always a direct summand of G , and more generally, if $K \subseteq G$ is a subgroup with trivial intersection with H , we can write $G = H \oplus K'$ for some $K' \supseteq K$.

Presburger arithmetic is officially the theory of the monoid $\langle \mathbb{N}, + \rangle$, but this structure is bi-interpretable with the more convenient ordered group $\langle \mathbb{Z}, +, \leq \rangle$, and we will work exclusively with the latter. (Bi-interpretation preserves the automorphism group, among many other things, hence this change is transparent for our purposes.)

Models of $\text{Th}(\langle \mathbb{Z}, +, \leq \rangle)$ are called *\mathbb{Z} -groups*, and they may be characterized as discretely ordered groups G such that G/\mathbb{Z} is divisible. Here, an ordered group is *discrete* if there exists a least positive element, conventionally denoted 1; the subgroup generated by 1, which is the least

nontrivial convex subgroup of G , gives a canonical embedding of the ordered group \mathbb{Z} in G , and G/\mathbb{Z} denotes the corresponding quotient group.

The theory of \mathbb{Z} -groups admits partial quantifier elimination: any formula $\varphi(\vec{x})$ is equivalent to a Boolean combination of linear inequalities $\sum_i n_i x_i \geq n$, where $n_i, n \in \mathbb{Z}$, and congruences $x_i \equiv k \pmod{m}$, where $0 \leq k < m \in \mathbb{N}$.

Let G be a \mathbb{Z} -group. For any integer $n > 0$, the *residue map* $x \mapsto (x \bmod n)$ is a unique group homomorphism $r_n: G \rightarrow \mathbb{Z}/n\mathbb{Z}$ such that $r_n(1) = 1$. These maps combine to a unique group homomorphism $r: G \rightarrow \hat{\mathbb{Z}}$ such that $r(1) = 1$, where

$$\hat{\mathbb{Z}} = \varprojlim_n \mathbb{Z}/n\mathbb{Z} = \prod_{p \text{ prime}} \mathbb{Z}_p$$

is the profinite completion of \mathbb{Z} , and \mathbb{Z}_p denotes the p -adic integers.

We will also consider models of the theory $\text{Th}(\langle \mathbb{Z}, +, 1 \rangle)$, which we will call *unordered \mathbb{Z} -groups*. If G is a torsion-free group with a distinguished element $1 \neq 0$, let \mathbb{Z} denote the subgroup of G generated by 1; then G is an unordered \mathbb{Z} -group iff G/\mathbb{Z} is divisible, and 1 is not p -divisible for any p (equivalently: \mathbb{Z} is a pure subgroup of G ; equivalently: G/\mathbb{Z} is torsion-free).

If $\langle G, +, \leq \rangle$ is a \mathbb{Z} -group with least positive element 1, then $\langle G, +, 1 \rangle$ is an unordered \mathbb{Z} -group, and the convexity of $\mathbb{Z} \subseteq G$ ensures that \leq induces an order \leq' on the quotient group G/\mathbb{Z} . Conversely, if $\langle G, +, 1 \rangle$ is an unordered \mathbb{Z} -group, the torsion-free group G/\mathbb{Z} can be ordered, and for any order on G/\mathbb{Z} , the corresponding lexicographic order on G that makes \mathbb{Z} convex gives G the structure of a \mathbb{Z} -group. That is, any unordered \mathbb{Z} -group expands to a \mathbb{Z} -group, and these expansions are in 1–1 correspondence with orders on G/\mathbb{Z} .

Quantifier elimination for unordered \mathbb{Z} -groups takes the form that every formula $\varphi(\vec{x})$ is equivalent to a Boolean combination of linear equalities $\sum_i n_i x_i = n$, and congruences $x_i \equiv k \pmod{m}$.

The residue maps $r_n: G \rightarrow \mathbb{Z}/n\mathbb{Z}$ and $r: G \rightarrow \hat{\mathbb{Z}}$ can also be defined for unordered \mathbb{Z} -groups just like before.

