On some algebraic properties of p-adic analytic pro-p groups

Inaugural-Dissertation

zur Erlangung des Doktorgrades
der Mathematisch-Naturwissenschaftlichen Fakultät
der Heinrich-Heine-Universität Düsseldorf

vorgelegt von

Martina Conte
aus Lucca

Düsseldorf, Oktober 2023

aus dem Mathematischen Institut
der Heinrich-Heine-Universität Düsseldorf

Gedruckt mit der Genehmigung der
Mathematisch-Naturwissenschaftlichen Fakultät der
Heinrich-Heine-Universität Düsseldorf

Berichterstatter:

1. Prof. Dr. Benjamin Klopsch

2. Prof. Dr. H. Dugald Macpherson

Tag der mündlichen Prüfung: 24.01.2024

Abstract

This thesis deals with algebraic properties of profinite groups. It is divided into two parts, corresponding to two distinct topics. The first part is devoted to proving the finite axiomatizability of the rank and the dimension of pro-π groups, while the second part is about the unique product property for pro-p groups.

Recently, Nies, Segal and Tent investigated finite axiomatizability in the realm of profinite groups. They prove that the rank of a p-adic analytic pro-p group is finitely axiomatizable up to an error term. It is therefore natural to ask whether the rank of a pro-p group can be completely determined by a single first-order sentence. Here we give a positive answer to this question. More generally, given a finite set of primes π, we consider the class of pro-π groups and we prove that the rank of a pro-π group, as well as the ranks and dimensions of its Sylow pro-p subgroups, are finitely axiomatizable in the first-order language of groups. Moreover, we show that this result is optimal in the class of profinite groups. The result is first proved for the profinite groups in the class $\mathcal{C}_\pi$ of pronilpotent groups whose order is divisible only by primes in π and it is subsequently extended to pro-π groups. Its proof is based on group-theoretic results that are of independent interest.

The second part of the thesis concerns the unique product property for pro-p groups. A group G has the unique product property, or equivalently G is a unique product group, if, given two non-empty, finite subsets A and B of G, there always exists at least one element g of G that can be written in a unique way as a product $g = ab$ with $a \in A$ and $b \in B$. The unique product property was introduced in 1964 by Rudin and Schneider in connection with Kaplansky's conjecture on zero divisors in group rings. It is indeed not difficult to show that a unique product group satisfies this conjecture. Recently, Craig and Linnell conjectured that uniform pro-p groups possess the unique product property. By extending one of their results we prove that the conjecture holds true for virtually soluble saturable pro-p groups. A well-known property that is stronger than the unique product property is local indicability. A group is locally indicable if each of its non-trivial finitely generated subgroups has infinite abelianisation. We start to study local indicability for soluble profinite groups, producing some results that relate being locally indicable to a topological version of local indicability. Another property related to local indicability and the unique product property is orderability. Indeed, one can show that a bi-orderable group is locally indicable. We give an elementary proof of the fact that insoluble pro-p groups of finite rank are not bi-orderable and we adapt one of the proofs that RAAGs are bi-orderable to show that also pro-p completions of RAAGs are bi-orderable, hence locally indicable.

Acknowledgements

First and foremost I thank my main advisor Benjamin Klopsch for his guidance and support during my PhD. I also thank my second advisor Holger Kammeyer, my mentor Marcus Zibrowius and my Postdoc tutor Pablo Cubides Kovacsics.
I am thankful to the second reviewer Dugald Macpherson for taking the time to read this thesis. I wish to extend my gratitude also to the other members of the committee. I wish to express my gratitude to all the members of the Mathematical Institute at HHU Düsseldorf for the nice and supportive atmosphere.
I am especially grateful to the GRK2240: Algebro-Geometric Methods in Algebra, Arithmetic and Topology funded by the DFG for the stimulating environment and the financial support.

