Tim Clausen

Dp-Minimal Profinite Groups

and

Planes in Sharply 2-Transitive Groups

2020

Mathematik

Dp-Minimal Profinite Groups and Planes in Sharply 2-Transitive Groups

Inaugural-Dissertation
zur Erlangung des Doktorgrades
Dr. rer. nat.
der Naturwissenschaften im Fachbereich
Mathematik und Informatik
der Mathematisch-Naturwissenschaftlichen Fakultät
der Westfälischen Wilhelms-Universität Münster

vorgelegt von
Tim Clausen
aus Dormagen
2020

Dekanin/Dekan:	Prof. Dr. Xiaoyi Jiang
Erste Gutachterin/Erster Gutachter:	Prof. Dr. Dr. Katrin Tent
Zweite Gutachterin/Zweiter Gutachter:	Prof. Dr. Pierre Simon
Tag der mündlichen Prüfung(en):	25.09.2020
Tag der Promotion:	25.09.2020

Abstract

In the first part of this thesis, we study dp-minimal infinite profinite groups that are equipped with a uniformly definable fundamental system of open subgroups. We show that these groups have an open subgroup A such that either A is a direct product of countably many copies of $\mathbb{F}_p$ for some prime p, or A is of the form $A \cong \prod_p \mathbb{Z}_p^{\alpha_p} \times A_p$ where $\alpha_p < \omega$ and A_p is a finite abelian p-group for each prime p. Moreover, we show that if A is of this form, then there is a fundamental system of open subgroups such that the expansion of A by this family of subgroups is dp-minimal. Our main ingredient is a quantifier elimination result for a class of valued abelian groups. We also apply it to $(\mathbb{Z}, +)$ and we show that if we expand $(\mathbb{Z}, +)$ by any chain of subgroups $(B_i)_{i<\omega}$, we obtain a dp-minimal structure. This structure is distal if and only if the size of the quotients B_i/B_{i+1} is bounded.

The second part of this thesis is about sharply 2-transitive groups of finite Morley rank. We show that sharply 2-transitive groups of Morley rank 6 are standard, i.e. of the form $\mathrm{AGL}_1(K)$ for an algebraically closed field K. Our main tool is the following: If the point-stabilizers of such a group contain involutions, then there is a point line geometry on the set of involutions. This geometry was already studied by Borovik and Nesin in [5]. We introduce the notion of a *generic projective plane*, a generalization of projective planes. Generic projective planes cannot exist in the point-line geometry on the set of involutions. We then show that a non-standard sharply 2-transitive group of Morley rank 6 would allow us to construct such a generic projective plane. This construction uses geometric arguments which are similar to those used by Frécon in [12] in the setting of bad groups.

Acknowledgments

Firstly, I would like to thank my supervisor, Katrin Tent, for her help and support during the last years and for giving me the opportunity to work on these exciting topics. I am especially thankful for many interesting and helpful conversations about groups of finite Morley rank and for all the helpful feedback.

I would like to thank the Logic group in Münster for a great time, for many enjoyable and interesting discussions, and for the opportunity to learn so much about mathematics. In particular, I would like to thank Martin Bays for his help, many useful comments, and proofreading.

I would like to thank Pierre Simon for interesting and useful discussions and valuable suggestions while I visited UC Berkeley.

Finally, I would like to thank Verena and my family for their love and support.

Contents

Part I.

Dp-minimal profinite groups

1. Introduction and overview

A profinite group G together with a fundamental system $\{K_i : i \in I\}$ of open subgroups can be viewed as a two-sorted structure (G, I) in the two-sorted language $\mathcal{L}_{\text{prof}}$. In these structures the fundamental system of open subgroups is definable. Since a fundamental system of open subgroups is a neighborhood basis at the identity, this implies that the topology on G is definable.

These structures have been studied by Macpherson and Tent in [31]. They mainly considered *full* profinite groups, i.e. profinite groups G where the family $\{K_i : i \in I\}$ consists of all open subgroups. Their main result states that a full profinite group (G, I) is NIP if and only if it is NTP_2 if and only if it is virtually a finite direct product of analytic pro-p groups.

Since analytic pro-p groups can be described as products of copies of $\mathbb{Z}_p$ with a twisted multiplication, profinite NIP groups are composed of "one-dimensional" profinite NIP groups. In the setting of full profinite groups the combinatorial structure of the lattice of open subgroups is visible in the model theoretic structure. This plays an important role in the classification.

Without the fullness assumption, only a portion of this lattice is visible. In general the family $\{K_i : i \in I\}$ could simply consist of a chain of open subgroups. In this more general setting, we will restrict ourselves to the "one-dimensional", i.e. dp-minimal case. A profinite group (G, I) is dp-minimal if it has NIP and is dp-minimal in the group sort. We prove the following classification result:

Theorem. *Let (G, I) be a dp-minimal profinite group. Then G has an open abelian subgroup A such that either A is a direct product of countably many copies of $\mathbb{F}_p$ for some prime p, or A is isomorphic to $\prod_p \mathbb{Z}_p^{\alpha_p} \times A_p$ where $\alpha_p < \omega$ and A_p is a finite abelian p-group for each prime p. Moreover, every abelian profinite group A of the above form admits a fundamental system of open subgroups such that the corresponding $\mathcal{L}_{prof}$-structure is dp-minimal.*

The main ingredient of this theorem is a quantifier elimination result which is also applicable in other settings. We apply it to this situation: Consider the structure $(\mathbb{Z}, +)$. If we expand it by the full lattice of subgroups, then the expanded structure interprets Peano Arithmetic and hence is not tame in any sense. However, if we only name a chain in this lattice, we obtain a tame structure. A chain of subgroups $\mathbb{Z} = B_0 > B_1 > \dots$ is the same as a valuation $v : \mathbb{Z} \to \omega \cup \{\infty\}$ defined by

$$v(a) = \max\{i : a \in B_i\}.$$

Theorem. *Let $(B_i)_{i<\omega}$ be a strictly descending chain of subgroups of $\mathbb{Z}$, $B_0 = \mathbb{Z}$, and let $v : \mathbb{Z} \to \omega \cup \{\infty\}$ be the valuation defined by*

$$v(x) = \max\{i : x \in B_i\}.$$

Then $(\mathbb{Z}, 0, 1, +, v)$ is dp-minimal. Moreover, $(\mathbb{Z}, 0, 1, +, v)$ is distal if and only if the size of the quotients B_i/B_{i+1} is bounded.

This stays true if we expand the value sort by unary predicates and monotone binary relations. There has been recent interest in dp-minimal expansions of $(\mathbb{Z}, +)$ (e.g. [2], [34], [1], and [36]). Alouf and d'Elbée showed in [2] that if p is a prime and v_p denotes the p-adic valuation, then $(\mathbb{Z}, 0, 1, +, v_p)$ is a minimal expansion of $(\mathbb{Z}, 0, 1, +)$ in the sense that there are no proper intermediate expansions. We show that this does not hold true for all valuations and we conjecture that the p-adic valuations are essentially the only examples with this property among valuations v such that $(\mathbb{Z}, 0, 1, +, v)$ is distal.

The proof of the classification theorem for dp-minimal profinite groups consists of three parts: We analyze the algebraic structure of dp-minimal profinite groups in Chapter 3. This will imply the first part of the theorem. It then remains to show that these groups appear as dp-minimal profinite groups. This is done in Chapter 4. The case where the group is given by an $\mathbb{F}_p$-vector space has already been done by Maalouf in [17]. We explain this result in Section 4.1. The remaining case is handled by a quantifier elimination result (see Section 4.2). This quantifier elimination result allows us to show that a certain class of profinite groups as $\mathcal{L}_{\text{prof}}$-structures is dp-minimal (Theorem 4.4.2) and we are able to characterize distality in this class (Theorem 4.4.5).

We will also apply the quantifier elimination result to valuations on $(\mathbb{Z}, +)$. This will be done in Chapter 5 where we discuss the second theorem and its consequences for the study of dp-minimal expansions of $(\mathbb{Z}, +, 0, 1)$. We also show that the p-adic valuations have a limit theory (Proposition 5.1.9) and we consider expansions of $(\mathbb{Z}, +, 0, 1)$ given by multiple valuations.

Chapter 6 contains a few results which are related to dp-minimal profinite groups. We show that our main result implies some structural consequences for uniformly definable families of finite index subgroups in dp-minimal groups (Proposition 6.1.4). Jarden and Lubotzky [14] showed that two elementarily equivalent profinite groups are isomorphic if one of them is finitely generated. This was generalized to strongly complete profinite groups by Helbig [13]. We will give an alternative proof for these results in Section 6.2. Finally, we prove a result about uniformly definable families of normal subgroups in NTP_2 groups (Proposition 6.3.2)[1]: If such a family is closed under finite intersections, then it must be defined by an NIP formula.

[1] Thanks to Pierre Simon for bringing this question to my attention.

2. Preliminaries

We assume that the reader is familiar with both profinite groups and model theory. We will give a quick overview about the notions and tools that are used to prove the main result.

2.1. Profinite groups

A topological group is *profinite* if it is the inverse limit of an inverse system of (discrete) finite groups. This condition is equivalent to the group being Hausdorff, compact, and totally disconnected. If G is a profinite group, then

$$G \cong \varprojlim G/N$$

where N ranges over all open normal subgroups.

The open subgroups generate the topology on G, i.e. every open set is a union of cosets of open subgroups. A *fundamental system of open subgroups* is a family $\mathcal{F}$ consisting of open subgroups which generate the topology on G. Equivalently, every open subgroup of G contains a subgroup in $\mathcal{F}$. If $\mathcal{P}$ is a property of groups, we will say that G is virtually $\mathcal{P}$ if G has an open subgroup H which satisfies $\mathcal{P}$.

We will use a number of results about the structure of abelian profinite groups. Recall that a profinite group is pro-p if it is the inverse limit of finite p-groups. A free abelian pro-p group is a direct product of copies of $\mathbb{Z}_p$.

Proposition 2.1.1 (Theorem 4.3.4 of [22])**.** *Let p be a prime.*

(a) If G is a torsion free pro-p abelian group, then G is a free abelian pro-p group.

(b) Let G be a finitely generated pro-p abelian group. Then the torsion subgroup $\mathrm{tor}(G)$ *is finite and*

$$G \cong F \oplus \mathrm{tor}(G)$$

where F is a free pro-p abelian group of finite rank.

Proposition 2.1.2 (Corollary 4.3.9 of [22])**.** *Let G be a torsion profinite abelian group. Then there is a finite set of primes π and a natural number e such that*

$$G \cong \prod_{p\in\pi}(\prod_{i=1}^{e}(\prod_{m(i,p)} C_{p^i}))$$

where each $m(i,p)$ is a cardinal and each C_{p^i} is the cyclic group of order p^i. In particular, G is of finite exponent.

Proposition 2.1.3 (Proposition 1.13 and Proposition 1.14 of [10])**.** *Let G be a pro-p group. Then G is (topologically) finitely generated if and only if the Frattini subgroup $\Phi(G) = \overline{G^p[G,G]}$ is open in G.*

Proposition 2.1.4. *Let A be an abelian profinite group. Then $nA \leq A$ is an open subgroup for all $n \geq 1$ if and only if*

$$A \cong \prod_p \mathbb{Z}_p^{\alpha_p} \times A_p$$

where $\alpha_p < \omega$ and A_p is a finite abelian p-group for each prime p.

Proof. An abelian profinite group is the direct product of its p-Sylow subgroups. Let P be a p-Sylow subgroup of A. If $pP \leq P$ has finite index, then P is finitely generated by Proposition 2.1.3. Then by Proposition 2.1.1 the p-Sylow subgroup P has the desired form. □

We will also need the following result by Zelmanov:

Theorem 2.1.5 (Theorem 2 of [38])**.** *Every infinite compact group has an infinite abelian subgroup.*

We will view profinite groups as two-sorted structures in the following language which was introduced in [31]:

Definition 2.1.6. $\mathcal{L}_{\text{prof}}$ is a two-sorted language containing the group sort $\mathcal{G}$ and the index sort $\mathcal{I}$. The language $\mathcal{L}_{\text{prof}}$ then consists of:

- the usual language of groups on $\mathcal{G}$,
- a binary relation $\leq$ on $\mathcal{I}$, and
- a binary relation $K \subseteq \mathcal{G} \times \mathcal{I}$.

Remark 2.1.7. A profinite group G together with a fundamental system of open subgroups $\{K_i : i \in I\}$ can be viewed as an $\mathcal{L}_{\text{prof}}$ structure (G, I) as follows:

- we set $i \leq j$ if and only if $K_i \supseteq K_j$, and
- the relation K is defined by $K(G, i) = K_i$ for all $i \in I$.

2.2. Model theoretic notions of complexity

We will mostly work in the context of an NIP theory. We use [28] as our main reference for this section.

2.2.1. The independence property

An important class of model theoretic theories is the class of NIP (or dependent) theories, i.e. the class of theories which cannot code the $\in$-relation on an infinite set. This notion was introduced by Shelah.

Definition 2.2.1. A formula $\varphi(x, y)$ has the *independence property (IP)* if there are sequences $(a_i)_{i<\omega}$ and $(b_J)_{J\subseteq\omega}$ such that

$$\models \varphi(a_i, b_J) \iff i \in J.$$

We say that $\varphi(x, y)$ has NIP if it does not have IP. This notion is symmetric in the sense that a formula $\varphi(x, y)$ has NIP if and only if the formula $\psi(y, x) \equiv \varphi(x, y)$ has NIP (see Lemma 2.5 of [28]).

We will make use of the following characterization of IP:

Lemma 2.2.2 (Lemma 2.7 of [28])**.** *A formula $\varphi(x, y)$ has IP if and only if there exists an indiscernible sequence $(a_i)_{i<\omega}$ and a tuple b such that*

$$\models \varphi(a_i, b) \iff i \text{ is odd}.$$

We call a theory NIP if all formulas have NIP.

Definition 2.2.3. A subset $X \subseteq M \models T$ is *externally definable* if there is a formula $\varphi(x, y)$, an elementary expansion M^* of M, and an element $b \in M^*$ such that $X = \varphi(M, b)$.

By a result of Shelah, naming all externally definable sets in an NIP structure preserves NIP:

Theorem 2.2.4 (Proposition 3.23 and Corollary 3.24 of [28])**.** *Let M be a model of an NIP theory and let M^{Sh} be the Shelah expansion, i.e. the expansion of M by all externally definable sets. Then M^{Sh} has quantifier elimination and is NIP.*

Theorem 2.2.5 (Baldwin-Saxl, Theorem 2.13 of [28])**.** *Let G be an NIP group and let $\{H_i : i \in I\}$ be a family of uniformly definable subgroups of G. Then there is a constant K such that for any finite subset $J \subseteq I$ there is $J_0 \subseteq J$ of size $|J_0| \leq K$ such that*

$$\bigcap\{H_i : i \in J\} = \bigcap\{H_i : i \in J_0\}.$$

As an easy consequence we obtain:

Corollary 2.2.6. *If (G, I) is an NIP profinite group, then $\{K_i : i \in I\}$ can only contain finitely many subgroups of any given finite index.*

By a result of Shelah, abelian subgroups of NIP groups have definable envelopes given by centralizers of definable sets:

Theorem 2.2.7 (Proposition 2.27 of [28])**.** *Let G be an NIP group and let X be a set of commuting elements. Then there is a formula $\varphi(x, y)$ and a parameter b (in some elementary extension G^*) such that* $\mathrm{Cen}(\mathrm{Cen}(\varphi(G^*, b)))$ *is an abelian (definable) subgroup of G^* and contains X.*

2.2.2. Dp-minimality

NIP theories admit a notion of dimension given by dp-rank:

Definition 2.2.8 (Definition 4.2 of [28])**.** Let p be a partial type over a set A, and let κ be a cardinal. We define

$$\text{dp-rk}(p, A) < \kappa$$

if and only if for every family $(I_t)_{t<\kappa}$ of mutually indiscernible sequences over A and $b \models p$, one of these sequences is indiscernible over Ab.

A theory is called *dp-minimal* if $\text{dp-rk}(x = x, \emptyset) = 1$ where x is a singleton. We call a multi-sorted theory with distinguished home-sort *dp-minimal* if it is NIP and it is dp-minimal in the home-sort, i.e. $\text{dp-rk}(x = x, \emptyset) = 1$ where x is a singleton in the home-sort.

Remark 2.2.9. As a consequence of the quantifier elimination in Theorem 2.2.4 the Shelah expansion of a dp-minimal structure is dp-minimal.

We will use the fact that definable subgroups in a dp-minimal group are always comparable in the following sense:

Lemma 2.2.10 (Claim in Lemma 4.31 of [28])**.** *Suppose G is dp-minimal and H_1 and H_2 are definable subgroups. Then $|H_1 : H_1 \cap H_2|$ or $|H_2 : H_1 \cap H_2|$ is finite.*

2.2.3. Distality

Distality is a notion introduced by Simon to describe the unstable part of an NIP theory. The general definition of distality is slightly more complicated than the definitions of NIP and dp-minimality (see Definition 2.1 in [27] or Chapter 9 in [28]). In case of a dp-minimal theory distality can be described as follows:

Proposition 2.2.11. *A dp-minimal theory T is distal if and only if there is no infinite non-constant totally indiscernible set of singletons.*

Proof. This characterization follows from Example 2.4 and Lemma 2.10 in [27]. □

By Exercise 9.12 of [28] distality is preserved under going to T^{eq}:

Proposition 2.2.12. *If T is distal, then so is T^{eq}.*

2.3. Quantifier elimination

Recall that a theory T has quantifier elimination if every formula is equivalent to a quantifier free formula modulo T. The proof of Theorem 3.2.5 in [32] gives the following useful criterion for quantifier elimination:

Proposition 2.3.1. *Let T be a theory and let $\varphi(x)$ be a formula. Then $\varphi(x)$ is equivalent to a quantifier free formula modulo T if and only if for all $\mathcal{M}_1, \mathcal{M}_2 \models T$ with common substructure $\mathcal{A}$ and all $a \in \mathcal{A}$ we have*

$$\mathcal{M}_1 \models \varphi(a) \implies \mathcal{M}_2 \models \varphi(a).$$

If T is a two-sorted theory and the only symbols that connect the two sorts are functions from one sort to the other, then it suffices to check quantifier elimination for very specific formulas:

Lemma 2.3.2. *Let T be a theory in a two-sorted language $\mathcal{L} = \mathcal{L}_0 \cup \mathcal{L}_1 \cup \{f_j : j \in J\}$ with sorts $\mathcal{S}_0$ and $\mathcal{S}_1$ where $\mathcal{L}_0$ is purely in the sort $\mathcal{S}_0$, $\mathcal{L}_1$ is purely in the sort $\mathcal{S}_1$, and each f_j is a function from sort $\mathcal{S}_0$ to sort $\mathcal{S}_1$. Suppose*

(a) every $\mathcal{L}_1$-formula is equivalent to a quantifier free formula modulo T and

(b) every formula of the form

$$\exists x \in \mathcal{S}_0 \bigwedge_{r \in R} \varphi_r(x, \bar{y}_r, \bar{z}_r)$$

is equivalent to a quantifier free formula modulo T where x is a singleton, $\bar{y}_r \subseteq \mathcal{S}_0$, $\bar{z}_r \subseteq \mathcal{S}_1$, and each φ_r is either a basic $\mathcal{L}_0$-formula or is of the form $f_j(t(x, \bar{y}_r)) = z$ where t is an $\mathcal{L}_0$ term and z is one of the variables in the tuple $\bar{z}_r$.

Then T eliminates quantifiers.

Proof. To show quantifier elimination it suffices to consider simple existential formulas. Consider a formula of the form

$$\exists \gamma \in \mathcal{S}_1 \bigwedge_{r \in R} \varphi_r(\gamma, \bar{y}_r, \bar{z}_r)$$

where γ is a singleton, $\bar{y}_r \subseteq \mathcal{S}_0$, $\bar{z}_r \subseteq \mathcal{S}_1$, and each φ_r is a basic formula. We may assume that γ appears non-trivially in each formula φ_r. Then each φ_r is a basic $\mathcal{L}_1$-formula where the variables $\bar{y}_r$ only appear as terms of the form

$$f(t(\bar{y}_r))$$

where f is a function symbol and t is an $\mathcal{L}_0$-term. Now the $\mathcal{S}_1$-quantifier can be eliminated by (a).

Now consider a formula of the form

$$\exists x \in \mathcal{S}_0 \bigwedge_{r \in R} \varphi_r(x, \bar{y}_r, \bar{z}_r)$$

where x is a singleton, $\bar{y}_r \subseteq \mathcal{S}_0$, $\bar{z}_r \subseteq \mathcal{S}_1$, and each φ_r is a basic formula.