Quantifier elimination immediately implies a characterization of elementary substructures: if $\langle G, +, 1 \rangle$ is an unordered \mathbb{Z} -group, a substructure $H \subseteq G$ is elementary iff it is itself an unordered \mathbb{Z} -group iff it is a pure subgroup of G . We will call such substructures *\mathbb{Z} -subgroups of G* . Likewise, if $\langle G, +, \leq \rangle$ is a \mathbb{Z} -group, its elementary substructures are its \mathbb{Z} -subgroups, and these are exactly the substructures containing 1 that are \mathbb{Z} -groups.

3 Leibnizian models

What structures can be said to be rigid for trivial reasons? One case that immediately springs to mind are *pointwise definable models*: i.e., structures M such that every element $a \in M$ is definable in M without parameters. Clearly, a complete theory may have only one pointwise definable model up to isomorphism (if at all). In our case, the unique pointwise definable \mathbb{Z} -group is the standard model $\langle \mathbb{Z}, +, \leq \rangle$. We are, however, more interested in non-standard (i.e., non-archimedean) examples.

We may, in fact, loosen the condition a bit: in the obvious argument that pointwise definable structures are rigid, we do not really need that each element be isolated by a single formula from the rest of the model—it is enough if we can tell apart any pair of distinct elements. Thus, we are led to the class of *pointwise type-definable models*; following Enayat [1], we will call them more concisely *Leibnizian models*, as they are models that validate one reading of Leibniz’s law of *the identity of indiscernibles*.

Definition 3.1 A structure M is *Leibnizian* if for any $a \neq b \in M$, there exists a formula $\varphi(x)$ (without parameters) such that $M \models \varphi(a)$ and $M \not\models \varphi(b)$. In other words, distinct elements have

distinct parameter-free 1-types.

For example, a real-closed field is Leibnizian if and only if it is archimedean. (This follows easily from quantifier elimination: in a non-archimedean real-closed field, any two infinitely large elements have the same type.) Notice that a Leibnizian structure in a countable language must have cardinality at most 2^{\aleph_0} . An elementary substructure of a Leibnizian model is Leibnizian.

Observation 3.2 *Leibnizian structures are rigid.* □

Now, how do Leibnizian models of Presburger arithmetic look like? Curiously, the answer does not depend on availability of the order.

Theorem 3.3 *For any \mathbb{Z} -group $\langle G, +, \leq \rangle$, the following are equivalent:*

- (i) $\langle G, +, \leq \rangle$ is Leibnizian.
- (ii) The unordered \mathbb{Z} -group $\langle G, +, 1 \rangle$ is Leibnizian.
- (iii) The residue map $r: G \rightarrow \hat{\mathbb{Z}}$ is an embedding.

Proof:

(ii) \rightarrow (i) is obvious.

(iii) \rightarrow (ii): Let $a \neq b \in G$. By assumption $r(a) \neq r(b)$, hence $r_n(a) \neq r_n(b)$ for some $n > 0$; thus, the formula $x \equiv k \pmod{n}$ separates a from b , where $k = r_n(a)$.

(i) \rightarrow (iii): If the group homomorphism r is not injective, there is $a \neq 0$ such that $r(a) = 0$. We claim that $a \neq 2a$ have the same types, witnessing that G is not Leibnizian.

This is clear for formulas of the form $x \equiv k \pmod{m}$, as $a \equiv 0 \equiv 2a \pmod{m}$ by the choice of a . As for linear inequalities, they become somewhat degenerate in one variable: $nx \geq m$ is equivalent to $x \geq \lceil m/n \rceil$ if $n > 0$, and to $x \leq \lfloor m/n \rfloor$ if $n < 0$. Thus, all nonstandard elements of the same sign (such as a and $2a$) satisfy the same inequalities. □

Thus, any Leibnizian \mathbb{Z} -group embeds in $\hat{\mathbb{Z}}$; to see that there are many such groups, we only need to observe that $\hat{\mathbb{Z}}$ itself already works:

Lemma 3.4 $\hat{\mathbb{Z}}$ is an unordered \mathbb{Z} -group.