Contents

Introduction

This thesis is about algebraic properties of profinite groups. Profinite groups are topological groups but it is natural to ask which purely algebraic properties they possess when considered as abstract groups, forgetting their topology. A groundbreaking result in this direction is the *strong completeness theorem* by Nikolov and Segal, that states that (topologically) finitely generated profinite groups are *strongly complete*, i.e., their open subgroups coincide with those of finite index. In other words, the topology of a finitely generated profinite group is already completely determined by the algebraic structure of the group. It can easily be seen that this does not hold true in general for non finitely generated profinite groups (see Section 1.2). Nikolov and Segal's theorem generalises a result of Serre, who proved that every finitely generated pro-p group is strongly complete and asked whether the same holds true for finitely generated profinite groups. The strong completeness theorem has numerous applications. For example, it is not difficult to see that a consequence of the theorem is that a homomorphism from a finitely generated profinite group to any profinite group is automatically continuous. The proof of the strong completeness theorem relies on results on the finite width of certain words proved by Nikolov and Segal. We recall here briefly the definition of width. Let w be a word in k variables and G a group. Consider the set

$$G_w := \{w(\mathbf{g})^{\pm 1} \mid \mathbf{g} \in G^{(k)}\}$$

of w-values in G. Given a set S and $m \in \mathbb{N}$ we denote by S^{*m} the set

$$\{s_1 s_2 \cdots s_m \mid s_i \in S\}$$

of products of m elements of S and by $\langle S \rangle$ the group generated by S. The *verbal subgroup* corresponding to w is defined as

$$w(G) := \langle G_w \rangle = \bigcup_{m \in \mathbb{N}} G_w^{*m}.$$

We say that the word w has *width* (more precisely, width at most) m in G if

$$w(G) = G_w^{*m},$$

for a fixed $m \in \mathbb{N}$. For example, in a d-generated pro-p group G, the commutator word has width d, i.e., every element of the commutator subgroup of G can be written as the product of d commutators ([Se], Theorem 4.1.5). Actually, it is even possible to give a concrete description of the commutator subgroup of a finitely generated pro-p group. Namely, if G is a pro-p group generated by elements $a_1, \ldots, a_d$, then

$$[G, G] = [a_1, G] \cdots [a_d, G]$$

(see [Se], Corollary 4.3.2). This result has many consequences in the theory of pro-p groups. For example, it is a fundamental ingredient for proving Serre's theorem on the strong completeness of finitely generated pro-p groups (see the exposition in [DDMS], Chapter 1). In the thesis we will also see that, as shown in [NST], such a description of the commutator subgroup allows to axiomatize with one first-order sentence the property that a finitely generated pro-p group has a certain minimal number of generators. We will also use the formula for the commutator subgroup of a finitely generated pro-p group more than once in our proofs in the course of this thesis.

The kind of profinite groups that we will mainly consider are pro-p groups and, among pro-p groups, we will mostly work with p-adic analytic pro-p groups. These are groups with a Lie structure but purely group-theoretic characterisations, proved mainly by Lubotzky, Mann, Dixon, du Sautoy and Segal building on previous work of Lazard. One of the characterisations is given in terms of the rank. Given a profinite group G, its *rank* is defined as the supremum of the minimal number of (topological) generators $\mathrm{d}(H)$, where H runs over the closed subgroups of G. Then the following holds.

Theorem 1 ([DDMS], Corollary 8.33)**.** *A pro-p group is p-adic analytic if and only if it has finite rank.*

Other characterisations are given in terms of powerful and uniform pro-p subgroups (see Section 1.3 for more details). Uniform pro-p groups can be defined as torsion-free powerful pro-p groups. In a way, they replaced Lazard's *p-saturable* groups as they are better suited for group-theoretic applications. It turns out that uniform pro-p groups form a proper subclass of saturable pro-p groups (see [K]). A characterisation of p-adic analytic pro-p groups in terms of uniform pro-p groups is the following.