Let $\tilde{R} \subseteq R$ be the set of all $r \in R$ such that φ_r is a basic $\mathcal{L}_1$-formula. If $r \in \tilde{R}$, then we may write φ_r as

$$\varphi_r \equiv \psi_r(\bar{f}_r(\bar{t}_r(x, \bar{y}_r)), \bar{z}_r)$$

where ψ_r is a basic $\mathcal{L}_1$-formula such that all variables of ψ_r are in $\mathcal{S}_1$. Then φ_r is equivalent to

$$\exists \bar{\xi} \in \mathcal{S}_1 : (\bar{\xi} = \bar{f}_r(\bar{t}_r(x, \bar{y}_r)) \wedge \psi_r(\bar{\xi}, \bar{z}_r)).$$

Now we may rewrite

$$\exists x \in \mathcal{S}_0 \bigwedge_{r \in R} \varphi_r(x, \bar{y}_r, \bar{z}_r)$$

as a formula of the form

$$\exists (\bar{\xi}_r)_{r \in \tilde{R}} \in \mathcal{S}_1 : ((\bigwedge_{r \in \tilde{R}} \psi_r(\bar{\xi}, \bar{z}_r)) \wedge (\exists x \in \mathcal{S}_0 \bigwedge_{r \in \tilde{R}} \bar{\xi}_r = \bar{f}_r(\bar{t}_r(x, \bar{y}_r)) \wedge \bigwedge_{r \in R \setminus \tilde{R}} \varphi_r(x, \bar{y}_r))).$$

We can now eliminate the $\mathcal{S}_0$-quantifier by (b) and then eliminate the $\mathcal{S}_1$-quantifiers as in the first step. $\square$

3. Algebraic properties of dp-minimal profinite groups

We view a profinite group G together with a fundamental system of open subgroups $\{K_i : i \in I\}$ as an $\mathcal{L}_{\mathrm{prof}}$-structure (G, I) (as in Remark 2.1.7). The aim of this chapter is to prove the first part of the main theorem: If (G, I) is a dp-minimal profinite group, then G has an open abelian subgroup A such that either A is a vector space over $\mathbb{F}_p$ for some prime p, or $A \cong \prod_p \mathbb{Z}_p^{\alpha_p} \times A_p$ where $\alpha_p < \omega$ and A_p is a finite abelian p-group for each prime p.

Simon showed in [26] that all dp-minimal groups are abelian-by-finite-exponent. An example of a dp-minimal group that is not abelian-by-finite was given by Simonetta in [29].

We will show that all dp-minimal profinite groups have an open abelian subgroup. We will then analyze the structure of this abelian profinite group. For dp-minimal profinite groups the fundamental system of open subgroups can always be replaced by a chain of open subgroups:

Lemma 3.0.1. *Let (G, I) be a dp-minimal profinite group. Then the subgroups*

$$H_i := \bigcap \{K_j : |G : K_j| \leq |G : K_i|\}$$

are uniformly definable open subgroups and hence the topology on G is generated by a definable chain of open subgroups.

Proof. The H_i are open subgroups by Corollary 2.2.6. By Lemma 2.2.10 and compactness we can find a constant K such that for all i, j $|K_i : K_i \cap K_j| < K$ or $|K_j : K_i \cap K_j| < K$. Given $i, j \in I$ we have

$$|G : K_i| \leq |G : K_j| \iff |K_i : K_i \cap K_j| \geq |K_j : K_i \cap K_j|.$$

Moreover, we have $|K_i : K_i \cap K_j| < K$ or $|K_j : K_i \cap K_j| < K$. Therefore this is a definable condition and hence the subgroups H_i are uniformly definable. ☐

In a dp-minimal profinite group we cannot find infinite definable subgroups of infinite index:

Lemma 3.0.2. *Let (G, I) be a dp-minimal profinite group. Let (G^*, I^*) be an elementary extension and let $H < G^*$ be a definable subgroup. If $G \cap H$ is infinite, then $|G^* : H|$ is finite.*

Proof. If $|K_i^* : K_i^* \cap H|$ is finite for some $i \in I$, then clearly $|G^* : H| < \infty$.

Now assume $|K_i^* : K_i^* \cap H|$ is infinite for all $i \in I$. We aim to show that $|H : K_i^* \cap H|$ must be unbounded: Since $G \cap H$ is infinite and $\bigcap_{i \in I} K_i = 1$, $|G \cap H : K_i \cap H|$ must be unbounded. Therefore $|H : K_i^* \cap H|$ must be unbounded. This contradicts Lemma 2.2.10. □

As a consequence of Zelmanov's theorem (Theorem 2.1.5) and the existence of definable envelopes for abelian subgroups (Theorem 2.2.7) we get that a dp-minimal profinite group must be virtually abelian:

Proposition 3.0.3. *Let (G, I) be a dp-minimal profinite group. Then G is virtually abelian.*

Proof. By Theorem 2.1.5 G has an infinite abelian subgroup A. By Theorem 2.2.7, we can find an elementary extension (G^*, I^*), a formula $\varphi(x, y)$, and a parameter $b \in (G^*, I^*)$ such that $\mathrm{Cen}(\mathrm{Cen}(\varphi(G^*, b)))$ is an abelian subgroup of G^* and contains A. Therefore $\mathrm{Cen}(\mathrm{Cen}(\varphi(G^*, b)))$ has finite index in G^* by Lemma 3.0.2. By elementarity there is some $b' \in (G, I)$ such that $\mathrm{Cen}(\mathrm{Cen}(\varphi(G, b')))$ is an abelian group and has finite index in G. Moreover, $\mathrm{Cen}(\mathrm{Cen}(\varphi(G, b')))$ is closed since it is a centralizer. Closed subgroups of finite index are open and therefore $\mathrm{Cen}(\mathrm{Cen}(\varphi(G, b')))$ is an open abelian subgroup of G. □

We are now able to prove the first part of the main theorem:

Theorem 3.0.4. *Let (A, I) be an abelian dp-minimal profinite group. Then either A is virtually a direct product of countably many copies of $\mathbb{F}_p$ for some prime p, or $A \cong \prod_p \mathbb{Z}_p^{\alpha_p} \times A_p$ where $\alpha_p < \omega$ and A_p is a finite abelian p-group for each prime p.*

Proof. Consider the closed subgroup $A[n] := \{x \in A : nx = 0\}$. Suppose there is a minimal n such that $A[n]$ is infinite. Then $A[n]$ has finite index in A (by Lemma 3.0.2) and hence is an open subgroup of A. Therefore we may assume $A = A[n]$. Now the minimality of n and Proposition 2.1.2 imply that n must be prime and therefore A is a direct product of copies of $\mathbb{F}_p$ (again by Proposition 2.1.2). Since A admits a countable fundamental system of open subgroups, this direct product must be a direct product of countably many copies of $\mathbb{F}_p$.

Now assume $A[n]$ is finite for all n. Then the closed subgroup nA must be open in A for all n (by Lemma 3.0.2). Now Proposition 2.1.4 implies the theorem. □

4. Valued abelian profinite groups

If A is an abelian group and $(A_i)_{i<\omega}$ is a strictly descending chain of subgroups such that $A_0 = A$ and $\bigcap_{i<\omega} A_i = \{0\}$, then we can define a valuation map $v : A \to \omega \cup \{\infty\}$ by setting

$$v(x) = \max\{i : x \in A_i\}.$$

We have $v(x) = \infty$ if and only if $x = 0$, and this valuation satisfies the inequality

$$v(x - y) \geq \min\{v(x), v(y)\}$$

where we have equality in case $v(x) \neq v(y)$.

The valued group (A, v) can be seen as a two-sorted structure consisting of the group A, the linear order $(\omega \cup \{\infty\}, \leq)$, and the valuation $v : A \to \omega \cup \{\infty\}$.

Our goal is to classify dp-minimal profinite groups up to finite index. We know by Lemma 3.0.1 that the fundamental system of open subgroups can be assumed to be a chain. Moreover, by Theorem 3.0.4 we only need to consider groups of the form

$$\prod_{i<\omega} \mathbb{F}_p \quad \text{or} \quad \prod_p \mathbb{Z}_p^{\alpha_p} \times A_p$$

where $\alpha_p < \omega$ and A_p is a finite abelian p-group for each prime p.

If A is such a group and $\{B_i : i < \omega\}$ is a fundamental system of open subgroups which is given by a strictly descending chain, then the above construction yields a definable valuation $v : A \to \omega \cup \{\infty\}$. Conversely, given such a valuation v, we can recover the fundamental system of open subgroups by setting

$$B_i = \{a \in A : v(a) \geq i\}.$$

Hence the valuation and the fundamental system are interdefinable.

We will show that if A is of the above form, then A admits a fundamental system given by a chain of open subgroups such that the expansion of A by the corresponding valuation (and hence the corresponding $\mathcal{L}_{\text{prof}}$-structure) is dp-minimal. If $A = \prod_{i<\omega} \mathbb{F}_p$, this follows from results by Maalouf in [17] and will be explained in Section 4.1.

Definition 4.0.1. (a) The subgroups $B_i = \{a \in A : v(a) \geq i\}$ are called the *v-balls of radius i*. We will also denote them by B_i^v to emphasize that they correspond to the valuation v.

(b) A valuation $v : A \to \omega \cup \{\infty\}$ is *good* if for all $i < \omega$ the subgroup B_i is of the form $B_i = nA$ for some positive integer n.

In case $A \cong \prod_p \mathbb{Z}_p^{\alpha_p} \times A_p$, we will prove a quantifier elimination result for good valuations. Note that by Proposition 2.1.4 each such group can be equipped with a good valuation such that $\{B_i : i < \omega\}$ is a fundamental system of open subgroups. We will show the following theorem:

Theorem 4.0.2. *Let $A \cong \prod_p \mathbb{Z}_p^{\alpha_p} \times A_p$ as above and let v be a good valuation. Then the structure $(A, +, v)$ is dp-minimal. Moreover, it is distal if and only if the size of the quotients B_i/B_{i+1} is bounded.*

This theorem will be proven in this chapter. If π is a set of primes, a natural number $n \geq 1$ is called a π-number if the prime decomposition of n only contains primes in π. An immediate consequence of the above theorem is the following:

Corollary 4.0.3. *Let $(\pi_i)_{i<\omega}$ be a sequence of finite non-empty disjoint sets of primes. For each $i < \omega$ fix a finite non-trivial abelian group A_i such that $|A_i|$ is a π_i-number. Set*

$$A = \prod_{i<\omega} A_i$$

and let v be the valuation defined by

$$v((a_i)_{i<\omega}) = \min\{i : a_i \neq 0\}.$$

Then $(A, +, v)$ is dp-minimal but not distal.

Proof. We have $B_k^v = (\prod_{i<k} |A_i|)A$. Hence v is a good valuation and the theorem applies. □

4.1. Valued vector spaces

Valued vector spaces have been studies by S. Kuhlmann and F.-V. Kuhlmann in [16] and by Maalouf in [17]. Set $A = \prod_{i<\omega} \mathbb{F}_p$ and let $v : A \to \omega \cup \{\infty\}$ be the valuation given by

$$v((x_i)_{i<\omega}) = \min\{i : x_i \neq 0\}.$$

It follows from results by Maalouf in [17] that this valued abelian profinite group is dp-minimal:

Proposition 4.1.1. *The valued abelian profinite group (A, v) is dp-minimal.*

Proof. Set $B = \bigoplus_{i<\omega} \mathbb{F}_p$ and let $w : B \to \omega \cup \{\infty\}$ be the valuation given by

$$w((x_i)_{i<\omega}) = \min\{i : x_i \neq 0\}.$$

By Proposition 4 of [17] the valued vector space (B, w) is C-minimal and hence dp-minimal (by Theorem A.7 of [28]).

Théorème 1 of [17] implies that (A, v) and (B, w) are elementarily equivalent. Hence (A, v) is dp-minimal. □

Remark 4.1.2. The last step of the previous proof also follows from results in Section 6.1. Let (B, w) be as in the proof of Proposition 4.1.1 and set

$$B_i = \{x \in B : w(x) \geq i\}.$$

Then $A \cong \varprojlim_{i<\omega} B/B_i$ and hence (A, v) is dp-minimal by Lemma 6.1.2.

4.2. A quantifier elimination result

We denote the set of primes by $\mathbb{P}$. For each prime $p \in \mathbb{P}$ we fix an integer $\alpha_p \geq 0$ and a finite p-group A_p. Let

$$Z \prec \prod_{p\in\mathbb{P}} \mathbb{Z}_p^{\alpha_p} \times A_p$$

be an abelian group that is (as a pure group) an elementary substructure. We will always assume Z to be infinite. We fix a set of constants $\{c_j : j < \omega\} \subseteq Z$ containing 0 such that the set is dense with respect to the profinite topology on Z and contains every torsion element. It follows from Proposition 2.1.4 that the set of constants is also dense with respect to the profinite topology on $\prod_{p\in\mathbb{P}} \mathbb{Z}_p^{\alpha_p} \times A_p$.

Definition 4.2.1. If π is a set of primes, we set

$$Z_\pi = Z \cap (\prod_{p\in\mathbb{P}} \mathbb{Z}_p^{\alpha_p} \times \prod_{p\in\mathbb{P}\setminus\pi} A_p) \quad \text{and} \quad A_\pi = Z \cap \prod_{p\in\pi} A_p.$$

Note that we have $Z = Z_\pi \times A_\pi$ for any set $\pi \subseteq \mathbb{P}$. The group A_π is the π-torsion part of Z and the group Z_π has no π-torsion.

Let v be a good valuation and set $I := \omega \cup \{+\infty, -\infty\}$. For each $l \geq 1$ we define a function $v^l : Z \to I$ by

$$v^l(a) = \begin{cases} +\infty & \text{iff } a = 0 \\ i & \text{iff } a \in lB_i \setminus lB_{i+1} \\ -\infty & \text{iff } a \notin lZ. \end{cases}$$

Note that if $a \in lZ$, then $v^l(a) = v(a/l)$. Now Z together with the valuation v may be viewed as a two-sorted structure with group sort $\mathcal{Z}$ and value sort $\mathcal{I}$ in the language $\mathcal{L}^- = \mathcal{L}_\mathcal{Z} \cup \mathcal{L}_v \cup \mathcal{L}_\mathcal{I}^-$ where

- $\mathcal{L}_\mathcal{Z} = \{+, -, c_j : j < \omega\}$ is the obvious language on Z,
- $\mathcal{L}_v = \{v^l : l \geq 1\}$ consists of symbols for the functions v^l, and
- $\mathcal{L}_\mathcal{I}^- = \{\leq, 0, +\infty, -\infty\}$ is the obvious language on I.

Since we consider the group Z and the constants c_j to be fixed, this structure only depends on the valuation and we denote it by (Z, v).

We define the following binary relations on I:

- $\mathrm{Ind}_k^{\pi,l}(i,j) \iff i \leq j$ and $|Z_\pi \cap lB_i : Z_\pi \cap lB_j| \geq k$,
- $\mathrm{Div}_{q^k}^{\pi,l}(i,j) \iff i \leq j$ and $q^{k\alpha_q}$ divides $|Z_\pi \cap lB_i : Z_\pi \cap lB_j|$,

where π is a finite set of primes, $q \in \pi$ is a prime, and $k \geq 0$. We set $\mathrm{Ind}_k^{\pi,l}(i,+\infty)$ and $\mathrm{Div}_{q^k}^{\pi,l}(i,+\infty)$ to be always true.

Observation 4.2.2. (a) If $q \in \pi$ then $q^{k\alpha_q}$ divides $|Z_\pi \cap lB_i : Z_\pi \cap lB_j|$ if and only if $(Z_\pi \cap lB_i)/(Z_\pi \cap lB_j)$ has an element of order q^k. In particular, the predicate $\mathrm{Div}_{q^k}^{\pi,l}$ is definable.

(b) In the standard model $\mathrm{Div}_{q^k}^{\pi,l}(i,j)$ is equivalent to the statement that q^k divides $|\mathbb{Z}_q \cap lB_i : \mathbb{Z}_q \cap lB_j|$. In that sense the expression $|\mathbb{Z}_q \cap lB_i : \mathbb{Z}_q \cap lB_j|$ makes sense even in non-standard models.

(c) We have $x \in nZ$ if and only if $v^n(x) \geq 0$. Hence the subgroups nZ are quantifier free 0-definable. Since the subgroups nZ generate the profinite topology on Z, this implies that the open subgroups Z_π are quantifier free 0-definable for finite subsets $\pi \subseteq \mathbb{P}$. Moreover, in that case A_π is also quantifier free 0-definable since it is a finite set of constants.

Let V be the set of good valuations on Z. We set $T_Z := \bigcap_{v \in V} \mathrm{Th}((Z,v))$ to be the common $\mathcal{L}^-$-Theory of structures (Z,v), $v \in V$. The following quantifier elimination result will be shown in the next sections:

Theorem 4.2.3. *Let $\mathcal{L}_\mathcal{I} \supseteq \mathcal{L}_\mathcal{I}^-$ be an expansion on the sort $\mathcal{I}$ and let $T \supseteq T_Z$ be an expansion of T_Z to the language $\mathcal{L} = \mathcal{L}_\mathcal{Z} \cup \mathcal{L}_v \cup \mathcal{L}_\mathcal{I}$. Suppose that:*

1. *The relations $\mathrm{Div}_{q^k}^{\pi,l}$ and $\mathrm{Ind}_k^{\pi,l}$ are quantifier free 0-definable modulo T.*
2. *The successor function on $\mathcal{I}$ is contained in $\mathcal{L}_\mathcal{I}$.*
3. *Every $\mathcal{L}_\mathcal{I}$-formula is equivalent to a quantifier free $\mathcal{L}$-formula modulo T.*

Then T eliminates quantifiers.

To prove the quantifier elimination result we will need to understand formulas that describe systems of linear congruences. Therefore we will need to understand linear congruences in models of the theory T.

4.2.1. Linear congruences in $\mathbb{Z}$

We will need generalizations of the following well-known fact:

Fact 4.2.4. A linear congruence $nx \equiv a \mod m$ in $\mathbb{Z}$ has a solution if and only if $d = \gcd(n, m)$ divides a. In that case it has exactly d many solutions modulo m. If s is a solution, then a complete system of solutions modulo m is given by

$$s + tm/d, \quad t = 0, \dots d - 1.$$

Observation 4.2.5. Fact 4.2.4 has two important consequences:

(a) If $nx \equiv a \mod m$ has a solution and $n = \gcd(n, m)$, then n divides a and hence a/n is a solution.

(b) If $nx \equiv a \mod m$ has a solution, then all solutions agree modulo m/d.

Part (a) will be important since in that case a solution will be determined by the constant a. Part (b) tells us that solutions of linear congruences can "collapse". We will need to understand this collapsing of solutions.

We now fix a group $\mathbb{A}$ of the form $\mathbb{A} = \prod_{p \in \mathbb{P}} \mathbb{Z}_p^{\alpha_p}$, $\alpha_p < \omega$. If n is a positive integer, let $n(p)$ be the unique integer such that $n = \prod p^{n(p)}$. Note that Fact 4.2.4 can be applied to $\mathbb{Z}_p$ because $\mathbb{Z}_p / k\mathbb{Z}_p = \mathbb{Z}/p^{k(p)}\mathbb{Z}$.

We consider linear congruences

$$nx \equiv a \mod m$$

in $\mathbb{A}$ where n and m are positive integers and $a \in \mathbb{A}$. Note that solving the above linear congruence is equivalent to solving it in each copy of $\mathbb{Z}_p$ in the product $\mathbb{A} = \prod_{p \in \mathbb{P}} \mathbb{Z}_p^{\alpha_p}$:

Lemma 4.2.6. *(a) Let $nx \equiv a \mod m$ be a linear congruence in $\mathbb{A}$. Write*

$$a = (a_{p,i})_{p \in \mathbb{P}, i < \alpha_p} \in \mathbb{A} = \prod_{p \in \mathbb{P}} \mathbb{Z}_p^{\alpha_p}.$$

The solutions for $nx \equiv a \mod m$ in $\mathbb{A}$ are exactly the tuples $s = (s_{p,i})_{p \in \mathbb{P}, i < \alpha_p}$ where each $s_{p,i}$ is a solution for $nx \equiv a_{p,i} \mod m$ in $\mathbb{Z}_p$.

(b) Set $d = \gcd(n, m)$. Then the linear congruence $nx \equiv a \mod m$ has a solution if and only if d divides a in $\mathbb{A}$ (i.e. $a \in d\mathbb{A}$). In that case it has exactly $\prod_{p|d} p^{\alpha_p d(p)}$ many solutions modulo m in $\mathbb{A}$.

We call a finite family of linear congruences (and negations of linear congruences) a *system of linear congruences*. Recall Bézout's identity:

Fact 4.2.7 (Bézout's identity)**.** If $a_1, \dots a_n$ are integers, then $\gcd(a_1, \dots a_n)$ is a $\mathbb{Z}$-linear combination of $a_1, \dots a_n$.

We will look at systems of linear congruences where the modulus is fixed:

Proposition 4.2.8. *Let $n_r x \equiv a_r \mod m$, $r \in R$, be a system $\mathcal{S}$ of linear congruences in $\mathbb{A}$ (where R is a finite set). Set $n = \gcd(n_r : r \in R)$ and $d = \gcd(n, m)$. By Bézout's identity we can find integers z_r such that $n = \sum_{r \in R} z_r n_r$. Put $a = \sum_{r \in R} z_r a_r$.*

(a) *If the system $\mathcal{S}$ has a common solution, the solutions of $\mathcal{S}$ are exactly the solutions of $nx \equiv a \mod m$.*

(b) *Set $k = n/d$ and $d_r = n_r/k$. Then the system $\mathcal{S}$ has a solution if and only if the system $\mathcal{T}$:*

$$d_r x \equiv a_r \mod m, \quad r \in R,$$

has a solution. Moreover, the systems $\mathcal{S}$ and $\mathcal{T}$ have the same number of solutions modulo m.

Proof. (a) It suffices to show this for each factor in the product $\mathbb{A} = \prod_{p \in \mathbb{P}} \mathbb{Z}_p^{\alpha_p}$. Hence we may assume $\mathbb{A} = \mathbb{Z}_p$ and $m = p^{m(p)}$. Clearly any common solution of the system $\mathcal{S}$ solves $nx \equiv a \mod m$.