Proof: $\hat{\mathbb{Z}}$ is torsion-free as each \mathbb{Z}_p is a domain of characteristic 0. Notice that for any prime p , an element $a \in \hat{\mathbb{Z}}$ is p -divisible iff $a \equiv 0 \pmod{p}$. On the one hand, this ensures that 1 is not p -divisible; on the other hand, for any $a \in \hat{\mathbb{Z}}$, one of $a, a + 1, \dots, a + p - 1$ is. □

Corollary 3.5

- (i) Up to isomorphism, Leibnizian unordered \mathbb{Z} -groups are exactly the \mathbb{Z} -subgroups of $\hat{\mathbb{Z}}$.
- (ii) Up to isomorphism, Leibnizian \mathbb{Z} -groups are exactly the \mathbb{Z} -subgroups of $\langle \hat{\mathbb{Z}}, \leq \rangle$, where \leq is a lexicographic order induced by an order on $\hat{\mathbb{Z}}/\mathbb{Z}$.

In particular, for any $\aleph_0 \leq \kappa \leq 2^{\aleph_0}$, there are non-archimedean Leibnizian \mathbb{Z} -groups and unordered \mathbb{Z} -groups of cardinality κ . □

Notice that distinct \mathbb{Z} -subgroups of $\hat{\mathbb{Z}}$ are non-isomorphic, as they are the images of their own residue maps.

4 Non-Leibnizian models

As shown by the example of real-closed fields mentioned in Section 1, non-Leibnizian rigid models may be more elusive than Leibnizian models. Before we get to them, we first need to know a little about the general structure of non-Leibnizian models of Presburger arithmetic, or more precisely, of unordered \mathbb{Z} -groups.

Proposition 4.1 *Let G be an unordered \mathbb{Z} -group. We can write $G = D \oplus L$, where $D = \ker(r)$ is a divisible subgroup of G , and L is a Leibnizian \mathbb{Z} -subgroup of G .*

Proof: Put $D = \ker(r)$ as indicated. If $a \in D$ and $n \in \mathbb{N}^{>0}$, we have in particular $r_n(a) = 0$, hence $a = nb$ for some $b \in G$. Then $n r(b) = r(a) = 0$, hence $r(b) = 0$ as $\hat{\mathbb{Z}}$ is torsion-free. Thus, D is divisible.

Since $D \subseteq G$ is divisible, and $\mathbb{Z} \cap D = 0$, we have $G = D \oplus L$ for some subgroup $L \subseteq G$ such that $\mathbb{Z} \subseteq L$. Since direct summands are necessarily pure, this makes L a \mathbb{Z} -subgroup of G , and it is Leibnizian as $L \cap \ker(r) = 0$. \square

Remark 4.2 Thus, D (or its dimension as a \mathbb{Q} -linear space, if we want it numeric) can serve as a measure of non-Leibnizianity of G .

In a decomposition $G = D \oplus L$ with D divisible and L a Leibnizian \mathbb{Z} -subgroup, D is uniquely determined as $\ker(r)$, and also as the largest divisible subgroup of G . On the other hand, L is not unique as a subgroup of G , though it is of course unique up to isomorphism as $L \simeq G/D \simeq \text{im}(r)$.

We stress that the direct sum decomposition in Proposition 4.1 only works at the level of groups; if G is ordered, there is no telling how the orders of D and L interact.

With no order to complicate matters, Proposition 4.1 lends itself to an easy description of automorphisms. But first a bit of notation:

Definition 4.3 If G is an unordered \mathbb{Z} -group, and $H \subseteq G$ a subgroup, we will write H' for $H/(\mathbb{Z} \cap H)$. If moreover $f: H \rightarrow K$, $K \subseteq G$, is a homomorphism such that $f[\mathbb{Z} \cap H] \subseteq \mathbb{Z}$, let $f': H' \rightarrow K'$ be the induced homomorphism $f'(a + (\mathbb{Z} \cap H)) = f(a) + (\mathbb{Z} \cap K)$.