Theorem 2 ([DDMS], Corollary 4.3)**.** *A pro-p group is p-adic analytic if and only if it has a uniform subgroup of finite index.*

A standard example of a uniform pro-p group is the first congruence subgroup $\mathrm{GL}_d^1(\mathbb{Z}_p)$ given by the set of matrices in $\mathrm{GL}_d(\mathbb{Z}_p)$ that are congruent to the identity modulo p, for p an odd prime. More generally, a pro-p group has a p-adic analytic structure if and only if it is isomorphic to a closed subgroup of a Sylow pro-p subgroup of $\mathrm{GL}_d(\mathbb{Z}_p)$ for some degree d (see [K1], Corollary 2.3).
In the first part of the thesis we will consider a more general class of profinite groups. Namely, given a finite set of primes π we will work with pro-π groups, i.e., inverse limits of finite groups whose order is divisible only by primes in π. The Sylow pro-p subgroups of a pro-π group of finite rank are p-adic analytic pro-p groups. An example of a pro-π group is given by $\mathrm{GL}_d(\mathbb{Z}_p)$. Moreover, we will show in Chapter 2 that pro-π groups of finite rank contain a finite index subgroup that is a direct product of p-adic analytic pro-p groups, where p runs over π (compare with the proof of Theorem 2.6.4).

The thesis is divided into two parts. The first part is devoted to the finite axiomatizability of the rank and the dimension of pro-π groups while the second part concerns the unique product property for pro-p groups.

Finite axiomatizability of the rank and the rank and dimension of a pro-π group. In [JL], Jarden and Lubotzky used results on the finite width

of certain words proved by Nikolov and Segal to show that finitely generated profinite groups are first-order rigid, i.e., completely determined, up to isomorphism, by their first-order theory. More recently, Nies, Segal and Tent started to investigate which profinite groups can be axiomatized by a *single* first-order sentence. Among the classes of groups that they consider is the class of p-adic analytic pro-p groups. Concerning their rank, they state the following result.

Proposition 3 ([NST], Proposition 5.1)**.** *For each positive integer r, there is a sentence $\rho_{p,r}$ in the language of groups such that, for a pro-p group G,*

$$\mathrm{rk}(G) \leq r \quad \Rightarrow \quad G \models \rho_{p,r} \quad \Rightarrow \quad \mathrm{rk}(G) \leq r(2 + \log_2(r)).$$

It is therefore natural to ask whether the rank of a p-adic analytic pro-p group can be axiomatized by a single first-order sentence in the language of groups. Moreover, one can also consider another fundamental invariant of p-adic analytic groups, their *dimension*, and ask the same question. In the first part of the thesis we give a positive answer to these questions. More generally, given a finite set of primes π, we consider pro-π groups and prove the following main result (see Theorem 2.6.4 and Corollary 2.7.2).

Theorem 4. *Let π be a finite set of primes and let r be a positive integer. Let $\mathbf{r} = (r_p)_{p\in\pi}$ and $\mathbf{d} = (d_p)_{p\in\pi}$ be two tuples in $\{0, \ldots, r\}$. There is a single first-order sentence $\sigma_{\pi,r,\mathbf{r},\mathbf{d}}$ in the language of groups such that for every pro-π group G the following are equivalent:*

1. *$\sigma_{\pi,r,\mathbf{r},\mathbf{d}}$ holds true in the group G;*
2. *G has rank r and, for each $p \in \pi$, the Sylow pro-p subgroups of G have rank r_p and dimension d_p.*

Moreover, we show that this result is optimal in the class of profinite groups. Indeed, for model-theoretic reasons, it turns out that the rank of a profinite group whose order is divisible by an infinite number of primes cannot be finitely axiomatizable (see Proposition 2.3.9).
We first prove Theorem 4 for pronilpotent groups whose order is divisible only by primes in π, i.e., direct products of pro-p groups, where p runs over the primes in π. We will call such groups $\mathcal{C}_\pi$ groups. In order to show the finite axiomatizability of the rank of $\mathcal{C}_\pi$ groups, we prove group-theoretic results that are also interesting on their own. In their more general form they can be stated as follows (see Theorem 2.6.1).