Now suppose s is a solution of $\mathcal{S}$ (and hence a solution of $nx \equiv a \mod m$). Then by Fact 4.2.4 all solutions of $nx \equiv a \mod m$ are of the form $s + tm/d$ where $d = \gcd(n, m)$. Fix $r \in R$. Now d divides $d_r = \gcd(n_r, m)$, say $d_r = k_r d$. Therefore

$$s + tm/d = s + tk_r m/d_r$$

solves $n_r x \equiv a_r \mod m$ for all $t = 0, \dots d - 1$ (by Fact 4.2.4). Hence every solution of $nx \equiv a \mod m$ solves $\mathcal{S}$.

(b) We have $n = \gcd(n_r : r \in R) = \sum_{r \in R} z_r n_r$. If we divide by k, we get that $d = \gcd(d_r : r \in R) = \sum_{r \in R} z_r d_r$. We aim to show that $\mathcal{S}$ has a solution if and only if $\mathcal{T}$ has a solution. If s is a solution for $\mathcal{S}$, then ks solves $\mathcal{T}$. Now assume that $\mathcal{T}$ has a solution. Then by (a) the system $\mathcal{T}$ has the same solutions as the linear congruence

$$dx \equiv a \mod m.$$

Since we assume that $\mathcal{T}$ has a solution, this implies that $d = \gcd(d, m)$ divides a (by part (b) of Lemma 4.2.6). Then the linear congruence

$$nx \equiv a \mod m$$

also has solutions by part (b) of Lemma 4.2.6 since $d = \gcd(n, m)$ divides a. If s solves $nx \equiv a \mod m$, then ks solves $dx \equiv a \mod m$ and hence is a solution for $\mathcal{T}$. This implies that s solves $\mathcal{S}$. Hence $\mathcal{S}$ has a solution if and only if $\mathcal{T}$ has a solution. Moreover, if $\mathcal{S}$ and $\mathcal{T}$ have solutions, then by (a) the solutions of $\mathcal{S}$ are exactly the solutions of $nx \equiv a \mod m$ and the solutions of $\mathcal{T}$ are exactly the solutions of $dx \equiv a \mod m$. Hence they have the same number of solutions modulo m by part (b) of Lemma 4.2.6. □

We will now consider systems of linear congruences where we vary the modulus:

Lemma 4.2.9. *Let $nx \equiv a \mod p^m$ be a linear congruence in $\mathbb{Z}_p$. Set $d = \gcd(n, p^m)$ and suppose $l > 0$ divides p^m such that d divides p^m/l. Then*

$$nx \equiv a \mod p^m \quad \textit{and} \quad nx \equiv a \mod dl$$

have exactly d solutions modulo p^m respectively dl and all these solutions agree modulo l.

Proof. The assumption implies that dl divides p^m. Therefore

$$d = \gcd(n, p^m) = \gcd(n, dl).$$

By Fact 4.2.4 the congruences have a solution if and only if d divides a. In that case $nx \equiv a \mod p^m$ has exactly d solutions modulo p^m and the congruence $nx \equiv a \mod dl$ has exactly d solutions modulo dl. Moreover, by part (b) of Observation 4.2.5 all these solutions agree modulo l. □

Proposition 4.2.10. *Let $nx \equiv a \mod m$ be a linear congruence in $\mathbb{A}$. Set $d = \gcd(n, m)$. Suppose $l > 0$ divides m and is such that for all $p|d$ we have $p^{d(p)}|(m/l)$ or p does not divide (m/l). Set*

$$k = \prod_{p|d, p|(m/l)} p^{d(p)}.$$

Then the linear congruences

$$nx \equiv a \mod m \quad \text{and} \quad nx \equiv a \mod kl$$

have the same number of solutions modulo m respectively kl. Moreover, if X is the set of solutions modulo m of $nx \equiv a \mod m$, Y is the set of solutions modulo kl of $nx \equiv a \mod kl$, and X/l and Y/l are the images of X and Y in $\mathbb{A}/l\mathbb{A}$, then $X/l = Y/l$ and each element in X/l (resp. Y/l) has exactly $\prod_{p|d,p|(m/l)} p^{\alpha_p d(p)}$ many preimages in X (resp. Y).

Proof. By an application of Lemma 4.2.6 it suffices to show this in case $\mathbb{A} = \mathbb{Z}_p$. Hence we will assume $\mathbb{A} = \mathbb{Z}_p$.

If p does not divide d, then d is a unit in $\mathbb{Z}_p$ and hence each of the congruences has a unique solution in $\mathbb{Z}_p$.

Hence we may assume p divides d. If p does not divide m/l, then $m(p) = l(p)$ and $k(p) = 0$. Then $m\mathbb{Z}_p = kl\mathbb{Z}_p = l\mathbb{Z}_p$ and therefore the linear congruences

$$nx \equiv a \mod m, \qquad nx \equiv a \mod kl, \quad \text{and} \quad nx \equiv a \mod l$$

have the same solutions (in $\mathbb{Z}_p$). Since solutions modulo m (resp. modulo kl) are the same as solutions modulo l, each element of X/l (resp. Y/l) has a unique preimage in X (resp. Y).

Now assume p divides m/l. Then by assumption $p^{d(p)}$ divides m/l. In that case the result follows by Lemma 4.2.9. Note that each element in X/l (resp. Y/l) has exactly d preimages in X (resp. Y). □

4.2.2. Linear congruences in $\mathcal{Z}$

Fix $T \supset T_Z$ as in Theorem 4.2.3 (for a group $Z \prec \prod_{p\in\mathbb{P}} \mathbb{Z}_p^{\alpha_p} \times A_p$ as in the beginning of Section 4.2). We have $v^l(a) \geq i$ if and only if $a \in B_i^{v^l} = lB_i$. Therefore we will consider certain formulas as linear congruences:

$$v^l(nx - a) \geq i \iff nx \equiv a \mod lB_i,$$
$$v^l(nx - a) < i \iff nx \not\equiv a \mod lB_i.$$

Here x will be a variable and a will be a constant. The integer n will be part of the formula. In particular, it will always be a standard integer. Recall that for a subset $\pi \subseteq \mathbb{P}$ a natural number $n \geq 1$ is called a π-number if the prime decomposition of n only contains primes in π.

We will often work in the π-torsion free group Z_π defined in Definition 4.2.1. If we assume that π is finite, then by part (c) of Observation 4.2.2 the subgroup Z_π is quantifier free 0-definable. If $M \models T$ is any model, then we set $Z_\pi(M)$ to be the subgroup defined by the formula which defines Z_π in Z. The subgroup $A_\pi(M)$ is defined analogously.

If we use the notation in part (b) of Observation 4.2.2, then

$$\gcd(n, lB_i) := \gcd(n, \prod_{\{p:\alpha_p>0\}} |\mathbb{Z}_p : \mathbb{Z}_p \cap lB_i|)$$

is well-defined even if lB_i has infinite index because n is always a standard integer. Therefore the results in Section 4.2.1 can be formulated using the divisibility predicates and they will hold true for models of T.

Proposition 4.2.11. *Let M be a model of T and let $nx \equiv a \mod lB_i$ be a linear congruence in $Z(M)$. Let π be a finite set of primes such that n is a π-number and $a \in Z_\pi(M)$. Then the linear congruence has a solution in $Z_\pi(M)$ if and only if $d = \gcd(n, lB_i)$ divides a (i.e. $a \in dZ_\pi(M)$). In that case there are exactly $\prod p^{\alpha_p d(p)}$ many solutions modulo lB_i in $Z_\pi(M)$.*

Proof. This is essentially part (b) of Lemma 4.2.6. Since this is a first-order statement, it suffices to consider good valuations v on Z. Since the statement only affects the quotients Z/lB_i, we may assume that Z is of the form

$$Z = \prod_{p\in\mathbb{P}} \mathbb{Z}_p^{\alpha_p} \times A_p.$$

Put $\mathbb{A} = \prod_{p\in\mathbb{P}} \mathbb{Z}_p^{\alpha_p}$ and $H = \prod_{p\notin\pi} A_p$. Then

$$Z_\pi = \mathbb{A} \times H$$

and H has no π-torsion. Write $a = a_0 h$ for $a_0 \in \mathbb{A}$ and $h \in H$. Then we can apply Lemma 4.2.6 to the linear congruence

$$nx \equiv a_0 \mod lB_i$$

in $\mathbb{A}$. Note that the linear congruence

$$nx \equiv h \mod lB_i$$

has a unique solution modulo lB_i in H (namely h/n). This shows the proposition. □

Proposition 4.2.12. *Let M be a model of T and let $n_r x \equiv a_r \mod lB_i$, $r \in R$, be a system of linear congruences. Let π be a finite set of primes such that all n_r are π-numbers and all a_r are contained in $Z_\pi(M)$. Set $n = \gcd(n_r : r \in R)$ and $d = \gcd(n, lB_i)$. By Bézout's identity we can find integers z_r such that $n = \sum_{r\in R} z_r n_r$. Put $a = \sum_{r\in R} z_r a_r$.*

(a) If the system has a common solution in $Z_\pi(M)$, the solutions of the system in $Z_\pi(M)$ are exactly the solutions of $nx \equiv a \mod lB_i$ in $Z_\pi(M)$.

(b) Set $k = n/d$ and $d_r = n_r/k$. Then the system has a solution in $Z_\pi(M)$ if and only if the system

$$d_r x \equiv a_r \mod lB_i, \quad r \in R,$$

has a solution in $Z_\pi(M)$. Moreover, these systems have the same number of solutions modulo lB_i in $Z_\pi(M)$.

Proof. This follows from Proposition 4.2.8 by the same arguments that are used in Proposition 4.2.11. □

Proposition 4.2.13. *Let M be a model of T and let $nx \equiv a \mod lB_i$ be a linear congruence. Let π be a finite set of primes such that n is a π-number and $a \in Z_\pi(M)$. Set $d = \gcd(n, lB_i)$. Fix $u > 0$ and $j > i$ such that $ulB_j < lB_i$ is a subgroup and is such that for all $p|d$ we have that $p^{d(p)}$ divides $|\mathbb{Z}_p \cap lB_i : \mathbb{Z}_p \cap ulB_i|$ or p does not divide $|\mathbb{Z}_p \cap lB_i : \mathbb{Z}_p \cap ulB_i|$. Set*

$$k = \prod\{p^{d(p)} : p \text{ divides } d \text{ and } |\mathbb{Z}_p \cap lB_i : \mathbb{Z}_p \cap ulB_i|\}.$$

Then the linear congruences

$$nx \equiv a \mod lB_i \quad \text{and} \quad nx \equiv a \mod kulB_j$$

have the same number of solutions modulo lB_i respectively $kulB_j$ in $Z_\pi(M)$. Moreover, if X is the set of solutions modulo lB_i of $nx \equiv a \mod lB_i$, Y is the set of solutions modulo $kulB_j$ of $nx \equiv a \mod kulB_j$, and X/ulB_j and Y/ulB_j are the images of X and Y modulo ulB_j, then $X/ulB_j = Y/ulB_j$ and each element in X/ulB_j (resp. Y/ulB_j) has exactly $\prod_{p|d, p|(m/l)} p^{\alpha_p d(p)}$ many preimages in X (resp. Y).

Proof. This follows from Proposition 4.2.10 by the same arguments that are used in Proposition 4.2.11. □

The following lemma will often be useful:

Lemma 4.2.14. *Fix a model $M \models T$, let π be a finite set of primes, let $a \in Z_\pi(M)$, and let t be a π-number. Then the linear congruences*

$$nx \equiv a \mod lB_i \quad \text{and} \quad tnx \equiv ta \mod tlB_i$$

have the same solutions in $Z_\pi(M)$.

Proof. Multiplying by t is injective since $Z_\pi(M)$ does not have t-torsion. □

4.2.3. Systems of linear congruences in $\mathcal{Z}$

Fix T as in Theorem 4.2.3. Note that we assume that the successor function S (on $\mathcal{I}$) is contained in $\mathcal{L}_{\mathcal{I}}$.

Lemma 4.2.15. *Let M_1 and M_2 be models of T and let (A, J) be a common substructure. Let π be a finite set of primes and let $\mathcal{S}$:*

$$n_r x \equiv a_r \mod lB_i, \quad r \in R,$$

be a system of linear congruences where each n_r is a π-number, $a_r \in Z_\pi(A)$, and $i \in J$. Suppose there is a π-number t and a constant $b \in A$ such that t divides b and b/t solves $\mathcal{S}$ in $Z_\pi(M_1)$. Then b/t solves $\mathcal{S}$ in $Z_\pi(M_2)$.

Proof. We have t divides b if and only if $v^t(b) \geq 0$. This does not depend on the model. Moreover, b/t solves $n_r x \equiv a_r \mod lB_i$ if and only if $v^l(n_r(b/t) - a_r) \geq i$. By Lemma 4.2.14 we have

$$v^l(n_r(b/t) - a_r) = v^{tl}(n_r b - t a_r).$$

Therefore this value does not depend on the model. □

Lemma 4.2.16. *Let M_1 and M_2 be models of T and let (A, J) be a common substructure. Let π be a finite set of primes and let*

$$n_r x \equiv a_r \mod lB_i, \quad r \in R,$$

be a system of linear congruences where each n_r is a π-number, $a_r \in Z_\pi(A)$, and $i \in J$. Then the system has the same number of solutions modulo lB_i in $Z_\pi(M_1)$ and $Z_\pi(M_2)$.

Proof. Set $n := \gcd(n_r : r \in R)$, say $n = \sum_{r\in R} z_r n_r$ (by Bézout's identity), and put $a := \sum_{r\in R} z_r a_r$. Set $d := \gcd(n, \prod_{\{p:\alpha_p>0\}} |\mathbb{Z}_p : \mathbb{Z}_p \cap lB_i|)$, $k = n/d$, and $d_r = n_r/k$. Then by Proposition 4.2.12 (b) the system

$$n_r x \equiv a_r \mod lB_i,\ r \in R,$$

has the same number of solutions modulo lB_i in $Z_\pi(M_1)$ (resp. $Z_\pi(M_2)$) as the system

$$d_r x \equiv a_r \mod lB_i,\ r \in R.$$

We have $d = \gcd(d_r : r \in R) = \sum_{r\in R} z_r d_r$. By Proposition 4.2.12 (a) any solution of the system

$$d_r x \equiv a_r \mod lB_i,\ r \in R,$$

is a solution of $dx \equiv a \mod lB_i$. Now by Proposition 4.2.11 the linear congruence $dx \equiv a \mod lB_i$ has a solution if and only if d divides a. In that case a/d must be a solution and we can apply Lemma 4.2.15 to see that this must hold true in both models.

Hence $Z_\pi(M_1)$ contains a solution if and only if $Z_\pi(M_2)$ contains a solution. In that case the solutions are exactly the solutions of $nx \equiv a \mod lB_i$ and by Proposition 4.2.11 the number of solutions modulo lB_i does not depend on the model. □

Lemma 4.2.17. *Let M_1 and M_2 be models of T and let (A, J) be a common substructure. Let π be a finite set of primes and let $\mathcal{S}$ be a system*

$$n_r x \equiv a_r \mod lB_{i_r}, \quad r \in R,$$

of linear congruences where l and each n_r is a π-number, $a_r \in Z_\pi(A)$, $i_r \in J$. Suppose moreover, that the index $|B_{i_r} : B_{i_{r'}}|$ is a π-number whenever it is finite. Fix $r_{max} \in R$ such that $i_{r_{max}}$ is maximal. Then $\mathcal{S}$ has the same number of solutions modulo $lB_{i_{r_{max}}}$ in $Z_\pi(M_1)$ and $Z_\pi(M_2)$.

Proof. If $|lB_{i_r} : lB_{i_{r'}}|$ is finite, then there is a π-number t such that $lB_{i_r} = tlB_{i_{r'}}$. Lemma 4.2.14 allows us to replace the linear congruence

$$n_{r'} x \equiv a_{r'} \mod lB_{i_{r'}}$$

by the linear congruence

$$tn_{r'} x \equiv ta_{r'} \mod lB_{i_r}.$$

Hence we may assume that the index $|lB_{i_r} : lB_{i_{r'}}|$ is infinite whenever $i_r < i_{r'}$.

For $r_0 \in R$ set $R[r_0] = \{r \in R : i_r = i_{r_0}\}$ and consider the system $\mathcal{S}_{r_0}$:

$$n_r x \equiv a_r \mod lB_{i_r}, \quad r \in R[r_0].$$

By Lemma 4.2.16 the system $\mathcal{S}_{r_0}$ has the same number of solutions modulo $lB_{i_{r_0}}$ in $Z_\pi(M_1)$ and $Z_\pi(M_2)$. If $\mathcal{S}_{r_0}$ has no solution, then $\mathcal{S}$ has no solution and we are done. Hence assume that $\mathcal{S}_{r_0}$ has a solution (and hence has the same number of solutions in both models by Lemma 4.2.16).

Then by Proposition 4.2.12 we can replace the system $\mathcal{S}_{r_0}$ by a single linear congruence without changing the solutions.

Hence we may assume

$$i_r = i_{r'} \iff r = r'$$

for all $r, r' \in R$. Now we may write $R = \{r_0, \dots r_m\}$ such that $i_{r_0} > \cdots > i_{r_m}$. We prove the lemma by induction on m. The case $m = 0$ is done by Lemma 4.2.16. Hence we assume $m > 0$.

The system $\mathcal{S}$ has the form

$$\begin{aligned} n_{r_0} x &\equiv a_{r_0} \mod lB_{i_{r_0}}, \\ &\vdots \\ n_{r_m} x &\equiv a_{r_0} \mod lB_{i_{r_m}}. \end{aligned}$$

Now set $d := \gcd(n_{r_0}, \prod_{p \in \mathbb{P}, \alpha_p > 0} |\mathbb{Z}_p : \mathbb{Z}_p \cap lB_{i_{r_0}}|)$ and put

$$u = \prod_{p | d, \alpha_p > 0} \{|\mathbb{Z}_p \cap lB_{i_{r_1}} : \mathbb{Z}_p \cap lB_{i_{r_0}}| : |\mathbb{Z}_p \cap lB_{i_{r_1}} : \mathbb{Z}_p \cap lB_{i_{r_0}}| \text{ is finite}\}.$$

Set $k = \prod\{p^{d(p)} : \alpha_p > 0 \text{ and p does not divide } u\}$ and consider the system $\mathcal{S}'$:

$$\begin{aligned} n_{r_0}x &\equiv a_{r_0} \mod kulB_{i_{r_1}}, \\ un_{r_1}x &\equiv ua_{r_1} \mod ulB_{i_{r_1}}, \\ un_{r_2}x &\equiv ua_{r_2} \mod ulB_{i_{r_2}}, \\ &\vdots \\ un_{r_m}x &\equiv ua_{r_m} \mod ulB_{i_{r_m}}. \end{aligned}$$

By Proposition 4.2.13 the linear congruences $n_{r_0}x \equiv a_{r_0} \mod lB_{i_{r_0}}$ and $n_{r_0}x \equiv a_{r_0} \mod kulB_{i_{r_1}}$ have the same number of solutions modulo $lB_{i_{r_0}}$ respectively $kulB_{i_{r_1}}$ and the sets of solutions agree modulo $ulB_{i_{r_1}}$. The statement about the number of preimages in Proposition 4.2.13 implies that $\mathcal{S}$ and $\mathcal{S}'$ have the same number of solutions modulo $lB_{i_{r_0}}$ respectively $kulB_{i_{r_1}}$. By Lemma 4.2.14 we can rewrite $\mathcal{S}'$ as follows:

$$\begin{aligned} n_{r_0}x &\equiv a_{r_0} \mod kulB_{i_{r_1}}, \\ kun_{r_1}x &\equiv kua_{r_1} \mod kulB_{i_{r_1}}, \\ kun_{r_2}x &\equiv kua_{r_2} \mod kulB_{i_{r_2}}, \\ &\vdots \\ kun_{r_m}x &\equiv kua_{r_m} \mod kulB_{i_{r_m}}. \end{aligned}$$

By induction the system $\mathcal{S}'$ has the same number of solutions modulo $kulB_{i_{r_1}}$ in $Z_\pi(M_1)$ and $Z_\pi(M_2)$. Hence $\mathcal{S}$ has the same number of solutions modulo $lB_{i_{r_0}}$ in $Z_\pi(M_1)$ and $Z_\pi(M_2)$. □

To deal with the general case we will make use of the following:

Fact 4.2.18 (Inclusion-exclusion priciple)**.** Let $A_1, \dots A_n$ be finite sets. Then

$$|\bigcup_{i=1}^{n} A_i| = \sum_{\emptyset \neq J \subseteq \{1,\dots n\}} (-1)^{|J|+1} |\bigcap_{j \in J} A_j|.$$

Proposition 4.2.19. *Let M_1 and M_2 be models of T and let (A, J) be a common substructure. Let π be a finite set of primes and let $\mathcal{S}$ be a system*

$$\begin{aligned} n_r x &\equiv a_r \mod lB_{i_r}, \quad r \in R, \\ n_s x &\not\equiv a_s \mod lB_{i_s}, \quad s \in S, \end{aligned}$$

of linear congruences where each n_t is a π-number, $a_t \in Z_\pi(A)$, $i_t \in J$ for all $t \in R \cup S$. Assume there is $r_0 \in R$ such that i_{r_0} is maximal in $\{i_t : t \in R \cup S\}$. Suppose moreover, that the index $|B_{i_t} : B_{i_{t'}}|$ is a π-number whenever it is finite. Then $\mathcal{S}$ has the same number of solutions modulo $lB_{i_{r_0}}$ in $Z_\pi(M_1)$ and $Z_\pi(M_2)$.