Lemma 4.4 *Let G be an unordered \mathbb{Z} -group, and D and L as in Proposition 4.1. Since $D \cap \mathbb{Z} = 0$, the natural quotient map is a group isomorphism of D to D' .*

Any automorphism f of G induces an automorphism f' of the group G' such that $f'(a) - a \in D'$ for all $a \in G'$. Such an f' can be represented in a unique way as

$$f'(d+l) = g'(d) + h'(l) + l \quad (d \in D', l \in L'),$$

where g is an automorphism of the group D , and $h: L \rightarrow D$ is a group homomorphism with $\mathbb{Z} \subseteq \ker(h)$.

Conversely, any f' as above is induced by a unique automorphism f of G , namely

$$f(d+l) = g(d) + h(l) + l \quad (d \in D, l \in L).$$

We stress that in the statement above, the language of the structure G includes the constant 1, hence it is fixed by all automorphism (whereas f' and g are just group automorphisms).

Proof: An automorphism f of G has to fix \mathbb{Z} pointwise, hence it indeed induces a group homomorphism $f': G' \rightarrow G'$, which is in fact an automorphism as f^{-1} induces its inverse. Moreover, f must preserve congruence formulas, i.e., the residue map $r: G \rightarrow \hat{\mathbb{Z}}$; thus, $f(a) - a \in D = \ker(r)$ for all $a \in G$, and likewise for f' .

Since $G' = D' \oplus L'$, f' can be uniquely represented as $f'(d + l) = g_1(d) + h_0(l)$, where $g_1: D' \rightarrow G'$, and $h_0: L' \rightarrow G'$. The condition $f'(a) - a \in D'$ further ensures that $g_1: D' \rightarrow D'$, and that $h_1(l) = h_0(l) - l$ is a homomorphism $h_1: L' \rightarrow D'$. If π denotes the natural isomorphism of D to D' , define $g: D \rightarrow D$ and $h: L \rightarrow D$ by $g(d) = \pi^{-1}(g_1(\pi(d)))$ and $h = \pi^{-1}(h_1(l + \mathbb{Z}))$. Then $g' = g_1$ and $h' = h_1$. Since f' is an automorphism, so is g .

The converse direction is likewise easy to check. \square

Remark 4.5 If G is a \mathbb{Z} -group, then $f: G \rightarrow G$ is an automorphism of $\langle G, +, \leq \rangle$ if and only if it is an automorphism of the unordered \mathbb{Z} -group $\langle G, +, 1 \rangle$, and it is order-preserving. The latter holds if and only if the induced group automorphism $f': G' \rightarrow G'$ is order-preserving, as $\mathbb{Z} \subseteq G$ is a convex subgroup fixed by f .

Corollary 4.6 *The only rigid unordered \mathbb{Z} -groups are the Leibnizian ones.*

Proof: If G is a non-Leibnizian unordered \mathbb{Z} -group, the divisible torsion-free group D in the decomposition $G = D \oplus L$ is nontrivial. But then $D \simeq D'$ has a nontrivial automorphism g , for instance $g(x) = 2x$. By Lemma 4.4, this lifts to a nontrivial automorphism of G , using, e.g., $h = 0$. \square

This was a rather anticlimactic answer. However, we will see that the situation for ordered \mathbb{Z} -groups is more interesting: some non-Leibnizian \mathbb{Z} -groups are rigid after all. The reason is that some of the automorphisms provided by Lemma 4.4 are not order-preserving. Even so, rigidity severely constraints D and L , as we will see in a short while.

We will work for a while with divisible subgroups of G' . Recall that a torsion-free divisible group is nothing else than a \mathbb{Q} -linear space, hence we may treat it with methods from linear algebra. Also notice that a convex subgroup of a divisible ordered group is divisible.

Lemma 4.7 *Let G be a rigid \mathbb{Z} -group, and $D = \ker(r)$. Then G' has no proper convex subgroup C such that $C + D' = G'$.*

Proof: Assume for contradiction that C is such a subgroup. By linear algebra, D' has a linear subspace D_0 such that $D' = D_0 \oplus (D' \cap C)$, which implies $G' = D_0 \oplus C$. Since C is convex, this is not just a direct sum of groups, but also a lexicographic product of the corresponding orders. Thus,

$$f'(d + c) = 2d + c \quad (d \in D_0, c \in C)$$

defines an order-preserving automorphism of G' , which is nontrivial as $D_0 \neq 0$. Since $f'(a) - a \in D'$ for all $a \in G'$, f' lifts to a (still order-preserving) automorphism of G by Lemma 4.4 and Remark 4.5. \square