Theorem 5. *Let R be a positive integer. Suppose that the profinite group G has an open normal subgroup $F \trianglelefteq_{\mathrm{o}} G$ which is pronilpotent and such that each Sylow subgroup of F is powerful.*

1. *If $\mathrm{rk}_p(G) \leq R$ for some prime p, then*
$$\mathrm{rk}_p(G) = \mathrm{rk}_p\big(G/\Phi^{2R+1}(F)\big).$$
2. *If $\mathrm{rk}(G) \leq R$, then*
$$\mathrm{rk}(G) = \mathrm{rk}\big(G/\Phi^{2R+1}(F)\big).$$

Here $\mathrm{rk}_p(G)$ denotes the rank of a Sylow pro-p subgroup of G and $\Phi^{2R+1}(F)$ the $2R+1$ iterated Frattini subgroup of F.
Regarding the finite axiomatizability of the dimension of $\mathcal{C}_\pi$ groups, we give two different proofs. The first one uses the adjoint representation of a p-adic analytic pro-p group while the second one depends on the following new description of the dimension of a finitely generated powerful pro-p group that is also of independent interest (see Theorem 2.5.1).

Theorem 6. *Let G be a finitely generated powerful pro-p group with torsion subgroup T. Then*

$$\dim(G) = \mathrm{d}(G) - \mathrm{d}(T).$$

Moreover, using different approaches, we write alternative sentences that axiomatize the dimension of $\mathcal{C}_\pi$ groups in different classes: soluble $\mathcal{C}_\pi$ groups, $\mathcal{C}_\pi$ groups whose factors are just-infinite p-adic analytic pro-p groups and $\mathcal{C}_\pi$ groups satisfying a certain condition and whose factors have non-abelian simple Lie algebra (see Section 2.4.3).
In order to eventually prove Theorem 4, we show that in a pro-π group one can find an open definable $\mathcal{C}_\pi$ group with certain properties that will allow to prove the desired result. This relies on the classification of finite simple groups. Finally, we analyse the quantifier complexity of the sentences that we produced, proving that they are of the form $\exists\forall\exists$, hence in particular independent of any input data. This first part of the thesis led to the preprint [CK] written together with my advisor Benjamin Klopsch (see the end of Section 2.1).

The unique product property for pro-p groups. We say that a group G has the *unique product property* if, given two non-empty, finite subsets A and B of G, there always exists at least one element g of G that can be written in a unique way as a product $g = ab$ with $a \in A$ and $b \in B$. The unique product property was introduced by Rudin and Schneider in [RS] in relation to the Kaplansky conjecture on zero divisors in group rings. The conjecture, which is still open, predicts that, if K is a field and G is a torsion-free group, then the group ring $K[G]$ has no non-trivial zero divisors. It is not difficult to see that a group with the unique product property satisfies the zero divisor conjecture. Recently, Craig and Linnell conjectured that uniform pro-p groups possess the unique product property ([CL]). This is motivated by the fact that, if G is a uniform pro-p group and K is a field of characteristic zero or p, then $K[G]$ has no non-trivial zero divisors ([FL]). Moreover, Craig and Linnell prove their conjecture for virtually soluble subgroups of uniform pro-p groups. Here we extend their result to the class of virtually soluble subgroups of saturable pro-p groups by using Lie-theoretic tools (see Corollary 3.3.7):

Theorem 7. *Virtually soluble subgroups of saturable pro-p groups have the unique product property.*

Furthermore, as an example, we verify that the unique product property holds for sets of a specific form in some of the simplest non-soluble p-adic analytic pro-p groups, namely, congruence subgroups of $\mathrm{SL}_2(\mathbb{Z}_p)$ (see Example 3.3.20). Then we consider a property that implies the unique product property, namely local indicability. A group G is *locally indicable* if every non-trivial finitely generated subgroup of G maps homomorphically onto $\mathbb{Z}$. Actually, for soluble groups, local

indicability is equivalent to right-orderability. In order to prove Theorem 7 we actually show that virtually soluble subgroups of saturable pro-p groups are right-orderable, hence locally indicable. Motivated by this we start to study local indicability for soluble profinite groups. In particular, we try to compare local indicability with a topological analogue, i.e., every closed subgroup of a given profinite group has infinite topological abelianisation.