Proof. For pairwise distinct $s_1, \dots s_n \in S$ let $A_{s_1,\dots s_n}$ be the set of solutions modulo $lB_{i_{r_0}}$ of the system $\mathcal{S}_{s_1,\dots s_n}$:

$$\begin{aligned} n_r x &\equiv a_r \mod lB_{i_r}, \quad r \in R, \\ n_{s_1} x &\equiv a_{s_1} \mod lB_{i_{s_1}}, \\ &\vdots \\ n_{s_n} x &\equiv a_{s_n} \mod lB_{i_{s_n}}. \end{aligned}$$

By Lemma 4.2.17 the system $\mathcal{S}_{s_1,\dots s_n}$ has the same number of solutions in $Z_\pi(M_1)$ and $Z_\pi(M_2)$. In particular, this holds true for the system $\mathcal{S}_\emptyset$:

$$n_r x \equiv a_r \mod lB_{i_r}, \quad r \in R.$$

Moreover, $\bigcup_{s \in S} A_s$ is exactly the set of solutions modulo $lB_{i_{r_0}}$ for $\mathcal{S}_\emptyset$ that do not solve $\mathcal{S}$.

Note that $A_{s_1} \cap \dots \cap A_{s_n} = A_{s_1,\dots s_n}$ and hence by an application of the inclusion-exclusion principle the number $|\bigcup_{s \in S} A_s|$ (which is finite since we only count solutions modulo $lB_{i_{r_0}}$) does not depend on the model.

Now the system $\mathcal{S}$ is solved by exactly

$$|A_\emptyset| - |\bigcup_{s \in S} A_s|$$

many solutions modulo $lB_{i_{r_0}}$ and this number does not depend on the model. □

4.2.4. Proof of quantifier elimination

Proof of Theorem 4.2.3. By Lemma 2.3.2 it suffices to show that every formula of the form

$$\psi(\bar{z}, \bar{i}) \equiv \exists x \in \mathcal{Z} \bigwedge_{r \in R} \varphi_r(x, \bar{z}, \bar{i})$$

is equivalent to a quantifier free formula modulo T where $\bar{z} \subseteq \mathcal{Z}$, $\bar{i} \subseteq \mathcal{I}$ and each φ_r is either a basic $\mathcal{L}_Z$-formula or is of the form

$$v^{l_r}(t_r(x, \bar{z})) = i_r$$

where t_r is an $\mathcal{L}_Z$-term and i_r is one variable in the tuple $\bar{i}$.

Write $R = R_0 \cup R_1 \cup R_2$ such that

$$\begin{aligned} \varphi_r(x, \bar{z}, \bar{i}) &\equiv n_r x - t_r(\bar{z}) = 0, \quad \text{for } r \in R_0, \\ \varphi_r(x, \bar{z}, \bar{i}) &\equiv n_r x - t_r(\bar{z}) \neq 0, \quad \text{for } r \in R_1, \quad \text{and} \\ \varphi_r(x, \bar{z}, \bar{i}) &\equiv v^{l_r}(n_r x - t_r(\bar{z})) = i_r, \quad \text{for } r \in R_2. \end{aligned}$$

Now let π be a finite set of primes such that n_r, l_r, and the cardinalities of all finite quotients $|lB_{i_r} : lB_{i_{r'}}|$ are π-numbers. Fix two models M_1, M_2 of T and let (A, J) be a common substructure, $\bar{a} \subseteq A, \bar{\eta} \subseteq J$. Set $a_r := t_r(\bar{a})$. We have $A = Z_\pi(A) \times A_\pi(A)$ (since A_π is a finite set of constants) and hence each a_r can be written as $a_r = a_r^\pi b_r^\pi$ with $a_r^\pi \in Z_\pi(A)$ and $b_r^\pi \in A_\pi(A)$. Now suppose the formula $\psi(\bar{a}, \bar{\eta})$ has a solution in M_1. By Proposition 2.3.1 it suffices to show that it has a solution in M_2.

If $r \in R_0$, then φ_r must be satisfied in $Z_\pi(M_1)$ and $A_\pi(M_1)$. If $r \in R_1$, then it suffices if φ_r is satisfied in $Z_\pi(M_1)$ or $A_\pi(M_1)$. If $r \in R_2$, then we have

$$\varphi_r(x, \bar{a}, \bar{\eta}) \equiv v^{l_r}(n_r x - a_r) = i_r.$$

This is satisfied if we have "=" in $Z_\pi(M_1)$ or $A_\pi(M_1)$ and "$\geq$" in the other subgroup. Hence there are subsets $R_1^\pi \subseteq R_1$ and $R_2^\pi \subseteq R_2$ such that the formulas

$$\begin{aligned}\psi^\pi \equiv \exists x \in Z_\pi & \bigwedge_{r \in R_0} n_r x - a_r^\pi = 0 \\ & \wedge \bigwedge_{r \in R_1^\pi} n_r x - a_r^\pi \neq 0 \\ & \wedge \bigwedge_{r \in R_2^\pi} v^{l_r}(n_r x - a_r^\pi) = i_r \\ & \wedge \bigwedge_{r \in R_2 \setminus R_2^\pi} v^{l_r}(n_r x - a_r^\pi) \geq i_r\end{aligned}$$

and

$$\begin{aligned}\overline{\psi^\pi} \equiv \exists x \in A_\pi & \bigwedge_{r \in R_0} n_r x - b_r^\pi = 0 \\ & \wedge \bigwedge_{r \in R_1 \setminus R_1^\pi} n_r x - b_r^\pi \neq 0 \\ & \wedge \bigwedge_{r \in R_2 \setminus R_2^\pi} v^{l_r}(n_r x - b_r^\pi) = i_r \\ & \wedge \bigwedge_{r \in R_2^\pi} v^{l_r}(n_r x - b_r^\pi) \geq i_r\end{aligned}$$

have a solution in $Z_\pi(M_1)$ respectively $A_\pi(M_1)$. Since A_π is a finite set of constants, this implies that $\overline{\psi^\pi}$ has a solution in $A_\pi(M_2)$. It remains to show that ψ^π has a solution in $Z_\pi(M_2)$.

If $R_2 = \emptyset$, then we are done since the formulas $x \in nZ$ are quantifier free 0-definable and hence the result follows from the usual quantifier elimination for abelian groups. Therefore we assume $R_2 \neq \emptyset$.

If $R_0 \neq \emptyset$, say $r_0 \in R_0$, then $a_{r_0}^\pi / n_{r_0}$ is the solution of ψ^π in $Z_\pi(M_1)$. Lemma 4.2.15 implies that $a_{r_0}^\pi / n_{r_0}$ also solves ψ^π in $Z_\pi(M_2)$. Hence we may assume $R_0 = \emptyset$.

If $i_r = +\infty$ for some r, then we have

$$v^{l_r}(n_r x - a_r^\pi) \geq i_r \iff n_r x - a_r^\pi = 0.$$

Hence we may assume $i_r < +\infty$ for all $r \in R_2$.

Given $l' \geq 1$ there is a finite set of constants $C_{l'}$ in the language such that the formula $v^{l'}(t(x,\bar{z})) = -\infty$ is equivalent to

$$\bigvee_{c \in C_{l'}} v^{l'}(t(x,\bar{z}) - c) \geq 0.$$

Thus we may also assume $i_r > -\infty$ for all $r \in R_2$.

Note that each formula of the form $n_r x - a_r^\pi \neq 0$ excludes only a single solution. Since we assume $R_2 \neq \emptyset$ and all formulas of the form

$$v^{l_r}(n_r x - a_r^\pi) = i_r \text{ or } v^{l_r}(n_r x - a_r^\pi) \geq i_r$$

are solved by cosets of $l_r B_{i_r+1}$, we may moreover assume $R_1 = \emptyset$.

By Lemma 4.2.14 we have $v^{l_r}(n_r x - a_r^\pi) = v^{ml_r}(mn_r x - ma_r^\pi)$ for all π-numbers m. Thus we may use Lemma 4.2.14 to replace each $l_{r'}$ by $l := \operatorname{lcm}(l_r : r \in R_2)$.

We consider formulas as linear congruences:

$$\begin{aligned} v^l(n_r x - a_r^\pi) = i_r &\iff (n_r x - a_r^\pi \equiv 0 \mod lB_{i_r} \quad \wedge \quad n_r x - a_r^\pi \not\equiv 0 \mod lB_{i_r+1}), \\ v^l(n_r x - a_r^\pi) \geq i_r &\iff n_r x - a_r^\pi \equiv 0 \mod lB_{i_r}. \end{aligned}$$

Hence it suffices to show that the system of linear congruences

$$\begin{aligned} n_r x - a_r^\pi &\equiv 0 \mod lB_{i_r}, \quad r \in R_2, \\ n_r x - a_r^\pi &\not\equiv 0 \mod lB_{i_r+1}, \quad r \in R_2^\pi, \end{aligned}$$

has a solution in $Z_\pi(M_2)$. After slightly adjusting the system (by using Lemma 4.2.14) and renaming, we get a system

$$\begin{aligned} n_s x - b_s &\equiv 0 \mod lB_{i_s}, \quad s \in S, \\ n_t x - b_t &\not\equiv 0 \mod lB_{i_t}, \quad t \in T, \end{aligned}$$

where $S \neq \emptyset$ and every index $|B_{i_r} : B_{i_{r'}}|, r, r' \in S \cup T$ is infinite or trivial. If there is an element $s \in S$ such that i_s is maximal in $\{i_r : r \in S \cup T\}$, then we are done by Proposition 4.2.19. Hence suppose there is $t_0 \in T$ such that $i_{t_0} > i_s$ for all $s \in S$. Then $|B_{i_s} : B_{i_{t_0}}|$ is infinite for all $s \in S$. In particular, the congruence

$$n_{t_0} x - b_{t_0} \not\equiv 0 \mod lB_{i_{t_0}}$$

can be ignored, since each lB_{i_s}-class consists of infinitely many lB_{t_0} classes. Hence we removed one linear congruence from the system. After iterating this, we can find $s \in S$ such that i_s is maximal. □

4.3. The monotone hull

Theorem 4.2.3 gives quantifier elimination up to a suitable language on $\mathcal{I}$. The following gives a tame expansion of $\mathcal{L}_{\mathcal{I}}^{-}$ which allows us to analyze the definable sets.

A binary relation R on a linear ordering is called *monotone* if and only if it satisfies

$$x' \leq xRy \leq y' \quad \text{implies} \quad x'Ry'.$$

The following result by Simon states that expanding a linear ordering by monotone binary relations is tame:

Proposition 4.3.1 (Proposition 4.1 and Proposition 4.2 of [26])**.** *Let $(I, \leq, R_\alpha, C_\beta)_{\alpha,\beta}$ be a linear order equipped with monotone binary relations and unary predicates such that every $\emptyset$-definable monotone binary relation is given by one of the R_α and every $\emptyset$-definable unary predicate is given by one of the C_β. Then $(I, \leq, R_\alpha, C_\beta)_{\alpha,\beta}$ has quantifier elimination and is dp-minimal.*

Fix a theory T_Z as in the quantifier elimination statement and let $M \models T_Z$ be a model. Note that the definable relations $\leq$, $\mathrm{Div}_{q^k}^{\pi,l}$, and $\mathrm{Ind}_k^{\pi,l}$ are monotone.

Definition 4.3.2. Let S be a set of unary predicates and monotone binary relations on the value set of M.

(a) We define $\mathcal{L}_{\mathcal{I},\mathrm{mon}}^{S}$ to be the monotone hull of

$$\mathcal{L}_{\mathcal{I}}^{S} := \mathcal{L}_{\mathcal{I}}^{-} \cup \{\mathrm{Div}_{q^k}^{\pi,l}, \mathrm{Ind}_k^{\pi,l}\}_{q,\pi,l,k} \cup S,$$

i.e. the expansion of $\mathcal{L}_{\mathcal{I}}^{S}$ by all 0-definable (in $\mathcal{L}_{\mathcal{I}}^{S}$) unary relations and all 0-definable monotone binary relations on the value sort.

(b) Set $\mathcal{L}_{\mathrm{mon}}^{S} = \mathcal{L}_{\mathcal{Z}} \cup \mathcal{L}_v \cup \mathcal{L}_{\mathcal{I},\mathrm{mon}}^{S}$ and define $\mathcal{L}_{\mathrm{mon}} = \mathcal{L}_{\mathrm{mon}}^{\emptyset}$.

Note that $\mathcal{L}_{\mathrm{mon}} \supseteq \mathcal{L}^{-}$ is an expansion by definitions.

Proposition 4.3.3. *Let S be as in Definition 4.3.2. Then* $\mathrm{Th}(M)$ *admits quantifier elimination in the language $\mathcal{L}_{\mathrm{mon}}^{S}$.*

Proof. The successor function and its inverse are 0-definable. If $R \in \mathcal{L}_{\mathcal{I},\mathrm{mon}}^{S}$ is a monotone binary relation, then so is $R_{m,n}(x,y) \iff R(x+m, y+n)$ for all $m, n \in \mathbb{Z}$. The same holds true for 0-definable unary predicates. Therefore adding the successor function to the language does not add any new definable sets in $\mathcal{I}$. Hence Theorem 4.2.3 and Proposition 4.3.1 imply quantifier elimination in $\mathcal{L}_{\mathrm{mon}}^{S}$. □

4.4. Dp-minimality and distality

Let T be a complete $\mathcal{L}_{\mathrm{mon}}^{S}$-theory as in Proposition 4.3.3.

Lemma 4.4.1. *Let $(Z, I, v) \models T$ be a sufficiently saturated model and let $(a_j)_{j \in J_1}$ and $(b_j)_{j \in J_2}$ be mutually indiscernible sequences in the group sort. Let $\gamma \in I$ be a singleton. Then one of the sequences is indiscernible over γ.*

Proof. We may assume that both sequences are indexed by a dense linear order. Suppose $(a_j)_{j \in J_1}$ is not indiscernible over γ. By the quantifier elimination result this must be witnessed by a formula of the form

$$R(v^l(t(\bar{x})), \gamma)$$

where t is an $\mathcal{L}_{\mathcal{Z}}$-term, R is a monotone binary relation on I, and $l \geq 1$. Hence we can find tuples $\bar{j}_0, \bar{j}_1 \subseteq J_1$ of the same order type such that

$$\models R(v^l(t(\overline{a}_{\overline{j_0}})), c) \quad \text{and} \quad \not\models R(v^l(t(\overline{a}_{\overline{j_1}})), c)$$

where $\overline{a}_{\overline{j_i}} = (a_j)_{j \in \overline{j_i}}$ is the tuple corresponding to $\overline{j_i} \subseteq J_1$.

After replacing $\bar{j}_0$ or $\bar{j}_1$ if necessary, we may assume that $\bar{j}_0$ and $\bar{j}_1$ have disjoint convex hulls in J_1. We can extend to a sequence $(\bar{j}_i)_{i<\omega}$ such that $(\overline{a}_{\overline{j_i}})_{i<\omega}$ is an indiscernable sequence. Then

$$(v^l(t(\overline{a}_{\overline{j_i}})))_{i<\omega}$$

is a non-constant indiscernible sequence in the value sort that is not indiscernible over γ.

By Proposition 4.3.1 the value sort is dp-minimal. Therefore $(b_j)_{j \in J_2}$ must be indiscernible over γ: Otherwise we could apply the above argument to the sequence $(b_j)_{j \in J_2}$ to get a second non-constant indiscernible sequence in the value sort which is not indiscernible over γ. Since these two sequences would be mutually indiscernible, this would contradict dp-minimality of the value sort. □

Theorem 4.4.2. *T is dp-minimal.*

Proof. Let $M = (Z, I, v) \models T$ be a sufficiently saturated model and let J_1 and J_2 be mutually indiscernible sequences. We will assume that both of them are indexed by a dense linear order. Let $z \in Z$ be a singleton. We aim to show that one of the sequences is indiscernible over z.

Since I is essentially an imaginary sort, we may assume that the sequences J_1 and J_2 live in the sort Z. Note that equality on the value sort can be expressed using the monotone binary relation $\leq$. By the quantifier elimination result, the failure of indiscernibility must be witnessed by formulas of the following form:

1. $t(\bar{x}) - nz = 0$,
2. $C(v^l(t(\bar{x}) - nz))$,
3. $R(v^{l_1}(t_1(\bar{x}) - n_1 z), v^{l_2}(t_2(\bar{x}) - n_2 z))$,

where t is an $\mathcal{L}_{\mathcal{Z}}$-term, C is a coloring on $\mathcal{I}$, R is a monotone binary relation on $\mathcal{I}$, $l \geq 1$, and $n \in \mathbb{Z}$. One of the terms in the third case could also be a quantifier free 0-definable constant in the value sort. This case is analogous to case (b) below and therefore we will not consider it separately.

Note that a formula of the first type would imply that z is algebraic over the parameters plugged in for $\bar{x}$. Hence it suffices to consider the other two types of formulas. If an indiscernible sequence J is not indiscernible over z, then this must be witnessed by $\bar{a}, \bar{a}' \subseteq J$ of the same order type such that we are in one of the following cases:

(a) We have

$$v^{l_1}(t(\bar{a}) - nz) \neq v^{l_1}(t(\bar{a}') - nz) \quad \text{and} \quad v^{l_2}(t'(\bar{a}) - n'z) \neq v^{l_2}(t'(\bar{a}') - n'z)$$

and

$$\models R(v^{l_1}(t(\bar{a}) - nz), v^{l_2}(t'(\bar{a}) - n'z)) \quad \text{and} \quad \not\models R(v^{l_1}(t(\bar{a}') - nz), v^{l_2}(t'(\bar{a}') - n'z))$$

for some choice of $t, t', n \neq 0, n' \neq 0$, and a relation R.

(b) We have

$$v^{l_1}(t(\bar{a}) - nz) \neq v^{l_1}(t(\bar{a}') - nz)$$

and

$$\models R(v^{l_1}(t(\bar{a}) - nz), v^{l_2}(t'(\bar{a}))) \quad \text{and} \quad \not\models R(v^{l_1}(t(\bar{a}') - nz), v^{l_2}(t'(\bar{a}')))$$

for some choice of $t, t', n \neq 0$, and a relation R.

(c) We have

$$v^{l_1}(t(\bar{a}) - nz) = v^{l_1}(t(\bar{a}') - nz) \quad \text{and} \quad v^{l_2}(t'(\bar{a})) < v^{l_2}(t'(\bar{a}'))$$

and

$$\not\models R(v^{l_1}(t(\bar{a}) - nz), v^{l_2}(t'(\bar{a}))) \quad \text{and} \quad \models R(v^{l_1}(t(\bar{a}') - nz), v^{l_2}(t'(\bar{a}')))$$

or

$$\models R(v^{l_2}(t'(\bar{a}), v^{l_1}(t(\bar{a}) - nz))) \quad \text{and} \quad \not\models R(v^{l_2}(t'(\bar{a}')), v^{l_1}(t(\bar{a}') - nz))$$

for some choice of $t, t', n \neq 0$, and a monotone binary relation R.

(d) We have

$$v^{l_1}(t(\bar{a}) - nz) = v^{l_1}(t(\bar{a}') - nz) \quad \text{and} \quad v^{l_2}(t'(\bar{a}) - n'z) < v^{l_2}(t'(\bar{a}') - n'z)$$

and

$$\not\models R(v^{l_1}(t(\bar{a}) - nz), v^{l_2}(t'(\bar{a}) - n'z)) \quad \text{and} \quad \models R(v^{l_1}(t(\bar{a}') - nz), v^{l_2}(t'(\bar{a}') - n'z))$$

or

$$\models R(v^{l_2}(t'(\bar{a}) - n'z), v^{l_1}(t(\bar{a}) - nz))) \quad \text{and} \quad \not\models R(v^{l_2}(t'(\bar{a}') - n'z), v^{l_1}(t(\bar{a}') - nz))$$

for some choice of $t, t', n \neq 0, n' \neq 0$, and a monotone binary relation R.

The case corresponding to a coloring is essentially the same as (b) so we will not do it explicitly.

We will use Lemma 4.2.14 to assume that all the l_i coincide: Let π be a finite set of primes. We want to be able to work in $Z_\pi(M)$. Fix a term

$$v^l(t(\bar{a}) - nz)$$

and write $t(\bar{a}) = b_0(\bar{a}) + b_1(\bar{a})$, $z = c_0 + c_1$ for $b_0(\bar{a}), c_0 \in Z_\pi(M)$, $b_1(\bar{a}), c_1 \in A_\pi(M)$. Since $A_\pi(M)$ is a finite set of constants, the value of $b_1(\bar{a})$ only depends on the order type of $\bar{a}$. Therefore

$$\gamma = v^l(b_1(\bar{a}) + nc_1) \in A_\pi(M)$$

also only depends on the order type of $\bar{a}$. We have

$$v^l(t(\bar{x}) - nz) = \min\{v^l(b_0(\bar{x}) - nc_0), \gamma\}$$

because $Z = Z_\pi(M) \times A_\pi(M)$. If $v^l(t(\bar{a}') - nz) = \gamma$ for all $\bar{a}'$ of the same order type as $\bar{a}$, then this value is a constant. If $v^l(t(\bar{a}') - nz) = v^l(b_0(\bar{a}') - nc_0)$ for all $\bar{a}'$ of the same order type as $\bar{a}$, then this value can always be calculated in $Z_\pi(M)$. If we are not in one of these two cases, then the quantifier free 0-definable coloring

$$C_{<\gamma}(i) \iff i < \gamma$$

witnesses (in $Z_\pi(M)$) that J is not indiscernible over z. Hence we can work in $Z_\pi(M)$ and therefore we can assume that all the l_i coincide (by Lemma 4.2.14). Moreover, to simplify the notation we will assume that all the l_i are equal to 1.

We say that an indiscernible sequence J has an approximation for z over $\alpha \in I$ if there is a set D such that J is indiscernible over D, α is definable over D, and the residue class of z modulo B_α is algebraic (in Z/B_α) over parameters in D.