Lemma 4.8 *Let G be a rigid \mathbb{Z} -group, and $D = \ker(r)$. If C is a convex subgroup of G' nontrivially intersecting D' , then $C + D' = G'$.*

Proof: If not, then $G'/(C + D')$ and $C \cap D'$ are nontrivial \mathbb{Q} -linear spaces, hence there exists a nonzero group homomorphism $f_0: G' \rightarrow C \cap D'$ that vanishes on $C + D'$. Define a group homomorphism $f': G' \rightarrow G'$ by $f'(x) = x + f_0(x)$. Clearly, $f'(x) - x \in D'$; since $f_0[D'] = 0$, this means f' has an inverse homomorphism $x - f_0(x)$, hence it is an automorphism of G' . It is also order-preserving: assume that $x \geq 0$. If $x > C$, then $f_0(x) \in C$ implies $f'(x) > C$, and a fortiori $f'(x) \geq 0$. If $x \in C$, then $f'(x) = x \geq 0$. Thus, f' lifts to a nontrivial automorphism of G using Lemma 4.4 and Remark 4.5. \square

Theorem 4.9 *Let G be a \mathbb{Z} -group, and write $G = D \oplus L$ with D divisible and L a Leibnizian \mathbb{Z} -subgroup of G as in Proposition 4.1. If G is rigid, the following conditions hold:*

- (i) D is archimedean.
- (ii) D is cofinal in G , or trivial.
- (iii) L is cofinal in G .

Proof:

(i) and (ii): We again identify D with $D' \subseteq G'$. If $a \in D'$ is positive, let C be the least convex subgroup of G' such that $a \in C$. Then $C + D' = G'$ by Lemma 4.8, hence $C = G'$ by Lemma 4.7. Thus, integer multiples of a are cofinal in G' (and in G after lifting back), including D' .

(iii): It suffices to show that L' is cofinal in G' . Let C be the least convex subgroup of G' that includes L' . Then $C + D' = G'$, hence $C = G'$ by Lemma 4.7. \square

Notice that in Theorem 4.9, L embeds in $\hat{\mathbb{Z}}$, and D , being archimedean, embeds in \mathbb{R} :

Corollary 4.10 *All rigid \mathbb{Z} -groups have cardinality at most 2^{\aleph_0} .* \square

Theorem 4.9 is not yet the end of the story, as the given conditions are only necessary, not sufficient. The missing condition is of a rather different (geometric) flavour, putting restrictions on how D and L sit next to each other inside G . On the one hand, it does not seem very illuminating, and on the other hand, it tends to be satisfied for typical examples that one comes up with in practice (as we will see shortly). But anyway, we formulate it here for completeness.

Theorem 4.11 *Let G be a \mathbb{Z} -group, written as $G = D \oplus L$ as in Proposition 4.1. Assume that D is archimedean, and D and L are both cofinal in G .*

Let C be the largest convex subgroup of G such that $C \cap D = 0$. By assumption, the ordered group G/C is archimedean, hence there is a homomorphism of ordered groups $\nu: G \rightarrow \mathbb{R}$ with $\ker(\nu) = C$, unique up to multiplication by a positive real constant. Put $G'' = \nu[G]$, $D'' = \nu[D]$, and $L'' = \nu[L]$.

The following are equivalent:

- (i) G is rigid.
- (ii) The only $\gamma \in \mathbb{R}^{>0}$ such that $\gamma D'' = D''$ and $(\gamma - 1)L'' \subseteq D''$ is $\gamma = 1$.

Proof: Notice that since $D \cap C = 0$, ν restricted to D is an isomorphism of D to D'' . Let $\nu_D^{-1}: D'' \rightarrow D$ denote its inverse.