Finally, as ordered groups have the unique product property, we start to study the orderability of profinite groups. For example, by adapting one of the proofs of the fact that (abstract) partially commutative groups are bi-orderable, we prove that partially commutative pro-p groups or, equivalently, pro-p completions of partially commutative groups, are bi-orderable (see Section 3.5). Moreover, we give an elementary proof of the fact that non-soluble pro-p groups of finite rank are not bi-orderable, based on an observation on the normal subsemigroups of these groups carried out with the help of commutator calculus and Lie-theoretic tools (Corollary 3.4.5).

The thesis is organised as follows. We start with a chapter of preliminaries divided into three sections, where we collect some facts that we will need later on. We present some basic notions on profinite and pro-p groups and on pro-p groups of finite rank or, equivalently, p-adic analytic pro-p groups. We will also give a brief overview on abstract properties of profinite groups.
The subsequent chapter concerns the finite axiomatizability of the rank and the dimension of pro-π groups. After the introduction and some preliminaries we first prove the finite axiomatizability of the rank of $\mathcal{C}_\pi$ groups. Then we give the first proof of the finite axiomatizability of the dimension of $\mathcal{C}_\pi$ groups using the adjoint representation of a p-adic analytic pro-p group and we present some alternative sentences for some classes of $\mathcal{C}_\pi$ groups. In the subsequent section we give another proof of the same result based on a result of Héthelyi and Lévai that allows us to formulate a new description of the dimension of finitely generated pro-p groups. In the next sections we extend these results to pro-π groups and we analyse the quantifier complexity of the sentences produced. Finally, we propose some further questions that arise from this work.
The last chapter is about the unique product property for pro-p groups. After the introduction and some preliminaries we prove the main result of the chapter, i.e., the generalisation of Craig and Linnell's theorem. In the same section we also study local indicability for soluble profinite groups with the ascending chain condition on closed subgroups. In the following two sections we prove that non-soluble p-adic analytic pro-p groups are not bi-orderable and that pro-p RAAGs are bi-orderable. Finally, we present some open questions and, in the appendix, a commutator formula.

Notation. The symbol $\mathbb{N}$ denotes the natural numbers including zero.
Given a natural number $n > 0$ we write C_n for the cyclic group of order n.
The commutator subgroup of G is denoted by $[G, G]$ or G'. More generally, if H and K are subgroups of G, $[H, K]$ is the subgroup of G generated by commutators of the form $[h, k]$, with $h \in H$ and $k \in K$.
Given a natural number m and an abstract group G, we denote by G^m the subgroup of G generated by the m-th powers of the elements of G and by $G^{\{m\}}$ the subset of G consisting of the m-th powers of the elements of G. Unless stated otherwise, when G is a topological group, by G^m we will denote the *topological*

closure of the group generated by the m-th powers of the elements of G.
Finally, the symbols $\leq_{\mathrm{c}}$ (respectively $\trianglelefteq_{\mathrm{c}}$), $\leq_{\mathrm{o}}$ (respectively $\trianglelefteq_{\mathrm{o}}$) indicate closed subgroup (respectively closed normal subgroup) and open subgroup (respectively open normal subgroup).
The rest of the notation is either standard or introduced when needed throughout the thesis.

Chapter 1

Preliminaries

In this chapter we will present some preliminary notions and facts that will be used throughout the thesis. The chapter is divided into three sections. The first one provides a brief overview of profinite and pro-p groups. The second section is devoted to presenting a few of the main results concerning abstract properties of profinite groups. This material is essential to us. On the one hand, we will use some of these facts later on and, on the other hand, the results give some insight into the area which this thesis focuses on, i.e., algebraic properties of pro-p groups. Finally, in the last section we will present some basics about pro-p groups of finite rank or, equivalently, p-adic analytic pro-p groups.

The main sources for this chapter are the monographs [RZ], [W1], [DDMS]. The material presented here is well known and there are no significant original contributions.

1.1 A few basics on profinite and pro-p groups

In this section we will present some basic facts on profinite and pro-p groups that we will need throughout the thesis. We will mostly follow [RZ], [W1] and Chapters 1 and 3 of [DDMS], where much more information on profinite groups can be found.