We now assume that the mutually indiscernible sequences J_1 and J_2 both fail to be indiscernible over z. Then this must be witnessed as in (a) to (d). Such a witness for J_1 (resp. J_2) is *good* if J_2 (resp. J_1) has an approximation for z for a suitable α defined as follows:

- If the witness is given as in (a), then we set

  $$\alpha = \max\{v(t(\bar{a}) - t(\bar{a}')), v(t'(\bar{a}) - t'(\bar{a}'))\} + 1.$$

  If (for example) $\alpha = v(t(\bar{a}) - t(\bar{a}')) + 1$ $(= v(t(\bar{a}) - nz) + 1 < v(t(\bar{a}') - nz) + 1)$, then $t(\bar{a}') \equiv n'z \mod B_\alpha$. Therefore the residue class of z modulo B_α is algebraic over $t(\bar{a}')$.

- If the witness is given as in (b), then we set

  $$\alpha = v(t(\bar{a}) - t(\bar{a}')) + 1 = \min\{v(t(\bar{a}) - nz), v(t(\bar{a}') - nz)\} + 1.$$

  If $v(t(\bar{a}) - nz) < v(t(\bar{a}') - nz)$, then $t(\bar{a}') \equiv n'z \mod B_\alpha$ and therefore the residue class of z modulo B_α is algebraic over $t(\bar{a}')$.

- If the witness is given as in (c), we set
$$\alpha = v(t(\bar{a}) - nz).$$
- Now assume the witness is given as in (d). We set
$$\alpha_1 = v(t(\bar{a}) - nz) \quad \text{and} \quad \alpha_2 = v(t'(\bar{a}) - n'z) + 1.$$
Now put $\alpha = \max\{\alpha_1, \alpha_2\}$.

In particular, every witness of type (a) or (b) is good because J_1 and J_2 are mutually indiscernible. Recall that if $v(x) < v(y)$, then $v(x - y) = v(x)$. We aim to show that we can always find a good witness:

Suppose the witness is given as in (c). Choose $\bar{a}_0 \subseteq J_1$ of the same order type as $\bar{a}$ and $\bar{a}'$ such that all indices involved in $\bar{a}_0$ are smaller than the indices in $\bar{a}$ and $\bar{a}'$ (from now on, we will write $\bar{a}_0 \ll \bar{a}, \bar{a}'$ in that case). If $v(t(\bar{a}_0) - nz) \neq v(t(\bar{a}) - nz)$, then either the pair $(\bar{a}_0, \bar{a})$ or the pair $(\bar{a}_0, \bar{a}')$ gives a good witness as in case (b).

Hence we will assume $v(t(\bar{a}_0) - nz) = v(t(\bar{a}) - nz)$. Let $J_1^{>\bar{a}_0}$ be the sequence consisting of all elements of J_1 with index larger than all indices in $\bar{a}_0$ and set $J_2 \cup \bar{a}_0$ to be the sequence J_2 where each tuple is expanded by $\bar{a}_0$. Then $J_1^{>\bar{a}_0}$ and $J_2 \cup \bar{a}_0$ are mutually indiscernible. Moreover, $J_1^{>\bar{a}_0}$ is not indiscernible over $\alpha = v(t(\bar{a}) - nz)$ (as witnessed by $\bar{a}$ and $\bar{a}'$). Hence $J_2 \cup \bar{a}_0$ is indiscernible over α by Lemma 4.4.1. Now J_2 is indiscernible over the set $\{\bar{a}_0, \alpha\}$ and we have $\bar{a}_0 \equiv nz \mod B_\alpha$. Therefore the residue class of z modulo B_α is algebraic over $\bar{a}_0$ and hence the witness is good.

Now suppose the witness is given as in (d). We set
$$\alpha_1 = v(t(\bar{a}) - nz) \quad \text{and} \quad \alpha_2 = v(t'(\bar{a}) - n'z) + 1.$$
If $\alpha_2 \geq \alpha_1$, then we have a good witness by the same arguments as in (a) and (b). Hence assume $\alpha := \alpha_1 > \alpha_2$. Suppose for all $\bar{a}_0 \ll \bar{a}, \bar{a}'$ we have $v(t(\bar{a}_0) - nz) = \alpha$. Fix
$$\bar{a}_0 \ll \bar{a}_1 \ll \bar{a}, \bar{a}'.$$
Consider the mutually indiscernible sequences $J_1^{>\bar{a}_0}$ and $J_2 \cup \bar{a}_0$.

Assume that $J_1^{>\bar{a}_0}$ is indiscernible over α. Then the residue class of z modulo B_α is algebraic over $t(\bar{a}_1)$. Since $t'(\bar{a}) \not\equiv n'z \mod B_\alpha$, we get $t'(\bar{a}') \not\equiv n'z \mod B_\alpha$ by indiscernibility (applied to α and $\bar{a}_1$). Therefore $v(t'(\bar{a}) - n'z)$ and $v(t'(\bar{a}') - n'z)$ only depend on the residue class of z modulo B_α (and can be calculated in Z/B_α) and hence cannot witness the failure of indiscernibility over z.

Hence $J_1^{>\bar{a}_0}$ is not indiscernible over α. Then $J_2 \cup \bar{a}_0$ is indiscernible over α by Lemma 4.4.1. Therefore J_2 is indiscernible over $\{\bar{a}_0, \alpha\}$ and the residue class of z modulo B_α is algebraic over $\bar{a}_0$. Hence we have a good witness.

Hence we assume that there is $\bar{a}_0 \ll \bar{a}, \bar{a}'$ such that
$$v(t(\bar{a}_0) - nz) \neq \alpha.$$

If $v(t(\bar{a}_0) - nz) > \alpha$, then $\alpha = v(t(\bar{a}_0) - t(\bar{a}))$ and we have a good witness as in cases (a) and (b). Hence we assume $v(t(\bar{a}_0) - nz) < \alpha$.

If $v(t'(\bar{a}_0) - n'z) \notin \{v(t'(\bar{a}) - n'z), v(t'(\bar{a}') - n'z)\}$, then $(\bar{a}_0, \bar{a})$ or $(\bar{a}_0, \bar{a}')$ gives a good witness as in case (a). If $v(t'(\bar{a}_0) - n'z) = v(t'(\bar{a}) - n'z)$, then either $(\bar{a}_0, \bar{a}')$ gives a witness as in case (a) or the new witness is given by $(\bar{a}_0, \bar{a})$ and we have

$$v(t(\bar{a}) - nz) > v(t(\bar{a}_0) - nz) \quad \text{and} \quad v(t'\bar{a}) - n'z) = v(t'(\bar{a}_0) - n'z).$$

Hence we are again in case (d) but J_2 is indiscernible over

$$v(t'(\bar{a}) - n'z) = v(t'(\bar{a}) - t'(\bar{a}'))$$

and hence this witness given by $(\bar{a}_0, \bar{a})$ must be good.

Now only the case $v(t'(\bar{a}_0) - n'z) = v(t'(\bar{a}') - n'z)$ is left. We then have

$$v(t(\bar{a}) - nz) = v(t(\bar{a}') - nz) > v(t(\bar{a}_0) - nz),$$

$$v(t'(\bar{a}) - n'z) < v(t'(\bar{a}') - n'z) = v(t'(\bar{a}_0) - n'z).$$

Assume the witnessing formula was of the form

$$R(v(t(\bar{x}) - nz), v(t'(\bar{x}) - n'z))$$

for a monotone binary relation R (the other case is done analogously).

We then have the following implications by monotonicity:

$$\begin{aligned} &\models R(v(t(\bar{a}) - nz), v(t'(\bar{a}) - n'z)) \\ \Longrightarrow &\models R(v(t(\bar{a}') - nz), v(t'(\bar{a}') - n'z)) \\ \Longrightarrow &\models R(v(t(\bar{a}_0) - nz), v(t'(\bar{a}_0) - n'z)). \end{aligned}$$

Hence $R(v(t(\bar{a}) - nz), v(t'(\bar{a}) - n'z))$ must be false and $R(v(t(\bar{a}') - nz), v(t'(\bar{a}') - n'z))$ must be true (since this was a witness for the failure of indiscernibility over z). Then $R(v(t(\bar{a}_0) - nz), v(t'(\bar{a}_0) - n'z))$ must be true. But then $\bar{a}$ and $\bar{a}_0$ give a witness as in (a). Hence we can always find a good witness.

Since we assume that both J_1 and J_2 fail to be indiscernible over z, we can find a good witness for each of them. Let α be the constant for the witness in J_1 and let β be the constant for the witness in J_2. We assume $\alpha \leq \beta$. Then J_1 is indiscernible over β and over the residue class of z in Z/B_β.

Suppose the witness for J_1 is given as in (a) or (b). If we have

$$v(t(\bar{a}) - nz) < v(t(\bar{a}') - nz),$$

then $v(t(\bar{a}) - nz) < \beta$ and indiscernibility (and algebraicity of z modulo B_β over a suitable parameter) imply that $v(t(\bar{a}') - nz) < \beta$. Hence those values only depend on the residue class of z modulo B_β (and can be calculated in Z/B_β with the restricted valuation). Therefore they cannot witness the failure of indiscernibility over z.

Now suppose the witness for J_1 is given as in case (c). If $\alpha = \beta$, then this cannot be a witness for the failure for indiscernibility. Hence we must have $\alpha < \beta$. But then

$$v(t(\bar{a}) - nz) = v(t(\bar{a}') - nz)$$

only depends on the residue class of z in B_β and we can argue as before. The same arguments work if the witness for J_1 is given as in case (d).

Hence J_1 or J_2 must be indiscernible over z. □

To characterize distality we will show that the quotients B_i/B_{i+1} are stable. We will make use of the following lemma:

Lemma 4.4.3 (Lemma 5.13 of [2]). *Let $\mathcal{L}_0$ be any language and let T_0 be an unstable $\mathcal{L}_0$-theory. Let $\mathcal{L}_0^- \subseteq \mathcal{L}_0$ be such that $T_0|_{\mathcal{L}_0^-}$ is stable. Then there exists an $\mathcal{L}_0$-formula $\varphi(x, y)$, $|x| = 1$, over $\emptyset$ and a parameter b such that $\varphi(x, b)$ is not $\mathcal{L}_0^-$-definable.*

Proposition 4.4.4. *Suppose B_i/B_{i+1} is infinite. Then the induced structure on B_i/B_{i+1} is stable.*

Proof. Suppose B_i/B_{i+1} is infinite. By Lemma 4.4.3 it suffices to show that for every formula $\tilde{\varphi}(\tilde{x}, \tilde{y})$ (in B_i/B_{i+1}) and every constant $\tilde{b} \in B_i/B_{i+1}$ the formula $\tilde{\varphi}(\tilde{x}, \tilde{b})$ is definable in the pure group $(B_i/B_{i+1}, +)$.

Given such a formula there is an $\mathcal{L}^S_{\text{mon}}$-formula $\varphi(x, y)$ such that φ is the preimage of $\tilde{\varphi}$ under the natural projection

$$\pi_i : B_i \to B_i/B_{i+1}.$$

Now fix a preimage b of $\tilde{b}$. Note that $\varphi(B_i, b)$ is a union of cosets of B_{i+1}.

By the quantifier elimination result φ is equivalent to a boolean combination of atomic $\mathcal{L}^S_{\text{mon}}$-formulas. We aim to show the following:

Claim. There is a formula $\psi(x, y)$ which is defined in the pure abelian group $(B_i, +)$ such that $\varphi(B_i, b)$ and $\psi(B_i, b)$ coincide on all but finitely many cosets of B_{i+1}.

It suffices to prove the claim for atomic formulas. Therefore we may assume that φ is atomic. Then we are in one of the following cases:

(a) $\varphi(x, b) \equiv nx - t(b) = 0$,

(b) $\varphi(x, b) \equiv R(v^{l_1}(n_1 x - t_1(b)), v^{l_2}(n_2 x - t_2(b)))$,

(c) $\varphi(x, b) \equiv C(v^l(nx - t(b)))$.

In case (a) there is nothing to show. Therefore we consider the cases (b) and (c) which include valuations. We show that sets of the form

$$(a + lB_j) \cap B_i$$

are definable in the pure abelian group $(B_i, +)$ up to a unique coset of B_{i+1}:

If $j < i$, then $B_j > B_i$ and lB_j has finite index in B_j. Hence $lB_j \cap B_i$ has finite index in B_i. Moreover, $lB_j \cap B_i$ is of the form

$$lB_j \cap B_i = l'B_i$$

for a positive integer l' because this holds true for the standard models. The cosets of $l'B_i$ are definable in the pure group language. If $j = i$, then $lB_i \cap B_i = lB_i$ is definable in the pure group language. Now assume $j > i$. Then $lB_j < B_j \leq B_{i+1}$ and therefore $B_i \cap (a + lB_j)$ is trivial outside of a single coset of B_{i+1}.

This also shows that there are only finitely many intersections of the form

$$(a + lB_j) \cap (B_i \setminus (a + B_{i+1}))$$

where everything except j is fixed. Therefore the restriction of $v^l(x-a)$ to $B_i \setminus (a+B_{i+1})$ is given by a finite chain of definable subgroups (in the pure abelian group $(B_i, +)$).

Since $nx \equiv 0 \mod B_{i+1}$ has only finitely many solutions modulo B_{i+1} the same holds true for the valuation $v^l(nx - a)$ restricted to B_i: Outside of finitely many cosets of B_{i+1} it is given by a finite chain of $(B_i, +)$-definable subgroups. In that sense $v^l(nx - a)$ is $(B_i, +)$-definable outside of finitely many cosets of B_{i+1}.

Therefore the formula φ in (a) or (b) is definable in $(B_i, +)$ outside of finitely many cosets of B_{i+1}. This shows the claim.

Hence we can find such a formula $\psi(x, y)$ defined in the pure abelian group $(B_i, +)$ such that $\varphi(B_i, b)$ and $\psi(B_i, b)$ coincide on all but finitely many cosets of B_{i+1}. The usual quantifier elimination result for abelian groups shows that $\psi(B_1, b)$ is a boolean combination of cosets of the trivial subgroup and groups of the form lB_i for $l \geq 1$. Each subgroup lB_i has finite index in B_i and the family $\{lB_i : l \geq 1\}$ is closed under finite intersections. Hence a boolean combination of such groups is a union of finitely many cosets of lB_i for a suitable l.

Since $\varphi(B_i, b)$ and $\psi(B_i, b)$ agree on all but finitely many cosets of B_{i+1} and $\varphi(B_i, b)$ is a union of cosets of B_{i+1}, the same must be true for $\tilde{\varphi}(B_i/B_{i+1}, \tilde{b})$, i.e. $\tilde{\varphi}(B_i/B_{i+1}, \tilde{b})$ is a boolean combination of cosets of $(B_i/B_{i+1}, +)$-definable subgroups. Therefore $\tilde{\varphi}(B_i/B_{i+1}, \tilde{b})$ is definable in $(B_i/B_{i+1}, +)$. □

Theorem 4.4.5. *T is distal if and only if there is a constant $k < \omega$ such that*

$$|B_i/B_{i+1}| \leq k$$

holds for all $i < \infty$.

Proof. Suppose $|B_i/B_{i+1}|$ is unbounded. Then there is some i_0 such that $|B_{i_0}/B_{i_0+1}|$ is infinite. By Proposition 4.4.4 the induced structure on B_{i_0}/B_{i_0+1} is stable. Hence it follows from Proposition 2.2.12 that T is not distal.

Now let X be a non-constant totally indiscernible set of singletons and fix $x, y \in X$. Put $i_0 = v(x^{-1}y)$. If $x \neq y$, then $i_0 < \infty$ and hence

$$xB_{i_0} = yB_{i_0} \qquad xB_{i_0+1} \neq xB_{i_0+1}.$$

It follows easily from total indiscernibility that i_0 does not depend on the choice of $x \neq y$. Hence $|X| \leq |B_{i_0}/B_{i_0+1}|$. □

5. Valuations on the integers

The most well-known example of a dp-minimal expansion of $(\mathbb{Z}, +)$ is $(\mathbb{Z}, +, \leq)$. Based on work by Palacín and Sklinos [20], Conant and Pillay [9] proved the remarkable result that $(\mathbb{Z}, +, 0)$ has no proper stable expansions of finite dp-rank. Hence any proper dp-minimal expansion must be unstable. The other known examples of dp-minimal expansions are:

- $(\mathbb{Z}, +, v_p)$ where v_p is the p-adic valuation on $\mathbb{Z}$. This was shown by Alouf and d'Elbée in [2].
- $(\mathbb{Z}, +, C)$ where C is cyclic order. These were found by Tran and Walsberg in [34].
- Proper dp-minimal expansions of $(\mathbb{Z}, +, S)$, where S is a dense cyclic order, and $(\mathbb{Z}, +, v_p)$ were very recently found by Walsberg in [36].

An overview about the current research on dp-minimal expansions of $(\mathbb{Z}, +)$ is given by Walsberg in Section 6 of [36].

5.1. A single valuation

We add the following family of examples which generalize the p-adic examples by Alouf and d'Elbée:

Theorem 5.1.1. *Let $(B_i)_{i<\omega}$ be a strictly descending chain of subgroups of $\mathbb{Z}$, $B_0 = \mathbb{Z}$, let $v : \mathbb{Z} \to \omega \cup \{\infty\}$ be the valuation defined by*

$$v(x) = \max\{i : x \in B_i\},$$

and let S be a set of unary predicates and monotone binary relations on the value set. Then $(\mathbb{Z}, 0, 1, +, v, S)$ admits quantifier elimination in the language $\mathcal{L}^S_{\text{mon}}$ (with 0 and 1 as constants) and is dp-minimal. Moreover, $(\mathbb{Z}, 0, 1, +, v, S)$ is distal if and only if the size of the quotients B_i/B_{i+1} is bounded.

Proof. Note that any infinite strictly descending chain of subgroups of $\mathbb{Z}$ must have trivial intersection. Moreover, every non-trivial subgroup of $\mathbb{Z}$ is of the form $n\mathbb{Z}$ for some $n \geq 1$ and hence v is a good valuation in the sense of Definition 4.0.1.

Moreover, $\mathbb{Z} \prec \hat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$ and $\langle 1 \rangle = \mathbb{Z}$ is dense. Hence Proposition 4.3.3 implies the quantifier elimination result. Dp-minimality follows by Theorem 4.4.2 and the claim about distality follows by Theorem 4.4.5. ☐

In case of the p-adic valuation Alouf and d'Elbée proved in Theorem 1.1 of [2] that $(\mathbb{Z},+,v_p)$ has quantifier elimination in the language $\mathcal{L}_p^E = \{+,-,0,1,|_p,D_n)_{n\geq 1}$ where

$$x|_p y \iff v_p(x) \leq v_p(y) \quad \text{and} \quad D_n = n\mathbb{Z}.$$

Conant [8] showed that the structure $(\mathbb{Z},+,0,1,\leq)$ is a minimal proper expansion of $(\mathbb{Z},+,0,1)$, i.e. there is no proper intermediate expansion. Alouf and d'Elbée proved the same for $(\mathbb{Z},+,0,1,v_p)$. We will show that this does not hold true for arbitrary valuations.

Proposition 5.1.2. *Fix distinct primes $p_0, p_1, q \in \mathbb{P}$ and put $s = p_0p_1q$. For $i < \omega$ fix $\sigma_i \in \operatorname{Sym}(\{0,1\})$, set $n_0 = 1$, and recursively define*

$$n_{3l+m} = \begin{cases} n_{3l-1}q & \text{iff } m = 0, \\ n_{3l}p_{\sigma_l(0)} & \text{iff } m = 1, \\ n_{3l+1}p_{\sigma_l(1)} & \text{iff } m = 2. \end{cases}$$

Set v_σ to be the valuation corresponding to $(n_i\mathbb{Z})_{i<\omega}$ and let w be the valuation corresponding to $(s^i\mathbb{Z})_{i<\omega}$. Then w is definable in $(\mathbb{Z},+,v_\sigma)$.

Proof. If $a \in \mathbb{Z}\setminus\{0\}$, then there is a unique $t_a \in \{p_0,p_1,q\}$ such that $v_\sigma(a) < v_\sigma(t_a a)$. Let $a,b \in \mathbb{Z}\setminus\{0\}$. If $|v_\sigma(a) - v_\sigma(b)| \geq 3$, then

$$w(a) < w(b) \iff v_\sigma(a) < v_\sigma(b).$$

If $|v_\sigma(a) - v_\sigma(b)| < 3$, then $w(a) \leq w(b)$ can be determined using t_a and t_b. □

Corollary 5.1.3. *Let w be as in Proposition 5.1.2. Then there are $2^{\aleph_0}$ many valuations v such that w is definable in $(\mathbb{Z},+,v)$. Only countably many of those can be definable in $(\mathbb{Z},+,w)$.*

Proof. There are $2^{\aleph_0}$ many valuations v_σ as in Proposition 5.1.2 and w is definable in each $(\mathbb{Z},+,v_\sigma)$. On the other hand, $(\mathbb{Z},+,w)$ has only countably many definable sets. □

Remark 5.1.4. Note that by Theorem 4.4.5 all these structures are distal. Hence not even all dp-minimal distal expansions by valuations are minimal expansions.

The fact that expansions by arbitrary valuations are dp-minimal allows us to construct other non-trivial examples: For $k \geq 2$ let v_k denote the valuation corresponding to the sequence $(k^i\mathbb{Z})_{i<\omega}$.

Proposition 5.1.5. *Let r and s be coprime positive integers. Then the expansion $(\mathbb{Z},+,v_r(x) < v_s(x))$ is dp-minimal.*

Proof. We have

$$v_r(x) < v_s(x) \iff v_{rs}(x) < v_{rs}(rx).$$

Hence the relation $v_r(x) < v_s(x)$ is definable in the dp-minimal structure $(\mathbb{Z},+,v_{rs})$. □

It seems unlikely that v_{rs} is definable from $v_r(x) \leq v_s(x)$.