(i) \rightarrow (ii): Let $\gamma > 0$ be such that $\gamma D'' = D''$ and $(\gamma - 1)L'' \subseteq D''$, which implies $(\gamma - 1)G'' \subseteq D''$. Define $f_\gamma: G \rightarrow G$ by

$$f_\gamma(x) = x + \nu_D^{-1}((\gamma - 1)\nu(x)).$$

Then f_γ is a group homomorphism, and $f_\gamma(x) - x \in D$ for each $x \in G$. We also have $\gamma^{-1}D'' = D''$ and $(\gamma^{-1} - 1)L'' = -\gamma^{-1}(\gamma - 1)L'' \subseteq -\gamma^{-1}D'' = D''$, hence we can apply the same construction to γ^{-1} ; a straightforward calculation shows that $f_{\gamma^{-1}}$ is the inverse of f_γ . Thus, f_γ is a group automorphism.

In order to see that it is order-preserving, let $x \geq 0$. Notice that $\nu(f_\gamma(x)) = \gamma\nu(x)$. Thus, if $x > C$, then $f_\gamma(x) > C$, and a fortiori $f_\gamma(x) \geq 0$. If $x \in C$, then $\nu(x) = 0$, hence $f_\gamma(x) = x \geq 0$ as well.

Thus, f_γ is an automorphism of G , hence it is the identity. But then $\gamma = 1$.

(ii) \rightarrow (i): Let f be an automorphism of G . By Lemma 4.4, f restricts to an automorphism of $D \simeq D'' \subseteq \mathbb{R}$. Pick any nonzero $a \in D$, and put $\gamma = \nu(f(a))/\nu(a)$. Since f is order-preserving,

and $\nu(a)\mathbb{Q}$ is dense in \mathbb{R} , we must have $\nu(f(x)) = \gamma\nu(x)$ for all $x \in D$; in particular, $\gamma D'' = D''$. More generally, the density of $\nu(a)\mathbb{Q}$ (along with convexity of C) implies that for any $x \in G$, $\nu(f(x)) = \gamma\nu(x)$, thus $(\gamma - 1)\nu(x) = \nu(f(x) - x)$. Since $f(x) - x \in D$ by Lemma 4.4, we obtain $(\gamma - 1)G'' \subseteq D''$. By (ii), $\gamma = 1$. Thus, $f(x) - x \in C \cap D = 0$ for all $x \in G$, i.e., f is the identity automorphism. \square

Remark 4.12 Recall that the subgroup L in the decomposition $G = D \oplus L$ is not uniquely determined. In the situation of Theorem 4.11, we may assume without loss of generality that L is chosen so that it includes the group C defined in the statement of the theorem, as $C \cap D = 0$. This makes the choice somewhat more canonical.

Let us mention some convenient sufficient conditions for Theorem 4.11 (ii).

Lemma 4.13 *Let D'' and L'' be nonzero \mathbb{Q} -subspaces of \mathbb{R} such that $D'' \cap L'' = 0$. Then condition (ii) from Theorem 4.11 is satisfied:*

- (i) *if $\dim_{\mathbb{Q}}(D'')$ is finite, or if $\dim_{\mathbb{Q}}(D'') < \dim_{\mathbb{Q}}(L'')$;*
- (ii) *if $L'' \not\subseteq D''^{-1}D''D''$, or more generally, if there is no $\alpha \in D''^{-1}D''$ such that $L'' \oplus D'' \subseteq \alpha D''$;*
- (iii) *if D'' is a subfield of \mathbb{R} , or more generally, if there exists a subfield $K \subseteq \mathbb{R}$ such that $D'' \subseteq K \subseteq L'' \oplus D''$.*

Proof:

(i): Either condition ensures $\dim_{\mathbb{Q}}(D'') < \dim_{\mathbb{Q}}(L'' \oplus D'')$. However, if $\gamma \neq 1$ is such that $(\gamma - 1)L'' \subseteq D'' = \gamma D''$, then $(\gamma - 1) \cdot -$ is a \mathbb{Q} -linear embedding of $L'' \oplus D''$ in D'' .

(ii): If $\gamma \neq 1$ is such that $\gamma D'' = D''$, then $\gamma = a/b$ for some nonzero $a, b \in D''$, thus $\alpha := (\gamma - 1)^{-1} = b/(a - b) \in D''^{-1}D''$, and $L'' \oplus D'' \subseteq \alpha D''$.