Definition 1.1.1. A profinite group is a compact Hausdorff topological group whose open subgroups form a base of neighbourhoods of the identity.

It turns out that the condition in the definition is equivalent to saying that the group is compact, Hausdorff and totally disconnected ([RZ], Theorem 1.1.12).

A useful characterisation of profinite groups in terms of inverse limits is the following ([DDMS], Proposition 1.3).

Proposition 1.1.2. *Let G be a profinite group. Then G is isomorphic, as a topological group, to*

$$\varprojlim_{N \trianglelefteq_o G} G/N.$$

Conversely, the inverse limit of any inverse system of finite discrete groups is a profinite group.

The isomorphism in the first part of the proposition is given by

$$g \mapsto (gN)_{N \trianglelefteq_o G}.$$

Example 1.1.3.

1. Let G be a group and let $\mathcal{N}$ be a directed family of normal subgroups of finite index in G ordered by reverse inclusion. Then the family of quotients $(G/N)_{N\in\mathcal{N}}$ gives an inverse system by considering, for every $N \leq M$, the natural epimorphism $\pi_{NM} : G/N \to G/M$. The resulting inverse limit

$$\widehat{G}_{\mathcal{N}} := \varprojlim_{N\in\mathcal{N}} G/N$$

is a profinite group by the previous proposition, that is called the completion of G with respect to $\mathcal{N}$. Note that the kernel of the natural homomorphism $G \to \widehat{G}_{\mathcal{N}}$ is given by $\bigcap_{N\in\mathcal{N}} N$.
If $\mathcal{N}$ consists of *all* normal subgroups of G of finite index, then $\widehat{G}_{\mathcal{N}}$ is called the *profinite completion* of G.
If instead $\mathcal{N}$ contains *all* normal subgroups of G whose index is the power of a fixed prime p, then $\widehat{G}_{\mathcal{N}}$ is called the *pro-p completion* of G.

2. As a special case of the previous example we get $\widehat{\mathbb{Z}}$, the profinite completion of the integers $\mathbb{Z}$, isomorphic to

$$\varprojlim_{\substack{n\in\mathbb{N}\\ n\geq 1}} \mathbb{Z}/n\mathbb{Z}.$$

Its elements can be regarded as equivalence classes of sequences of integers $(a_1, a_2, a_3, \ldots)$ such that, if i and j are integers with $i \mid j$, then $a_i \equiv a_j$ modulo i. Two sequences (a_i), (b_i) are equivalent if $a_i \equiv b_i$ modulo i for all $i \geq 1$.

3. Let R be a topological commutative ring with identity that is profinite, i.e., compact, Hausdorff and totally disconnected. For example, R could be $\widehat{\mathbb{Z}}$. Then the following groups obtained by R are profinite groups with the topology naturally induced by R: the group of units R^*, the group $\mathrm{GL}_d(R)$ of invertible $d \times d$ matrices with entries in R, the group $\mathrm{SL}_d(R)$ of $d \times d$ matrices with determinant 1 and entries in R.

4. Consider the group $\mathrm{SL}_d(\mathbb{Z})$ and, for every positive integer m, let $K(m)$ be the kernel of the homomorphism $\mathrm{SL}_d(\mathbb{Z}) \to \mathrm{SL}_d(\mathbb{Z}/m\mathbb{Z})$ obtained by reducing the entries of the matrices modulo m. Since $\mathrm{SL}_d(\mathbb{Z}/m\mathbb{Z})$ is a finite group, $K(m)$ has finite index in $\mathrm{SL}_d(\mathbb{Z})$ and therefore we can consider the completion of $\mathrm{SL}_d(\mathbb{Z})$ with respect to the family $\mathcal{N} = \{K(m) \mid m \geq 1\}$, that is the so-called *congruence completion* of $\mathrm{SL}_d(\mathbb{Z})$. Understanding the relation between the profinite completion and the congruence completion of $\mathrm{SL}_d(\mathbb{Z})$ is an instance of the congruence subgroup problem.