The induced structure on the index set $\omega \cup \{\infty\}$ seems to be important. If it is not o-minimal and $X \subseteq \omega \cup \{\infty\}$ is a definable infinite and co-infinite subset, then the set

$$A = \{a \in \mathbb{Z} : w(a) \in X\} \subseteq \mathbb{Z}$$

is definable. It is not clear if w is definable in $(\mathbb{Z}, +, 0, 1, A)$.

If the induced structure on $\omega \cup \{\infty\}$ is o-minimal, then $k = |B_i/B_{i+1}| \in \mathbb{N} \cup \{\infty\}$ must be constant for all sufficiently large i (in some elementary extension). If k is finite, then w is bounded and hence we are in the distal case.

Conjecture 5.1.6. Let $(\mathbb{Z}, +, 0, 1, v)$ be distal. Then the following are equivalent:

(a) $(\mathbb{Z}, +, 0, 1, v)$ is a minimal expansion of $(\mathbb{Z}, +, 0, 1)$,

(b) there is a prime p such that $|B_i/B_{i+1}| = p$ for almost all $i < \omega$,

(c) v is interdefinable with a p-adic valuation for some prime p,

(d) the $(\mathbb{Z}, +, v)$-induced structure on the value set of v' is o-minimal for all $(\mathbb{Z}, +, v)$-definable valuations v'.

Proposition 5.1.7. *If (a) implies (d), then Conjecture 5.1.6 holds.*

Proof. We already know (b) $\implies$ (c) $\implies$ (a) and by assumption (a) $\implies$ (d) holds. Hence (d) $\implies$ (b) remains to be shown.

Let $(\mathbb{Z}, +, 0, 1, v)$ be distal and assume (d). Then there is $k > 1$ such that

$$|B_i : B_{i+1}| = k$$

for almost all $i < \omega$. Therefore v and v_k are interdefinable and we may assume $v = v_k$.

If $k = st$ where s and t are coprime, then v is interdefinable with the valuation w such that $|B_i^w/B_{i+1}^w|$ alternates between s and t. Then the induced structure on the value set of w is not o-minimal. This contradicts (d).

Hence we may assume $k = p^n$ for some prime p and $n \geq 1$. If $n > 1$, then the p-adic valuation v_p is definable by

$$v_p(x) \leq v_p(y) \iff \bigwedge_{r=0}^{n-1} v_{p^n}(p^r x) \leq v_{p^n}(p^r y).$$

Now the set $v_p(\{a \in \mathbb{Z} : v_{p^n}(pa) > v_{p^n}(a)\})$ contradicts (d).

Hence $k = p$ must be a prime. This shows (b). $\square$

There are non-distal candidates for minimal expansions:

Question 5.1.8. Let $(p_i)_{0<i<\omega}$ be an enumeration of the primes such that each prime appears exactly once and let v be the valuation corresponding to $(p_1 \cdots p_i\mathbb{Z})_{i<\omega}$. Then the induced structure on the value set is o-minimal. Is $(\mathbb{Z}, +, 0, 1, v)$ a minimal expansion of $(\mathbb{Z}, +, 0, 1)$?

We end this section with the observation that the p-adic valuations have a limit theory:

Proposition 5.1.9. *For each prime p let v_p denote the p-adic valuation on $\mathbb{Z}$. Then the corresponding limit theory exists, i.e.*

$$\mathrm{Th}(\prod_p(\mathbb{Z},+,v_p)/\mathcal{U})$$

does not depend on the choice of the non-principal ultrafilter $\mathcal{U} \subseteq \mathcal{P}(\mathbb{P})$.

Proof. We fix the common $\mathcal{L}^-$-theory

$$T = \bigcap_{\mathcal{U}} \mathrm{Th}_{\mathcal{L}^-}(\prod_p(\mathbb{Z},+,v_p)/\mathcal{U})$$

of these ultraproducts. Note that the predicate $\mathrm{Div}^l_{q^k}(i,j)$ fails for all $0 < i < j$ and the predicate Ind^l_k holds true for all $0 < i < j$. Thus they are quantifier free 0-definable after naming the successor function S on $\mathcal{I}$. Therefore T has quantifier elimination after naming S by Theorem 4.2.3 (because $(\omega, 0, \leq, S)$ has quantifier elimination). The constants in $\mathcal{L}_Z$ generate a subgroup that is isomorphic to $\mathbb{Z}$. An element $a \in \mathbb{Z} \setminus \{0\}$ must have valuation 0 in all models of T. Therefore all models of T have isomorphic substructures and hence T is complete. □

5.2. Multiple valuations

If $P \subseteq \mathbb{P}$ is a non-empty set of primes, then Alouf and d'Elbée proved that the structure $(\mathbb{Z},+,v_p)_{p\in P}$ has dp-rank exactly $|P|$. We will generalize this result to expansions of $(\mathbb{Z},+)$ by arbitrary valuations which involve disjoint sets of primes.

Let V be a non-empty family of non-trivial valuations $v : \mathbb{Z} \to \omega \cup \{\infty\}$. For each $v \in V$ set

$$\pi_v = \{p \in \mathbb{P} : p \text{ divides } |B^v_i/B^v_{i+1}| \text{ for some } i < \omega\}.$$

We view $(\mathbb{Z},+)$ together with these valuations as a multi-sorted structure with group sort $\mathcal{Z}$ and with a distinct value sort $\mathcal{I}_v$ for each valuation $v \in V$. Now put

- $\mathcal{L}_{\mathcal{Z}} = \{0, 1, +, -\}$,
- $\mathcal{L}_v = \{v^l : l \geq 1\}$, and
- $\mathcal{L}^-_{\mathcal{I}_v} = \{-\infty, 0, +\infty, \leq, \mathrm{Div}^l_{q^k}, \mathrm{Ind}^l_k\}_{q,k,l}$

for each valuation $v \in V$. Let $\mathcal{L}^v_{\mathrm{mon}}$ be the monotone hull of $\mathcal{L}^-_{\mathcal{I}_v}$ as in Section 4.3 and set

$$\mathcal{L}_{\mathrm{mon}} = \mathcal{L}_{\mathcal{Z}} \cup (\bigcup_{v\in V} \mathcal{L}_v) \cup (\bigcup_{v\in V} \mathcal{L}^v_{\mathrm{mon}})$$

to be the disjoint union of these languages.

Proposition 5.2.1. *Suppose the sets π_v are pairwise disjoint. Then $(\mathbb{Z}, +, v)_{v\in V}$ has quantifier elimination in the language $\mathcal{L}_{mon}$.*

Proof. This is very similar to the proof of Theorem 4.2.3. Note that a multi-sorted version of Lemma 2.3.2 holds true in this setting. As in the proof of Theorem 4.2.3 it suffices to show the back-and-forth property for systems of linear congruences. Let $\mathcal{S}$ be the system

$$\begin{aligned} n_s x - b_s &\equiv 0 \mod l_s B^v_{i_s}, \quad s \in S^v, \\ n_t x - b_t &\not\equiv 0 \mod l_t B^v_{i_t}, \quad t \in T^v, \end{aligned}$$

where $S^v \neq \emptyset$ and T^v are finite index sets for each $v \in V_0$ for a finite subset $V_0 \subseteq V$. By an application of Lemma 4.2.14 we may assume that all the l_s and l_t have the same value which we denote by l.

Let a be a solution. We will show that we can assume that a and all constants b_s and b_t are contained in lB_0: If a is in lB_0, then all b_s must be contained in lB_0 since otherwise the congruences can not be satisfied. If b_t is not contained in lB_0, then the congruence

$$n_t x - b_t \not\equiv 0 \mod lB^v_{i_t}$$

does not impose any restrictions on lB_0 and we can ignore it without changing the solutions in lB_0.

If a is not contained in lB_0, then there is a constant $c \in \mathbb{Z}$ (and hence in the language) such that $a - c \in lB_0$. In that case the shifted system $\mathcal{S}^c$:

$$\begin{aligned} n_s(x + c) - b_s &\equiv 0 \mod lB^v_{i_s}, \quad s \in S^v, \\ n_t(x + c) - b_t &\not\equiv 0 \mod lB^v_{i_t}, \quad t \in T^v, \end{aligned}$$

is solved by $a - c \in lB_0$ and all the constants $n_s c - b_s$ and $n_t c - b_t$ can be assumed to lie in lB_0. Thus we can replace $\mathcal{S}$ by $\mathcal{S}^c$.

Hence we may assume that $\mathcal{S}$ is a system of linear congruences in the subgroup lB_0. We have

$$lB_0 \equiv \hat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$$

and the valuations v^l involve disjoint sets of primes. Therefore the system $\mathcal{S}$ can be solved independently for each valuation $v \in V$. This is done as in the proof of Theorem 4.2.3. □

Theorem 5.2.2. *Suppose the sets π_v are pairwise disjoint. Then*

$$\textit{dp-rk}((\mathbb{Z}, +, v)_{v\in V}) = |V|.$$

Proof. $\geq$ is shown exactly as in the case of the p-adic valuations which was done by Alouf and d'Elbée (Theorem 1.2 of [2]).

Now assume $\kappa :=$ dp-rk$((\mathbb{Z}, +, v)_{v\in V}) > |V|$. As in the proof of Theorem 4.4.2 this is witnessed by mutually indiscernible sequences $(I_i)_{i<\kappa}$ (in the group sort) and a singleton c in the group sort such that no sequence is indiscernible over c. As argued in Theorem 4.4.2, the fact that a sequence I is not indiscernible over c must be witnessed by an atomic $\mathcal{L}_{\mathrm{mon}}$-formula which involves a valuation.

Since $\kappa > |V|$, there must be two sequences I_1 and I_2 for which this witnessing formula involves the same valuation v. This is a contradiction because $(\mathbb{Z}, +, v)$ is dp-minimal by Theorem 4.4.2. □

6. Further results

6.1. Uniformly definable families of finite-index subgroups of dp-minimal groups

The classification of NIP profinite groups by Macpherson and Tent in [31] yields information about uniformly definable families of finite index subgroups in arbitrary NIP groups (see Theorem 8.7 in [7]). We will do the same in the dp-minimal case. The arguments are almost identical to those in Section 8 of [7] (see also Remark 5.5 in [31]), we only need to make sure that the construction presented there preserves dp-minimality.

Let H be a group and let $(N_i : i \in I)$ be a family of normal subgroups of finite index such that

$$\forall i, j \exists k : N_k \leq N_i \cap N_j.$$

We view H as an $\mathcal{L}_{\text{prof}}$-structure $\mathcal{H} = (H, I)$. Let $f_j : \varprojlim H/N_i \to H/N_j$ be the projection maps. Then $\{\ker f_j : j \in I\}$ is a neighborhood basis at the identity. Therefore we may view $\varprojlim H/N_i$ as an $\mathcal{L}_{\text{prof}}$-structure $(\varprojlim H/N_i, I)$.

Lemma 6.1.1. *Let $\mathcal{H}^* = (H^*, I^*)$ be an $|I|^+$-saturated elementary extension of $\mathcal{H}$. Then*

$$\mathcal{H}^* / \bigcap_{i \in I} N_i^* \cong \varprojlim_{i \in I} H/N_i$$

and $(N_j^* / \bigcap_{i \in I} N_i^* : j \in I)$ is a neighborhood basis for the identity consisting of open normal subgroups.

Proof. By elementarity we have $|H^* : N_i^*| = |H : N_i|$ for all $i \in I$. Using this and elementarity it is easy to see that

$$\varprojlim_{i \in I} H^*/N_i^* = \varprojlim_{i \in I} H/N_i.$$

Now write

$$\varprojlim_{i \in I} H^*/N_i^* = \{(g_i N_i^*)_i : \forall i \geq j : g_i N_j^* = g_j N_j^*\}$$

and let $f : H^* \to \varprojlim_{i \in I} H^*/N_i^*, g \mapsto (gN_i^*)_i$ be the natural homomorphism. Clearly $\ker f = \bigcap_{i \in I} N_i^*$. It remains to show that f is surjective.

Fix $(g_i N_i)_i \in \varprojlim_{i \in I} H^*/N_i^*$ and consider the partial type

$$\Sigma(x) = \{x \in g_i N_i^* : i \in I\}.$$

Given $I_o \subseteq I$ finite, there is $j \in I$ such that $N_j \leq \bigcap_{i \in I_0} N_i$. Then $g_i N_j = g_{i'} N_j$ for all $i, i' \in I_0$. Hence $\Sigma(x)$ is finitely satisfiable and as $\mathcal{H}^*$ is $|I|^+$-saturated, there exists $g \in H^*$ such that $g \in g_i N_i^*$ for all $i \in I$ and hence $f(g) = (g_i N_i^*)$.

The family $(N_j^* / \bigcap_{i \in I} N_i^* : j \in I)$ is a neighborhood basis for the identity consisting of open normal subgroups. □

Lemma 6.1.2. *If $\mathcal{H} = (H, I)$ has NIP, then $(\varprojlim_{i \in I} H/N_i, I)$ has NIP. If moreover (H, I) is dp-minimal, then $(\varprojlim_{i \in I} H/N_i, I)$ is dp-minimal.*

Proof. Since (H, I) has NIP, every uniformly definable family of subgroups contains only finitely many subgroups of each finite index. Let (H^*, I^*) be an $|I|^+$-saturated elementary extension. Then I is externally definable (since $I = \{i \in I^* : |H^* : K_i^*| < \infty\}$). If (H, I) is dp-minimal, then (H^*, I^*, I) is dp-minimal by Remark 2.2.9. By the above lemma the structure $(\varprojlim_{i \in I} H/N_i, I)$ is interpretable as a quotient in (H^*, I^*, I) and hence is NIP (resp. dp-minimal). □

Let G be a group and let $\varphi(x, y)$ be a formula. Set $\mathcal{N}_\varphi = \{N_i : i \in I\}$ to be the family of all normal subgroups which are finite intersections of conjugates of φ-definable subgroups of finite index. Note that every φ-definable subgroup of finite index contains some $N \in \mathcal{N}_\varphi$. The profinite group $\varprojlim_{i \in I} G/N_i$ naturally becomes an L_{prof}-structure $\mathcal{G}_\varphi = (\varprojlim_{i \in I} G/N_i, I)$.

Proposition 6.1.3. *Let G and φ be as above. If G is NIP, then $\mathcal{G}_\varphi$ is NIP. If moreover G is dp-minimal, then $\mathcal{G}_\varphi$ is dp-minimal in the group sort.*

Proof. By Baldwin-Saxl finite intersections of conjugates of φ-definable subgroups are uniformly definable by some formula $\psi(x, z)$. The set $J = \{b : \psi(G, b) \trianglelefteq G\}$ is definable. Put $J_0 = \{b : |G : \psi(G, b)| < \infty\}$. Then $\mathcal{N}_\varphi = \{\psi(G, b) : b \in J_0\}$. Since $\mathcal{N}_\varphi$ is closed under intersections, it follows that J_0 is externally definable. Let E be the equivalence relation defined by $aEb \iff \psi(G, a) = \psi(G, b)$. Now apply the previous lemma to the structure $(G, J_0/E)$. □

By Proposition 3.0.3 every dp-minimal profinite group (G, I) has an open abelian subgroup. Now Proposition 6.1.3 implies the following:

Proposition 6.1.4. *Let G be a dp-minimal group and let $\varphi(x, y)$ be a formula. Let $\mathcal{N}_\varphi$ be the family of all normal subgroups which are finite intersections of conjugates of φ-definable subgroups of finite index. If $\mathcal{N}_\varphi$ is infinite, then there is $N \in \mathcal{N}_\varphi$ such that for all $M \in \mathcal{N}_\varphi$ the quotient $N/(N \cap M)$ is abelian.*

Proof. The profinite group $(\varprojlim_{N \in \mathcal{N}_\varphi} G/N, \mathcal{N}_\varphi)$ is dp-minimal and therefore is virtually abelian by Proposition 3.0.3. Since the quotients G/N are preserved, this implies the proposition. □

Remark 6.1.5. By Theorem 3.0.4 there are essentially two types of dp-minimal profinite groups. This will also be seen in the abelian quotients in the statement of Proposition 6.1.4.

Remark 6.1.6. By Proposition 5.1 of [31] every profinite NIP group (G, I) has an open prosolvable subgroup. Hence if we only assume NIP in the previous theorem, the quotients will be solvable instead of abelian (see Theorem 8.7 of [7]).

6.2. Strong homogeneity of profinite groups

Jarden and Lubotzky [14] showed that two elementarily equivalent profinite groups are isomorphic if one of them is finitely generated. This was generalized to strongly complete profinite groups by Helbig [13]. The tools used by Helbig and the construction in Section 6.1 give a proof for strong homogeneity.

Let G be a profinite group and suppose $(N_i : i \in I)$ is a neighborhood basis at the identity consisting of open normal subgroups. Let $\mathcal{L}_P$ be the group language expanded by a family of unary predicates $(P_i : i \in I)$. We consider G as an $\mathcal{L}_p$ structure by setting $P_i(G) = N_i$. Note that if G^* is an elementary expansion, then there is a natural $\mathcal{L}_P$-structure on the quotient $G^*/(\bigcap_{i\in I} P_i(G^*))$.

Lemma 6.2.1. *Let G a profinite group equipped with an $\mathcal{L}_P$ structure as above. Let G^* be an elementary extension of G in the language $\mathcal{L}_P$. Then the composition*

$$G \to G^* \to G^*/(\bigcap_{i\in I} P_i(G^*))$$

is an $\mathcal{L}_P$-isomorphism.

Proof. The lemma follows from the same arguments as Lemma 6.1.1. □

Proposition 6.2.2. *Let G and H be profinite groups as $\mathcal{L}_P$ structures such that the predicates $(P_i : i \in I)$ encode neighborhood bases at the identity consisting of open normal subgroups in both groups. Suppose $A \subseteq G$ is a subset and $f : A \to H$ is an elementary map with respect to the language $\mathcal{L}_P$. Then f extends to an $\mathcal{L}_P$-isomorphism between G and H.*

Proof. Let G^* be a common strongly $|A|^+$-homogeneous elementary extension of G and H. We can find $\tilde{f} \in \mathrm{Aut}(G^*)$ such that $\tilde{f}|_A = f$. Since $\tilde{f}$ is an L_P-automorphism, it induces an automorphism of $G^*/(\bigcap_{i\in I} P_i(G^*))$. Now use Lemma 6.2.1 to get the desired isomorphism between G and H. □

The following observation in Remark 3.12 in [13] is a consequence of Theorem 2 in [30] and Corollary 52.12 in [19]:

Theorem 6.2.3. *Let G be a profinite group. Then the following are equivalent:*

(a) G is strongly complete.

(b) For each finite group A there exists a group word w such that $w(A) = 1$ and $w(G)$ is open in G.

Recall that a group word has *finite width* if $\langle w(G)\rangle = w(G)^n$ for some $n > \omega$. We will make use of the following result:

Proposition 6.2.4 (Proposition 5.2(b) of [37]). *Let G be a profinite group. If w is a group word, then $w(G)$ is closed in G if and only if w has finite width in G.*

Proposition 6.2.5. *Let G and H be profinite groups. Let $A \subseteq G$ be a subset of G and let $f : A \to H$ be an elementary map. If one of the groups is strongly complete, then f extends to an isomorphism.*

Proof. By Theorem 6.2.3 and Proposition 6.2.4 strong completeness is a first-order property among profinite groups. For each finite group A there is a group word w_A such that $w_A(A) = 1$, $w_A(G)$ is open in G, and $w_A(H)$ is open in H. Note that by Proposition 6.2.4 and elementary equivalence of G and H, $w_A(G)$ and $w_A(H)$ are definable by the same formula without parameters.

If N is an open normal subgroup of G then $w_{G/N}(G/N) = 1$ and hence $w_{G/N}(G) \subseteq N$. Therefore the family $(w_B(G) : B$ a finite group$)$ is a neighborhood basis at the identity.

Hence we may consider G and H as $\mathcal{L}_P$-structures where the predicates are given by $P_B(G) = w_B(G)$. By Proposition 6.2.2 f extends to an isomorphism. □

6.3. A result on families of subgroups of NTP$_2$ groups

By Theorem 1.1 of [31] a full profinite NIP group is NIP if and only if it is NTP$_2$. Since the structure of these groups is determined by the lattice of subgroups, this only depends on a single formula. We will show a version for formulas in NTP$_2$ groups. We will use the following lemma by Macpherson and Tent on groups in NTP$_2$:

Lemma 6.3.1 (Lemma 4.3 in [31]). *Let G be an $\emptyset$-definable group in a structure with NTP$_2$ theory, and $\varphi(x, \bar{y})$ a formula implying $x \in G$. Then there is $k = k_\varphi \in \mathbb{N}$ such that the following holds. Suppose that H is a subgroup of G, $\pi : H \longrightarrow \Pi_{i\in J} T_i$ is an epimorphism to the Cartesian product of the groups T_i, and $\pi_j : H \longrightarrow T_j$ is for each $j \in J$ the composition of π with the canonical projection $\Pi_{i\in J} T_i \to T_j$. Suppose also that for each $j \in J$, there is a subgroup $\bar{R}_j \leq G$ and group $R_j < T_j$ with $\bar{R}_j \cap H = \pi_j^{-1}(R_j)$, such that finite intersections of the groups $\bar{R}_j$ are uniformly definable by instances of $\varphi(x, \bar{y})$. Then $|J| \leq k$.*

Proposition 6.3.2. *Let G be an NTP$_2$ group and let $\varphi(x, y)$ be a formula such that $|x| = 1$. Suppose that the family $\{\varphi(G, b) : b \in G\}$ consists of normal subgroups of G and is closed under finite intersections. Then $\varphi(x, y)$ has NIP.*

Proof. We aim to show that φ satisfies the Baldwin-Saxl condition. Let $N_1, \dots N_n$ be instances of φ and fix k_φ as in Lemma 6.3.1. Now set $C_k = \bigcap\{N_i : 1 \leq i \leq n, i \neq k\}$ and $C = \bigcap\{N_i : 1 \leq i \leq n\}$. Note that $C_i \cap N_i = C$ and we have $C_i \subseteq N_j$ if $i \neq j$. Now set

$$H = \langle C_i : 1 \leq i \leq n\rangle.$$

We then have

$$H/C \cong \prod_{i=1}^{n} C_i/C.$$

Now set $T_i = C_i/C$ and assume that all T_i are non-trivial. Let

$$\pi : H \to H/C = \prod_{i=1}^{n} T_i$$

be the natural projection and let $\pi_j : H \to T_j$ be the projection on T_j. Set $R_j = 1 < T_j$ and put $\bar{R}_j = N_j$. Then

$$\bar{R}_j \cap H = N_j \cap H = \pi_j^{-1}(R_j).$$

Hence Lemma 6.3.1 implies $n \leq k_\varphi$.