(iii): If $K \subsetneq L'' \oplus D''$, this follows from (ii), as $D''^{-1}D''D'' \subseteq K$. If $K = L'' \oplus D''$, and $\gamma \neq 1$ is such that $(\gamma - 1)L'' \subseteq D'' = \gamma D''$, then

$$(\gamma - 1)K \subseteq D'' \implies \gamma - 1 \in D'' \subseteq K \implies (\gamma - 1)K = K \implies L'' \subseteq K \subseteq D'',$$

which is a contradiction. \square

Example 4.14 In order to see that the condition is not automatic, let $L'' = (\pi - 1)^{-1}\mathbb{Q}$, and $D'' = \sum_{n \in \mathbb{Z}} \pi^n \mathbb{Q} = \mathbb{Q}[\pi, \pi^{-1}]$. Clearly, L'' and D'' are \mathbb{Q} -linear subspaces of \mathbb{R} , and $\gamma = \pi$ satisfies $\gamma D'' = D''$ and $(\gamma - 1)L'' \subseteq D''$. That $L'' \cap D'' = 0$ amounts to $\pi^n(\pi - 1)^{-1} \notin \mathbb{Q}[\pi]$ for any $n \in \mathbb{N}$, which follows from the transcendence of π .

While all these classification results are entertaining, we have yet to show the existence of a single non-Leibnizian rigid \mathbb{Z} -group. We are going to remedy this now. First, a simple example.

Example 4.15 Let D''_0 be a proper subfield of \mathbb{R} of cardinality 2^{\aleph_0} , and $L''_0 = \alpha D''_0$ for some $\alpha \in \mathbb{R} \setminus D''_0$, so that $D''_0 \cap L''_0 = 0$. By Lemma 4.13, D''_0 and L''_0 satisfy condition (ii) of Theorem 4.11. Since $\dim_{\mathbb{Q}}(L''_0) = \dim_{\mathbb{Q}}(\hat{\mathbb{Z}}/\mathbb{Z})$, we may fix a group isomorphism $\phi: \hat{\mathbb{Z}}/\mathbb{Z} \rightarrow L''_0$, and use it to lift the order from $L''_0 \subseteq \mathbb{R}$ to $\hat{\mathbb{Z}}/\mathbb{Z}$. This induces a lexicographic order on $\hat{\mathbb{Z}}$ which makes it a Leibnizian \mathbb{Z} -group. We put $G = D''_0 \oplus \hat{\mathbb{Z}}$ as a group, and order it lexicographically so that $G/\mathbb{Z} \simeq D''_0 \oplus (\hat{\mathbb{Z}}/\mathbb{Z}) \simeq D''_0 \oplus L''_0 \subseteq \mathbb{R}$ using ϕ . Then G is a non-Leibnizian rigid \mathbb{Z} -group by Theorem 4.11.

We can generalize Example 4.15 to show that essentially any choice of the various parameters consistent with Theorems 4.9 and 4.11 (with the convention from Remark 4.12) can be realized.

Proposition 4.16 *Let*

- L_0 be a \mathbb{Z} -subgroup of $\hat{\mathbb{Z}}$ other than \mathbb{Z} ;
- C_0 be a proper \mathbb{Z} -subgroup of L_0 ;
- \leq_C be an order on the group C_0/\mathbb{Z} ;
- D_0'' and L_0'' be trivially intersecting nonzero \mathbb{Q} -subspaces of \mathbb{R} such that condition (ii) from Theorem 4.11 holds (for example, using Lemma 4.13), and $\dim_{\mathbb{Q}}(L_0'') = \dim_{\mathbb{Q}}(L_0/C_0)$.

Then there exists a rigid \mathbb{Z} -group G with direct decomposition $G = D \oplus L$ as in Proposition 4.1, and largest convex subgroup C trivially intersecting D , such that

- as a group, L is isomorphic to L_0 ;
- C is isomorphic to C_0 , equipped with the lexicographic order induced by \leq_C ;
- the ordered groups D/C and L/C are isomorphic to D_0'' and L_0'' , respectively.