Here are some important basic properties of profinite groups that we mention without proof (see for example [W1], Chapters 0 and 1):

Proposition 1.1.4. *Let G be a profinite group.*

1. *Every open subgroup is closed of finite index. Conversely, a closed subgroup is open if and only if it has finite index.*

2. *Every open subgroup of G contains an open normal subgroup of G.*

3. *The family of all open subgroups of G has trivial intersection.*

4. *Let X be a subset of G. Then, if we denote by $\overline{X}$ the topological closure of X,*
$$\overline{X} = \bigcap_{N \trianglelefteq_o G} XN.$$

5. *Let H be a closed subgroup of G. Then H is a profinite group with the induced topology. Every open subgroup of H is of the form $H \cap K$ where K is an open subgroup of G.*

6. *Let N be a closed normal subgroup of G. Then G/N is a profinite group with the quotient topology.*

7. *Let X and Y be closed subsets of G. Then $XY := \{xy \mid x \in X, y \in Y\}$ is closed in G.*

We now discuss generators of profinite groups. Since profinite groups, if not finite, are always uncountable ([RZ], Proposition 2.3.1), they can never be finitely generated as abstract groups. Therefore, when we talk about generators of a profinite group, we will always mean *topological* generators.

Definition 1.1.5. Let G be a topological group. We say that a subset X of G generates G topologically or that X is a set of topological generators for G if the abstract group generated by X is dense in G, i.e., if $\overline{\langle X \rangle} = G$.
We say that G is *finitely generated* if there exists a finite set X that generates G topologically.

From now on, when we write that a set X generates a profinite group G, we will always mean that X generates G topologically.

Proposition 1.1.6 ([DDMS], Proposition 1.5)**.** *Let G be a profinite group and let H be a closed subgroup of G.*

1. *A subset X of H generates H if and only if XN/N generates HN/N for every $N \trianglelefteq_o G$. In particular, if $H = G$, we have that X generates G if and only if XN/N generates G/N for every $N \trianglelefteq_o G$.*

2. *Let d be a positive integer. Then H can be generated by d elements if and only if HN/N can be generated by d elements for every $N \trianglelefteq_o G$. In particular, if $H = G$, then G can be generated by d elements if and only if G/N can be generated by d elements for every $N \trianglelefteq_o G$.*

Example 1.1.7. A profinite group is called *procyclic* if it is isomorphic to the inverse limit of finite cyclic groups. According to [W1], Proposition 1.2.1, if G is a procyclic group and N is an open normal subgroup of G, then the quotient G/N is a finite cyclic group. It follows that a procyclic group is 1-generated. Conversely, if a profinite group G is 1-generated then all its quotients by open normal subgroups are cyclic, hence G is a procyclic group.
By [W1], Theorem 1.2.5, closed subgroups of procyclic groups are also procyclic.

Let G be a profinite group. We define the minimal number of generators of G as

$$\mathrm{d}(G) := \min\{|X| : X \subseteq G, X \text{ generates } G\}.$$

Whenever we will talk of a group G with an infinite number of generators, we will simply mean that we are considering a set of generators of G of some infinite cardinality. From Proposition 1.1.6 it follows

Corollary 1.1.8. *Let G be a profinite group and let H be a closed subgroup of G. Then*

$$\mathrm{d}(H) = \sup\{\mathrm{d}(HN/N) \mid N \trianglelefteq_{\mathrm{o}} G\}.$$

In particular,

$$\mathrm{d}(G) = \sup\{\mathrm{d}(G/N) \mid N \trianglelefteq_{\mathrm{o}} G\}.$$

Proof. Let $s := \sup\{\mathrm{d}(HN/N) \mid N \trianglelefteq_{\mathrm{o}} G\}$. It is clear that $\mathrm{d}(HN/N) \leq \mathrm{d}(H)$ for every $N \trianglelefteq_{\mathrm{o}} G$, hence $s \leq \mathrm{d}(H)$. Conversely, HN/N can be generated by s elements for every $N \trianglelefteq_{\mathrm{o}} G$. Therefore, by Proposition 1.1.6, H can be generated by s elements and $\mathrm{d}(H) \leq s$. □