If $n > k_\varphi$, then there must be $1 \leq i \leq n$ such that $T_i = 1$ and hence $C = C_i$ can be written as in intersection of $n-1$ instances of φ. Inductively this shows that any intersection of instances of φ is an intersection of at most k_φ instances. Hence φ satisfies the Baldwin-Saxl condition.

This implies that φ has NIP: Otherwise we can find a constant a and an indiscernible sequence $(b_i)_{i<\omega}$ such that

$$\models \varphi(a, b_i) \iff i \text{ is odd.}$$

Set $n = k_\varphi$ and take $i_0, \dots i_n < \omega$, all of them odd. By the Baldwin-Saxl lemma we may assume

$$H_{i_0} \cap \dots H_{i_n} = H_{i_1} \cap \dots H_{i_n}.$$

By indiscernibility this implies

$$H_{i_0+1} \cap \dots H_{i_n} = H_{i_1} \cap \dots H_{i_n}.$$

But this is a contradiction since $a \notin H_{i_0+1}$. □

While it is clearly sufficient to assume that the φ-definable subgroups normalize each other, the above proof requires some normality assumption.

Question 6.3.3. Does Proposition 6.3.2 hold even without any normality assumption?

Part II.

Planes in sharply 2-transitive groups

7. Introduction and overview

The standard example of a sharply 2-transitive group is of the form $\mathrm{AGL}_1(K) \cong K_+ \rtimes K^*$ where K is a field or more generally a near-field. A sharply 2-transitive group is called split if it is of this form; equivalently, if it has a nontrivial abelian normal subgroup. By results of Zassenhaus and Jordan every finite sharply 2-transitive group is in fact split. Recently the first examples of non-split infinite sharply 2-transitive groups were constructed by Rips, Segev, and Tent in characteristic two [23], and by Rips and Tent in characteristic zero [24]. However, these groups are not of finite Morley rank. It is not known if non-split sharply 2-transitive groups of finite Morley rank exist.

The Algebraicity Conjecture by Cherlin and Zilber states that an infinite simple group of finite Morley rank should be an algebraic group over an algebraically closed field. This is known for groups of Morley rank up to three. Cherlin classified connected groups of Morley rank at most 3 up to the existence of a bad group. Frécon very recently showed that these bad groups of Morley rank 3 do not exist [12] and completed Cherlin's classification. Epstein and Nesin showed in [11] that the Algebraicity Conjecture would imply that Frobenius groups of finite Morley rank split. Since sharply 2-transitive groups are Frobenius groups, sharply 2-transitive groups of finite Morley rank can be considered a test case for the Algebraicity Conjecture. If the Morley rank of a sharply 2-transitive group is at most 4, then it is known that the group must be standard.

Recent results by Altınel, Berkman, and Wagner [3] show that any infinite sharply 2-transitive group of finite Morley rank and characteristic 2 is split and that any infinite split sharply 2-transitive group of finite Morley rank of characteristic different from 2 is of the form $\mathrm{AGL}_1(K)$ for some algebraically closed field K.

If G is an infinite non-split sharply 2-transitive group of finite Morley rank such that $\mathrm{char}(G) \neq 2$, then G admits a point-line geometry on the set of its involutions which has been studied by Borovik and Nesin in Section 11.4 of [5]. We show that G must be simple if the lines in this geometry are strongly minimal. Moreover, we show that this geometry cannot contain a proper projective plane.

This observation about planes is the starting point of this work. We use the geometry to prove new rank inequalities for G. These rank inequalities then imply:

Theorem. *A sharply 2-transitive group of Morley rank* 6 *is split and hence of the form* $\mathrm{AGL}_1(K)$ *for an algebraically closed field* K *of Morley rank 3.*

This result also holds true if $\mathrm{char}(G) = 2$. Our geometric arguments are similar to those used by Frécon in [12] to show that there is no bad group of Morley rank 3.

We consider *generic projective planes* which generalize proper projective planes. Our proof consists of the following two parts:

(a) Show that a sharply 2-transitive group of finite Morley rank and characteristic $\neq 2$ cannot contain a generic projective plane.

(b) Find such a plane in certain rank configurations.

This outline is remarkably similar to the outline of Frécon's proof. However, the two parts are proved differently. Part (a) relies on a generalization of Bachman's theorem: We show that if $H \leq G$ is a definable subgroup, then $H \cap J$ cannot be a generic projective plane. To find a generic projective plane in (b), we utilize properties of the product map $J \times J \times J \to J^3$. The role of this map in our proof is similar to the role of the commutator map in Frécon's proof.

8. Preliminaries

8.1. Sharply 2-transitive groups

A permutation group G acting on a set X, $|X| \geq 2$, is called *sharply 2-transitive* if it acts regularly on pairs of distinct points, or, equivalently, if G acts transitively on X and for each $x \in X$ the point stabilizer G_x acts regularly on $X \setminus \{x\}$. For two distinct elements $x, y \in X$ the unique $g \in G$ such that $(x, y)^g = (y, x)$ is an involution. Hence the set J of involutions in G is non-empty and forms a conjugacy class. We put $J^2 = \{ij : i, j \in J\}$ and call the elements of J^2 *translations* extending the terminology used in the standard examples of sharply 2-transitive groups.

The (permutation) characteristic of a group G acting sharply 2-transitively on a set X is defined as follows: put $\mathrm{char}(G) = 2$ if and only if involutions have no fixed points. If involutions have a (necessarily unique) fixed point, the G-equivariant bijection $i \mapsto \mathrm{fix}(i)$ allows us to identify the given action of G on X with the conjugation action of G on J. Thus in this case, the nontrivial translations also form a single conjugacy class. We put $\mathrm{char}(G) = p$ (or 0) if translations have order p (or infinite order, respectively). For standard examples this definition of characteristic agrees with the characteristic of the field.

The following are well-known properties of sharply 2-transitive groups:

Remark 8.1.1. Let G be a sharply 2-transitive group of characteristic $\mathrm{char}(G) \neq 2$.

(a) $\mathrm{Cen}(i)$ acts regularly on $J \setminus \{i\}$,

(b) the set J acts regularly on J, i.e. for any two involutions $i, j \in J$ there is a unique involution $k \in J$ such that $i^k = j$, and

(c) $J^2 \cap \mathrm{Cen}(i) = \{1\}$ for all $i \in J$.

In particular, a nontrivial translation does not have a fixed point.

The crucial criterion for the splitting of a sharply 2-transitive group is the following [18]:

Theorem 8.1.2. *A sharply 2-transitive group G splits if and only if the set of translations J^2 is a subgroup of G (and in that case, J^2 must in fact be abelian).*

Since we aim to show that sharply 2-transitive groups of finite Morley rank are necessarily split, we will be focusing on the failure of J^2 being a subgroup. By Theorem 3.7 of [15] the group G is split if and only if $iJ = J^2$ for all $i \in J$. It then follows from Remark 8.1.1 that:

Proposition 8.1.3. *If G is split, then $G = iJ \rtimes \mathrm{Cen}(i)$ for any $i \in J$.*

8.2. Groups of finite Morley rank

We assume that the reader is familiar with groups of finite Morley rank and we will give a quick overview about the notions and tools that we will use. A detailed introduction to the topic can be found in [21] and [5]. We will denote Morley rank by MR and Morley degree by MD.

8.2.1. Zilber's Indecomposability Theorem

Definition 8.2.1. A definable subset A of a group G is *indecomposable* if for every definable subgroup $H \leq G$ the cardinality

$$|\{aH : a \in A\}|$$

is either 1 or infinite.

In many cases it suffices to check indecomposability for a smaller family of subgroups:

Proposition 8.2.2. *Let G be a stable group and suppose S is a definable group of automorphisms of G. If $A \subset G$ is a definable subset which is normalized by S, then A is indecomposable if Definition 8.2.1 is satisfied for all S-normal definable subgroups $H \leq G$.*

Theorem 8.2.3 (Zilber's Indecomposability Theorem)**.** *Let G be a group of finite Morley rank and let $A_i, i \in I$, be a family of indecomposable definable subsets such that $1 \in A_i$ for all $i \in I$. Then the group*

$$H = \langle \bigcup \{A_i : i \in I\} \rangle$$

is definable and connected. In fact, there are $i_1, \ldots i_m \in I$, $m \leq \mathrm{MR}(H)$, such that

$$H = (A_{i_1} \cdots A_{i_m})^2.$$

Remark 8.2.4. The proof of Theorem 8.2.3 shows that we have $H = (A_{i_1} \cdots A_{i_m})^2$ whenever $A_{i_1} \cdots A_{i_m}$ has maximal rank among finite products of the A_i. In that case $\mathrm{MR}(H) = \mathrm{MR}(A_{i_1} \cdots A_{i_m})$.

8.2.2. Definable group actions

For definable sets X and Y, we write $X \approx Y$ if and only if $\mathrm{MR}(X \Delta Y) < \mathrm{MR}(X)$. Then we have

$$X \approx Y \iff (\mathrm{MR}, \mathrm{MD})(X) = (\mathrm{MR}, \mathrm{MD})(X \cap Y) = (\mathrm{MR}, \mathrm{MD})(Y)$$

and hence $\approx$ defines an equivalence relation on definable sets.

If G is a group of finite Morley rank and $X \subseteq G$ is a definable subset, then

$$N_G^{\approx}(X) = \{g \in G : X^g \approx X\}$$

is a definable subgroup of G.

We will use the following result by Wagner:

Proposition 8.2.5 (Lemma 4.3 of [35]). *Let G be a group acting definably on a set X in an ω-stable structure. Let Y be a definable subset of X such that $gY \approx Y$ for all $g \in G$. Then there is a G-invariant $Z \subseteq X$ such that $Z \approx Y$.*

8.2.3. Groups of small rank

By a result of Reineke connected groups of Morley rank 1 are abelian. Groups of Morley rank at most 3 have been studied by Cherlin in [6]. He classified them up to the possible existence of a bad group of Morley rank 3. It was very recently shown by Frécon [12] that these bad groups do not exist. We obtain the following description of groups of small rank:

Let G be a connected group of finite Morley rank.

(a) If $\mathrm{MR}(G) = 1$, then G is abelian.

(b) If $\mathrm{MR}(G) = 2$, then G is solvable.

(c) If $\mathrm{MR}(G) = 3$, then G is solvable or $G \cong \mathrm{PSL}_2(K)$ or $G \cong \mathrm{SL}_2(K)$ where K is an algebraically closed field.

8.3. Bachmann's theorem

The following form of Bachmann's theorem is due to Schröder [25] (see also sections 8.2 and 8.3 in [5]).

Theorem 8.3.1 (Bachmann). *Suppose the set J of all involutions of a group G admits the structure of a projective plane such that three involutions i, j and k are collinear if and only if their product ijk is an involution. Then the subgroup $\langle J \rangle$ is isomorphic to $\mathrm{SO}_3(K, f)$ for some G-interpretable field K of characteristic $\neq 2$ and a nonisotropic quadratic form f on K^3.*

Borovik and Nesin proved the following:

Theorem 8.3.2 (Theorem 8.18 of [5]). *The conditions in Theorem 8.3.1 cannot be satisfied by a group of finite Morley rank.*

9. A point-line geometry

Let G be a sharply 2-transitive group of characteristic $\mathrm{char}(G) \neq 2$ and let J be the set of involutions. If commuting is transitive on the set of non-trivial translations in J^2, there is a well-behaved point-line geometry first defined by Schröder [25] following ideas of Bachmann [4]. We follow the construction in Section 11 of [5] although we explicitly define lines as subsets of J.

9.1. Points and lines

The equivalent conditions in the following lemma can be viewed as *geometricity conditions*. They will allow us to define the point-line geometry.

Lemma 9.1.1. *If* $\mathrm{char}(G) \neq 2$*, the following conditions are equivalent:*

(a) Commuting is transitive on $J^2 \setminus \{1\}$*, i.e.* $[x, y] = 1$ *defines an equivalence relation on* $J^2 \setminus \{1\}$*.*

(b) $iJ \cap kJ$ *is uniquely 2-divisible for all involutions* $i \neq k \in J$*.*

(c) $\mathrm{Cen}(ik) = iJ \cap kJ$ *is abelian and is inverted by* k *for all* $i \neq k \in J$*.*

(d) The set $\{\mathrm{Cen}(\sigma) \setminus \{1\} : \sigma \in J^2 \setminus \{1\}\}$ *forms a partition of* $J^2 \setminus \{1\}$*.*

Proof. (a) ⇒ (b): Note that since $(ij)^2 = ii^j \in iJ$ every element of iJ has a unique square-root in iJ. Let $\tau \in iJ \cap kJ$. By assumption the group

$$A = \langle \mathrm{Cen}(\tau) \cap J^2 \rangle \leq \mathrm{Cen}(\tau)$$

is abelian. Moreover, $A \cap J = \emptyset$ by Remark 8.1.1. Hence the squaring map is an injective group homomorphism from A to A.

There is $\sigma_i \in iJ$ such that $\sigma_i^2 = \tau$ and therefore $\sigma_i \in \mathrm{Cen}(\tau) \cap iJ$ because commuting is transitive. Similarly we find $\sigma_k \in \mathrm{Cen}(\tau) \cap kJ$ such that $\sigma_k^2 = \tau$. Since the squaring map is injective, it follows that $\sigma_i = \sigma_k \in iJ \cap kJ$. Therefore $iJ \cap kJ$ is uniquely 2-divisible.

(b) ⇒ (c) is contained in Lemma 11.50 iv of [5].

(c) ⇒ (d) and (d) ⇒ (a) are obvious. □

Clearly, these conditions are satisfied in split sharply 2-transitive groups by Theorem 8.1.2. Furthermore, by Lemma 11.50 of [5], these conditions are automatically satisfied whenever $\mathrm{char}(G) = p \neq 0, 2$ or in case G satisfies the descending chain condition for centralizers and hence in particular if G has finite Morley rank. On the other hand, the examples constructed by Rips, Segev, and Tent [23] (see also [33]) show that in characteristic 2 these conditions need not be satisfied. The non-split examples in characteristic 0 constructed by Rips and Tent [24] satisfy the assumptions and it is an open question whether non-split sharply 2-transitive groups exist in characteristic 0 which fail to satisfy these conditions.

If any of the conditions of Lemma 9.1.1 is satisfied, we obtain a point-line geometry as follows: the points of this geometry are the involutions of G. Given two points $i \neq j \in J$, we set

$$\ell_{ij} = \{k \in J : ij \in kJ\}$$

to be the (unique) line containing i and j. By Lemma 9.1.1 we have $ij \in kJ$ if and only if $(ij)^k = (ij)^{-1} = ji$. Moreover, $(ij)^k = ji$ if and only if $k \in i\mathrm{Cen}(ij)$. Therefore we have

$$\ell_{ij} = \{k \in J : ij \in kJ\} = i\ \mathrm{Cen}(ij) = \{k \in J : (ij)^k = ji\}.$$

If $u \neq v$ are contained in ℓ_{ij}, then

$$ij \in uJ \cap vJ = \mathrm{Cen}(uv)$$

and hence $\mathrm{Cen}(uv) = \mathrm{Cen}(ij)$ by Lemma 9.1.1.

This implies that the point-line geometry is well-behaved: any two points are contained in a unique line and (hence) any two lines intersect in at most one point.

If G satisfies the geometricity conditions, then G contains split sharply 2-transitive subgroups:

Proposition 9.1.2 (Theorem 11.51 of [5])**.** *Suppose* $\mathrm{char}(G) \neq 2$ *and suppose that* G *satisfies the conditions in Lemma 9.1.1. Let* i *and* j *be two distinct involutions. Then*

$$N_G(\mathrm{Cen}(ij)) = \mathrm{Cen}(ij) \rtimes N_{\mathrm{Cen}(i)}(\mathrm{Cen}(ij))$$

is split sharply 2-transitive.

In that case, ℓ_{ij} is the set of involutions in $N_G(\mathrm{Cen}(ij)) = \mathrm{Cen}(ij) \rtimes N_{\mathrm{Cen}(i)}(\mathrm{Cen}(ij))$. Also note that

$$i\ell_{ij} = \ell_{ij}^2 = \mathrm{Cen}(ij).$$

9.2. Projective planes

We first observe that the geometry associated to such a group G does not contain a proper projective plane.

Lemma 9.2.1. *Suppose* $\mathrm{char}(G) \neq 2$ *and suppose that* G *satisfies the conditions in Lemma 9.1.1. Let* $H \subseteq J^2$ *be a subgroup of* G *which is uniquely 2-divisible and normalized by an involution* $i \in J$*. Then* $H = \mathrm{Cen}(\sigma)$ *for some* $\sigma \in J^2 \setminus \{1\}$*.*

Proof. H is uniquely 2-divisible and i acts as an involutionary automorphism without fixed points. Neumann showed in [18] that such a group is abelian and hence H must be contained in the centralizer of some translation. □

Proposition 9.2.2. *Suppose* $\operatorname{char}(G) \neq 2$ *and suppose that* G *satisfies the conditions in Lemma 9.1.1. There is no proper projective plane* $X \subseteq J$. *I.e. if* $X \subseteq J$ *satisfies*

(a) $\forall i \neq j \in X : \ell_{ij} \subseteq X$, *and*

(b) if λ *and* δ *are lines contained in* X *then* $\lambda \cap \delta \neq \emptyset$,

then X *contains at most one line.*

Proof. Suppose $X \subseteq J$ satisfies (a) and (b). Take $\sigma, \tau \in X^2 \setminus \{1\}$ and let i be a point in $\ell_\sigma \cap \ell_\tau$. We may write $\sigma = ai, \tau = ib$ for some $a \in \ell_\sigma, b \in \ell_\tau$. Then $\sigma\tau = ab \in X^2$. Therefore X^2 is closed under multiplication and thus must be a subgroup of G. Moreover, X^2 is uniquely 2-divisible since it is a union of centralizers of translations.

Each $j \in X$ acts on X^2 as an involutionary automorphism without fixed points. By the previous lemma $X^2 \leq \operatorname{Cen}(\sigma)$ and hence $X \subseteq \ell_\sigma$. □

Remark 9.2.3. The non-existence of a proper projective plane in Proposition 9.2.2 can also be seen as an instance of Bachmann's theorem: If $X \subseteq J$ is a proper projective plane, then $N_G(X) \cap J = X$ and hence Theorem 8.3.1 can be applied to $N_G(X)$. Therefore $\langle X \rangle$ must be isomorphic to $\mathrm{SO}_3(K, f)$ for a field K of characteristic $\neq 2$ and a nonisotropic quadratic form f on K^3. Such a group would contain commuting involutions and thus cannot be a subgroup of G.

10. Sharply 2-transitive groups of finite Morley rank

Let G be a non-split sharply 2-transitive group of finite Morley rank with $\mathrm{char}(G) \neq 2$ and let J denote the set of involutions in G. By Lemma 11.50 of [5], $iJ \cap jJ$ is uniquely 2-divisible for all $i \neq j \in J$ and so we can use the point-line geometry introduced in the previous section. We set $n = \mathrm{MR}(J)$ and $k = \mathrm{MR}(\mathrm{Cen}(ij))$ for involutions $i \neq j$. Note that k does not depend on the choice of i and j.

Since G acts sharply 2-transitively on J, it is easy to see that $\mathrm{MR}(G) = 2n$ and $\mathrm{MR}(J^2) = 2n - k$. Moreover, G and $\mathrm{Cen}(ij)$ have Morley degree 1 by Lemma 11.60 of [5].

Altınel, Berkman, and Wagner [3] showed that split sharply 2-transitive groups of finite Morley rank of characteristic $\neq 2$ are standard. In particular,

$$N_G(\mathrm{Cen}(ij)) = \mathrm{Cen}(ij) \rtimes N_{\mathrm{Cen}(i)}(\mathrm{Cen}(ij))$$

is standard, i.e. of the form $\mathrm{AGL}_1(K)$ for an algebraically closed field K. This implies the following:

Lemma 10.0.1. *$N_G(\mathrm{Cen}(ij))$ is planar, i.e.*

$$N_G(\mathrm{Cen}(ij)) = \mathrm{Cen}(ij) \cup \bigcup_{t \in \ell_{ij}} N_{\mathrm{Cen}(t)}(\mathrm{Cen}(ij)).$$

Proof. Theorem 7.2 and Theorem 7.3 in [15]. □

We will need the following lemma about lines:

Lemma 10.0.2. *Let λ be a line.*

(a) Suppose $\lambda^i = \lambda^j$ for involutions $i \neq j$. Then $i, j \in \lambda$.