Proof: We endow C_0 with the lexicographic order induced by \leq_C , making C_0 a \mathbb{Z} -group. Since $\dim_{\mathbb{Q}}(L_0'') = \dim_{\mathbb{Q}}(L_0/C_0)$, we may fix a group isomorphism of L_0/C_0 to L_0'' , which allows us to transfer the archimedean order from L_0'' to L_0/C_0 . We endow L_0 with the lexicographic order induced by the already constructed orders on L_0/C_0 and C_0 , making L_0 a \mathbb{Z} -group with a convex subgroup C_0 .

Put $G = L_0 \oplus D_0''$ as a group. We equip $G/C_0 = (L_0/C_0) \oplus D_0''$ with the order induced by the fixed isomorphism to $L_0'' \oplus D_0'' \subseteq \mathbb{R}$, and G with the lexicographic order induced by the orders on G/C_0 and C_0 , making C_0 convex. (This is compatible with the previously constructed order on L_0 .)

By construction, G is a \mathbb{Z} -group satisfying the listed properties, and by Theorem 4.11, it is rigid. \square

Corollary 4.17 *For any infinite cardinals $\kappa, \lambda \leq 2^{\aleph_0}$, there are non-Leibnizian rigid \mathbb{Z} -groups G such that $|D| = \kappa$ and $|L| = \lambda$, where $G = D \oplus L$ are as in Proposition 4.1. \square*

Remark 4.18 If our goal were to describe the composition of non-Leibnizian rigid \mathbb{Z} -groups uniquely up to isomorphism, the data used in Proposition 4.16 would not be quite satisfactory: on the one hand, one such \mathbb{Z} -group can be described in several different ways because L_0'' is not uniquely determined; on the other hand, the given data do not describe a unique \mathbb{Z} -group as we left unspecified the isomorphism of L_0'' to L_0/C_0 .

We may improve the description as follows: we replace L_0'' with G_0'' (a \mathbb{Q} -subspace of \mathbb{R} such that $D_0'' \subsetneq G_0''$ and satisfying an appropriate version of Theorem 4.11 (ii)), and a group isomorphism of L_0/C_0 to G_0''/D_0'' . Then any such data describes a unique non-Leibnizian rigid \mathbb{Z} -group up to isomorphism, and conversely, any non-Leibnizian rigid \mathbb{Z} -group is described by almost unique data, the remaining ambiguity being that G_0'' (along with its subspace D_0'') is only defined up to multiplication by a real constant.

Acknowledgement

I wish to thank Ali Enayat, whose question prompted the investigation leading to this paper. I would also like to thank Roman Kossak for interesting comments, and the anonymous referee for suggestions that helped to improve the clarity of the paper.

References

- [1] Ali Enayat, *Leibnizian models of set theory*, Journal of Symbolic Logic 69 (2004), no. 3, pp. 775–789.
- [2] Wilfrid Hodges, *Model theory*, Encyclopedia of Mathematics and its Applications vol. 42, Cambridge University Press, 1993.
- [3] Roman Kossak and James H. Schmerl, *The structure of models of Peano arithmetic*, Oxford Logic Guides vol. 50, Oxford University Press, 2006.
- [4] David Llewellyn-Jones, *Presburger arithmetic and pseudo-recursive saturation*, Ph.D. thesis, University of Birmingham, 2001.
- [5] David Marker, *Model theory: An introduction*, Graduate Texts in Mathematics vol. 217, Springer, 2002.
- [6] Alexander Prestel and Charles N. Delzell, *Mathematical logic and model theory: A brief introduction*, Springer, 2011.
- [7] Saharon Shelah, *Models with second order properties IV. A general method and eliminating diamonds*, Annals of Pure and Applied Logic 25 (1983), no. 2, pp. 183–212.
- [8] Saharon Shelah, *Universal classes*, in: Classification Theory: Proceedings of the U.S.–Israel Workshop on Model Theory in Mathematical Logic Held in Chicago, Dec. 15–19, 1985 (J. T. Baldwin, ed.), Lecture Notes in Mathematics vol. 1292, Springer, 1987, pp. 264–418.