(b) Suppose $\lambda \cap \lambda^i \neq \emptyset$ for some involution i. Then $i \in \lambda$.

Proof. Part (a) is contained in the proof of Theorem 11.71 in [5], part (b) is Lemma 11.59 in [5]. Since our definition of lines is slightly different from the one given in [5], we include proofs.

(a) If $\lambda^i = \lambda^j$, then $ij \in N_G(\lambda)$ and hence $ij \in N_G(\lambda^2)$. Now $\lambda^2 = \mathrm{Cen}(\sigma)$ for some $\sigma \in J^2 \setminus \{1\}$ such that $\lambda = \ell_\sigma$. Fix $s \in \lambda$. The group $N_G(\mathrm{Cen}(\sigma)) = \mathrm{Cen}(\sigma) \rtimes N_{\mathrm{Cen}(s)}(\mathrm{Cen}(\sigma))$ is split sharply 2-transitive by Proposition 9.1.2. Hence

$$ij \in N_G(\mathrm{Cen}(\sigma)) \cap J^2 = \mathrm{Cen}(\sigma)$$

and therefore $i, j \in \ell_\sigma = \lambda$.

(b) We may assume $\lambda \neq \lambda^i$. Hence there must be a unique $j \in \lambda \cap \lambda^i$. But then j is fixed by i and by Lemma 8.1.1 (b) we have $i = j \in \lambda$. □

Lemma 10.0.3. *Let $H \leq G$ be a definable subgroup such that* $\mathrm{MR}(H \cap J) = 2k$ *and* $\mathrm{MD}(H \cap J) = 1$. *Then* $\mathrm{MR}(\{\lambda : \lambda \text{ is a line s.t. } \lambda \subseteq H \cap J\}) < 2k$.

Proof. This is proved in the same way as Proposition 11.71 of [5]. Put $Z = H \cap J$ and let Λ be the set of lines contained in Z. Since each $\lambda \in \Lambda$ has Morley rank $2k$ many preimages in $Z \times Z$, we have $\mathrm{MR}(\Lambda) \leq 2k$. Now assume $\mathrm{MR}(\Lambda) = 2k$. By the above argument we have $\mathrm{MD}(\Lambda) = 1$ since $\mathrm{MD}(Z) = 1$.

Let $\lambda \in \Lambda$ be a line. By Lemma 10.0.2 the family $(\lambda^i : i \in Z \setminus \lambda)$ consists of Morley rank 2k many lines which do not intersect λ. Hence the set $\{\delta \in \Lambda : \lambda \cap \delta = \emptyset\} \subseteq \Lambda$ is a generic subset of Λ.

We aim to find a line which intersects Morley rank 2k many lines contradicting $\mathrm{MD}(\Lambda) = 1$. For $x \in Z$ set $\Lambda_x = \{\lambda \in \Lambda : x \in \lambda\}$ and set $B(x) = \bigcup \Lambda_x \subseteq Z$. Note that $\mathrm{MR}(B(x)) = \mathrm{MR}(\Lambda_x) + k$ and hence $\mathrm{MR}(\Lambda_x) \leq k$ for all $x \in Z$. Since each $\lambda \in \Lambda$ contains Morley rank k many points and we assume $\mathrm{MR}(\Lambda) = 2k = \mathrm{MR}(H \cap J)$, we must have $\mathrm{MR}(\Lambda_x) = k$ for a generic set of $x \in Z$.

Fix $x_0 \in Z$ such that Λ_{x_0} has Morley rank 2k. Then $B(x_0) \subseteq Z$ is generic and hence $\mathrm{MR}(\Lambda_x) = k$ for a generic set of $x \in B(x_0)$. Since $B(x_0) = \bigcup \Lambda_{x_0}$, we can find a line $\lambda \in \Lambda_{x_0}$ such that $\mathrm{MR}(\Lambda_x) = k$ for a generic set of $x \in \lambda$. But then λ intersects Morley rank 2k many lines in Λ. □

10.1. Generic projective planes

We will need a more general version of Proposition 9.2.2. Therefore we need to consider generalizations of projective planes. For definable sets X and Y we write $X \approx Y$ if and only if $\mathrm{MR}(X \Delta Y) < \mathrm{MR}(X)$ (as explained in Section 8.2.2).

Definition 10.1.1. A definable subset $X \subseteq J$ is a *generic projective plane* if

(a) $\mathrm{MR}(X) = 2k$ and $\mathrm{MD}(X) = 1$, and

(b) $\mathrm{MR}(\Lambda_X) = 2k$ and $\mathrm{MD}(\Lambda_X) = 1$,

where Λ_X is the set of all lines $\lambda \subseteq J$ such that $\lambda \cap X \approx \lambda$.

Lemma 10.1.2. *Let $X \subseteq J$ be a definable set of Morley rank 2k and Morley degree 1. The following are equivalent:*

(a) X is a generic projective plane,

(b) $\mathrm{MR}(\Lambda_X) \geq 2k$,

(c) $\mathrm{MR}(\{\lambda \in \Lambda_X : x \in \lambda\}) = k$ *for a generic set of* $x \in X$.

Proof. Since $\mathrm{MR}(X) = 2k$ and each line in Λ_X contains Morley rank k many points in X, each point is contained in at most Morley rank k many lines in Λ_X. The lemma follows from easy counting arguments. □

Remark 10.1.3. Lemma 10.0.3 can be seen as a version of Bachmann's theorem for generic projective planes: Let H be as in the statement of Lemma 10.0.3. Bachmann's theorem and Theorem 8.3.2 imply that $H \cap J$ cannot be a proper projective plane. If we assume $\mathrm{MR}(\{\lambda : \lambda \text{ is a line s.t. } \lambda \subseteq H \cap J\}) \geq 2k$, then $H \cap J$ is a generic projective plane. Hence Lemma 10.0.3 can be restated as: If $H \leq G$ is a definable subgroup, then $H \cap J$ cannot be a generic projective plane.

Lemma 10.1.4. *Assume $X \subseteq J$ is a generic projective plane and let $Z \subseteq J$ be a definable subset such that $X \approx Z$. Then Z is a generic projective plane.*

Proof. For $x \in X$ put $\Lambda_x = \{\lambda \in \Lambda_X : x \in \lambda\}$. If $\mathrm{MR}(\Lambda_x) = k$, then $B(x) = \bigcup \Lambda_x \approx X$. In particular, $B(x) \approx Z$ for a generic set of $x \in X \cap Z$. If $B(x) \approx Z$, then $\Lambda_x \cap \Lambda_Z$ must have Morley rank k. Hence it follows from the previous lemma that Z must be a generic projective plane. □

Proposition 10.1.5. *G does not contain a generic projective plane $X \subseteq J$.*

Proof. Assume $X \subseteq J$ is a generic projective plane and put

$$H = N_G^{\approx}(X) = \{g \in G : X^g \approx X\}.$$

By Proposition 8.2.5 we can find $Z \subseteq J, Z \approx X$ such that $H \leq N_G(Z)$. If the set $\Lambda_x = \{\lambda \in \Lambda_X : x \in \lambda\}$ has Morley rank k, then $\bigcup_{\lambda \in \Lambda_x} \lambda \approx X$ and hence $x \in H$. Thus $X \cap H \subseteq X$ is generic and therefore we may assume $Z \subseteq H$. Since H normalizes Z, it follows from Lemma 8.1.1 (b) that Z must be generic in $H \cap J$. Hence we may assume $Z = H \cap J$.

Note that if λ is a line such that $\lambda \cap H \subseteq \lambda$ is generic, then $\lambda \subseteq H$. Each line contained in H has rank 2k many preimages in $Z \times Z$. Since X is a generic projective plane and $Z \approx X$, the previous lemma implies that Z is a generic projective plane and hence the set of all lines in H has rank 2k and degree 1. This contradicts Lemma 10.0.3. □

10.2. Products of involutions

Proposition 10.2.1. *(a) The set iJ is indecomposable for all $i \in J$.*

(b) $\langle J^2 \rangle$ is a definable connected subgroup. In particular, there is a bound m such that any $g \in \langle J^2 \rangle$ is a product of at most m translations.

(c) J^2 is not generic in $\langle J^2 \rangle$.

(d) $\mathrm{MR}(J^3) > \mathrm{MR}(J^2)$.

Proof. (a) Fix an involution $i \in J$. The set iJ is normalized by $\mathrm{Cen}(i)$, hence it suffices to check indecomposability for $\mathrm{Cen}(i)$-normal subgroups. If $H \leq G$ is a $\mathrm{Cen}(i)$-normal subgroup of G, then either $\mathrm{Cen}(ij) \leq H$ for all $j \in J \setminus \{i\}$ or $H \cap \mathrm{Cen}(ij)$ has infinite index in $\mathrm{Cen}(ij)$ for all $j \in J \setminus \{i\}$. Therefore the set $iJ = \bigcup_{j \in J \setminus \{i\}} \mathrm{Cen}(ij)$ is indecomposable.

(b) Since $\langle J^2 \rangle = \langle iJ \rangle$, this follows from Zilber's indecomposability theorem using (a).

(c) Fix two involutions $i \neq j$. We claim that

$$\mathrm{MR}(\{\tau \in J^2 : i^\tau = j\}) \geq n - k.$$

To see this note that for any $r \in J$ by Remark 8.1.1 there is a unique $s \in J$ such that $i^{rs} = j$. Hence the set $T_{ij} = \{(r, s) \colon i^{rs} = j\} \subset J \times J$ has Morley rank n. The equivalence classes on T_{ij} given by $(r, s) \equiv (r', s')$ if and only if $rs = r's'$ have Morley rank at most k. Hence the claim follows.

In particular, for any $\sigma \in J^2 \setminus \{1\}$ and $i \in J$ the set $\Sigma_i = \{\tau \in J^2 : i^\sigma = i^\tau\}$ has Morley rank at least $n - k$. Since for $i \neq j \in J$ the sets Σ_i and Σ_j intersect only in σ, it follows that $\{\tau \in J^2 : \exists i \in J : i^\sigma = i^\tau\}$ has Morley rank (at least) $2n - k = \mathrm{MR}(J^2)$. Hence for every $\sigma \in J^2 \setminus \{1\}$ the set

$$\{\tau \in J^2 : \sigma\tau^{-1} \text{ has a fixed point}\}$$

is a generic subset of J^2. Since translations do not have fixed points, it follows that

$$\mathrm{MR}(\sigma J^2 \cap J^2) < 2n - k.$$

Thus, J^2 is not generic in $\langle J^2 \rangle$.

(d) Suppose $\mathrm{MR}(J^2) = \mathrm{MR}(J^3)$. Since $(iJ)^2 = J^i J = J^2$ and $(iJ)^3 = iJ^3$ we have $\mathrm{MR}((iJ)^2) = \mathrm{MR}((iJ)^3)$ and by (the proof of) Zilber's indecomposability theorem we get $\mathrm{MR}(\langle iJ \rangle) = \mathrm{MR}((iJ)^2)$. In particular, $J^2 \subseteq \langle iJ \rangle$ is a generic subset contradicting (c). □

Remark 10.2.2. The non-split examples of sharply 2-transitive groups of characteristic 0 constructed in [24] contain unbounded products of translations. By Proposition 10.2.1 (b) they cannot have finite Morley rank.

Corollary 10.2.3. *If the lines are strongly minimal, then G is simple.*

Proof. Let $N \neq 1$ be a normal subgroup of G. Fix an involution i and an element $g \in N \setminus \mathrm{Cen}(i)$. Then $ii^g = (g^{-1})^i g \in N$ and therefore $N \cap J^2 \neq 1$. Since $J^2 \setminus \{1\}$ is a conjugacy class, it follows that $J^2 \subseteq N$. If $k = 1$ then N must be generic since $\mathrm{MR}(J^3) > \mathrm{MR}(J^2) = 2n - 1$ and $iJ^3 \subseteq N$. Therefore $N = G$. □

10.3. Rank inequalities

By Proposition 11.71 of [5] we have the following inequality:

Proposition 10.3.1. $0 < 2k < n$.

We will improve this rank inequality. This will show that certain rank configurations (i.e. combinations of n and k) cannot appear.

Theorem 10.3.2. *Set* $l = \mathrm{MR}(J^3) - \mathrm{MR}(J^2) \geq 1$. *Then* $n > 2k + l$.

Proof. Consider the multiplication map $\mu : J \times J \times J \to J^3$. For $\alpha \in J^3$ we set X_α to be the set

$$X_\alpha = \{i \in J : \exists r, s \in J \; irs = \alpha\}.$$

Equivalently, $X_\alpha = \{i \in J : i\alpha \in J^2\}$ is the set of all involutions i such that $i\alpha$ is a translation.

Since $\mathrm{MR}(J^3) = 2n-k+l$ there must be some $\alpha \in J^3 \setminus J$ such that $\mu^{-1}(\alpha) \leq n+k-l$. Set $X = X_\alpha$ for such an $\alpha \in J^3 \setminus J$. If $irs = \alpha$, then $\mathrm{MR}(\{j \in J : rs \in jJ\}) = k$ and hence $\mathrm{MR}(\mu^{-1}(\alpha)) = \mathrm{MR}(X) + k$. Therefore we have $\mathrm{MR}(X) \leq n - l$.

We now aim to show that $2k < \mathrm{MR}(X)$. If $irs = \alpha$ and $v \in \ell_{rs}$, then $\ell_{iv} \subseteq X$: We have $irs = ivu$ for some $u \in \ell_{rs}$ and moreover for each $p \in \ell_{iv}$ there is some $q \in \ell_{iv}$ such that $pq = iv$ and hence $pqu = ivu = irs = \alpha$. Hence each point in X is contained in Morley rank k many lines which are contained in X. Hence X must have Morley rank at least $2k$.

Now assume $\mathrm{MR}(X) = 2k$ and set $m = \mathrm{MD}(X)$. Let Λ be the set of lines obtained as above. For each $x \in X$ the set $\{\lambda \in \Lambda : x \in \lambda\}$ has Morley rank k and Morley degree 1. Write X as the disjoint union of definable sets $X_1, \ldots X_m$, each of Morley rank $2k$ and Morley degree 1. For $a = 1, \ldots m$ let $\Lambda_a \subseteq \Lambda$ be the set $\Lambda_a = \{\lambda \in \Lambda : \lambda \cap X_a \approx \lambda\}$. Since each $x \in X$ is contained in Morley rank k many lines in Λ and each line in Λ contains Morley rank k many points, the set Λ must have Morley rank $2k$. Hence there is b such that Λ_b has Morley rank $2k$. Now X_b is a generic projective plane. This contradicts Proposition 10.1.5.

Therefore $2k < \mathrm{MR}(X) \leq n - l$ and hence $2k + l < n$. □

10.4. Sharply 2-transitive groups of Morley rank 6

As an immediate consequence of the improved rank inequality, sharply 2-transitive groups of Morley rank 6 and characteristic $\neq 2$ must be split (and hence standard by [3]). The description of the structure of groups of small Morley rank in Section 8.2.3 will also imply this in characteristic 2.

Theorem 10.4.1. *Let* G *be a sharply 2-transitive group of any characteristic and assume* $\mathrm{MR}(G) = 6$. *Then* $G = \mathrm{AGL}_1(K)$ *for an algebraically closed field* K *of Morley rank 3.*

Proof. If $\mathrm{char}(G) \neq 2$, then this follows from Theorem 10.3.2. Now assume $\mathrm{char}(G) = 2$. Then G is split by [3] and the point stabilizers have Morley rank 3 and are connected (by Lemma 11.60 of [5]). Since they do not contain involutions they must be solvable by Section 8.2.3. By Corollary 11.66 of [5] a split sharply 2-transitive group of finite Morley rank where the point stabilizer contains an infinite normal solvable subgroup must be standard. □

Bibliography

[1] Eran Alouf. On dp-minimal expansions of the integers, 2020. arXiv:2001.11480 [math.LO].

[2] Eran Alouf and Christian D'Elbée. A new dp-minimal expansion of the integers. *The Journal of Symbolic Logic*, 84(2):632–663, 2019.

[3] Tuna Altinel, Ayse Berkman, and Frank Olaf Wagner. Sharply 2-transitive groups of finite Morley rank, 2018. arXiv:1811.10854 [math.LO].

[4] Friedrich Bachmann. *Aufbau der Geometrie aus dem Spiegelungsbegriff*, volume 96 of *Grundlehren der mathematischen Wissenschaften*. Springer-Verlag Berlin Heidelberg, 1959.

[5] Alexandre Borovik and Ali Nesin. *Groups of Finite Morley Rank (Oxford Logic Guides)*. Clarendon Press, 1995.

[6] Gregory Cherlin. Groups of small Morley rank. *Annals of Mathematical Logic*, 17(1):1 – 28, 1979.

[7] Tim Clausen and Katrin Tent. Some model theory of profinite groups. *Lectures in Model Theory, Münster Lectures in Mathematics, EMS Publishing*, 2016.

[8] Gabriel Conant. There are no intermediate structures between the group of integers and presburger arithmetic. *The Journal of Symbolic Logic*, 83(1):187–207, 2018.

[9] Gabriel Conant and Anand Pillay. Stable groups and expansions of $(\mathbb{Z}, +, 0)$. *Fundamenta Mathematicae*, 01 2016.

[10] J. D. Dixon, M. P. F. Du Sautoy, A. Mann, and D. Segal. *Analytic Pro-P Groups*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2 edition, 1999.

[11] David Epstein and Ali Nesin. On Frobenius groups of finite morley rank ii. In *Automorphisms of First-Order Structures*, pages 341–350. Clarendon Press, 1994.

[12] Olivier Frécon. Simple groups of Morley rank 3 are algebraic. *Journal of the American Mathematical Society*, 31:1, 10 2017.

[13] Patrick Helbig. On small profinite groups. *Journal of Group Theory*, 20(5), 2017.

[14] Moshe Jarden and Alexander Lubotzky. Elementary equivalence of profinite groups. *Bulletin of The London Mathematical Society*, 40:887–896, 07 2008.

[15] William Kerby. *On infinite sharply multiply transitive groups.* Vandenhoeck & Ruprecht, 1974.

[16] Franz-Viktor Kuhlmann and Salma Kuhlmann. Ax-Kochen-Ershov principles for valued and ordered vector spaces. In W. Charles Holland, editor, *Ordered Algebraic Structures*, pages 237–259, Dordrecht, 1997. Kluwer.

[17] Fares Maalouf. Espaces vectoriels c-minimaux. *J. Symbolic Logic*, 75(2):741–758, 06 2010.

[18] B. H. Neumann. On the commutativity of addition. *Journal of the London Mathematical Society*, s1-15(3):203–208, 1940.

[19] Hanna Neumann. *Varieties of Groups*, volume 37 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 2. Folge.* Springer, first edition, 1967.

[20] Daniel Palacín and Rizos Sklinos. On superstable expansions of free abelian groups. *Notre Dame J. Formal Log.*, 59:157–169, 2018.

[21] Bruno Poizat. *Stable Groups*, volume 87 of *Mathematical Surveys and Monographs.* American Mathematical Society, 2001.

[22] Luis Ribes and Pavel Zalesskii. *Profinite Groups*, volume 40 of *A Series of Modern Surveys in Mathematics.* Springer, second edition, 2000.

[23] Eliyahu Rips, Yoav Segev, and Katrin Tent. A sharply 2-transitive group without a non-trivial abelian normal subgroup. *Journal of the European Mathematical Society*, 19:2895–2910, 06 2014.

[24] Eliyahu Rips and Katrin Tent. Sharply 2-transitive groups in characteristic 0. *Journal für die reine und angewandte Mathematik (Crelles Journal)*, 2019:227–238, 04 2016.

[25] Eberhard M. Schröder. Eine Gruppentheoretisch-Geometrische Kennzeichnung der Projektiv-Metrischen Geometrien. *Journal of Geometry*, 18(1):57–69, Dec 1982.

[26] Pierre Simon. On dp-minimal ordered structures. *J. Symb. Log.*, 76:448–460, 2011.

[27] Pierre Simon. Distal and non-distal nip theories. *Ann. Pure Appl. Log.*, 164:294–318, 2013.

[28] Pierre Simon. *A Guide to NIP Theories.* Cambridge, 2015.

[29] Patrick Simonetta. An example of a c-minimal group which is not abelian-by-finite. *Proceedings of the American Mathematical Society*, 131, 12 2003.

[30] M.G. Smith and John Wilson. On subgroups of finite index in compact hausdorff groups. *Archiv der Mathematik*, 80:123–129, 04 2003.

[31] Katrin Tent and Dugald Macpherson. Profinite groups with NIP theory and p-adic analytic groups. *Bull. Lond. Math. Soc.*, 48(6):1037–1049, 2016.

[32] Katrin Tent and Martin Ziegler. *A Course in Model Theory.* Lecture Notes in Logic. Cambridge University Press, 2012.

[33] Katrin Tent and Martin Ziegler. Sharply 2-transitive groups. *Adv. Geom.*, 16(1):131–134, 2016.

[34] Minh Tran and Erik Walsberg. A family of dp-minimal expansions of $(\mathbb{Z};+)$, 2017. arXiv:1711.04390 [math.LO].

[35] Frank Wagner. Bad groups, 2017. arXiv:1703.01764 [math.LO].

[36] Erik Walsberg. Dp-minimal expansions of $(\mathbb{Z},+)$ via dense pairs via Mordell-Lang, 2020. arXiv:2004.06847 [math.LO].

[37] J.S. Wilson. *Profinite Groups.* Clarendon Press, 1998.

[38] E. I. Zelmanov. On periodic compact groups. *Israel Journal of Mathematics*, 77:83–95, 1992.