Remark 1.1.9. It is clear that, if $\mathcal{N}$ is a base of neighbourhoods of the identity in G consisting of open normal subgroups, then

$$\mathrm{d}(G) = \sup\{\mathrm{d}(G/N) \mid N \in \mathcal{N}\}.$$

In general, given a finitely generated profinite group G, its subgroups are not automatically finitely generated. However, its *open* subgroups are ([DDMS], Proposition 1.7). Moreover, as free profinite groups satisfy Schreier's formula ([RZ], Theorem 3.6.2), it is possible to give a quantitative upper bound on the minimal number of generators of an open subgroup of a finitely generated profinite group G that depends on $\mathrm{d}(G)$ and on the index of the subgroup.

Proposition 1.1.10. *Let G be a finitely generated profinite group and let U be an open subgroup of G. Then,*

$$\mathrm{d}(U) \leq 1 + [G : U](\mathrm{d}(G) - 1).$$

We now move a step forward and introduce an invariant of profinite groups that takes into account the minimal number of generators of all closed subgroups of a given group.

Definition 1.1.11. Let G be a profinite group. The *rank* of G is defined as

$$\mathrm{rk}(G) := \sup\{\mathrm{d}(H) \mid H \leq_{\mathrm{c}} G\}.$$

In words, if finite, $\mathrm{rk}(G)$ is the minimal integer r such that every closed subgroup of G can be generated by r elements.

Proposition 1.1.12 ([DDMS], Proposition 3.11)**.** *Let G be a profinite group. Then the following numbers coincide:*

1. $r_1 := \mathrm{rk}(G)$;
2. $r_2 := \sup\{\mathrm{d}(H) \mid H \leq_{\mathrm{c}} G \text{ and } \mathrm{d}(H) < \infty\}$;

3. $r_3 := \sup\{\mathrm{d}(H) \mid H \leq_{\mathrm{o}} G\}$;

4. $r_4 := \sup\{\mathrm{rk}(G/N) \mid N \trianglelefteq_{\mathrm{o}} G\}$.

As the rank of a profinite group is a fundamental object for the topic of this thesis, we sketch the proof of the previous proposition.

Proof. It is clear that $r_2 \leq r_1$. Also, as every open subgroup is closed, $r_3 \leq r_1$. Now let N be an open normal subgroup of G and let K/N be a subgroup of G/N. Then K is a closed subgroup of G and $\mathrm{d}(K/N) \leq \mathrm{d}(K) \leq r_3$, i.e., $r_4 \leq r_3$. For proving $r_4 \leq r_2$, consider again N and K as before. Since K/N is finite, we can write $K = NX$ where X is a finite subset of G. Let $H = \overline{\langle X \rangle}$; by definition H is a closed and finitely generated subgroup of H, hence $\mathrm{d}(H) < \infty$. Now by construction

$$\mathrm{d}(K/N) = \mathrm{d}(NH/N) = \mathrm{d}(H/N \cap H) \leq \mathrm{d}(H) \leq r_2.$$

Finally we prove $r_1 \leq r_4$. Let H be a closed subgroup of G. By Corollary 1.1.8

$$\mathrm{d}(H) = \sup\{\mathrm{d}(HN/N) \mid N \trianglelefteq_{\mathrm{o}} G\} \leq r_4.$$

□

Remark 1.1.13. From Remark 1.1.9 it follows immediately that, if $\mathcal{N}$ is a base of neighbourhoods of the identity in G consisting of open normal subgroups, then

$$\mathrm{rk}(G) = \sup\{\mathrm{rk}(G/N) \mid N \in \mathcal{N}\}.$$

Two further important properties of the rank that we will subsequently use are the following (compare with [W1], Proposition 8.1.1).

Proposition 1.1.14. *Let G be a profinite group.*

1. *Suppose that G has rank r. Then closed subgroups and quotients by closed normal subgroups of G have rank bounded by r.*

2. *If $K \trianglelefteq_{\mathrm{c}} G$ and both K and G/K have finite rank then G has finite rank and*

$$\mathrm{rk}(G) \leq \mathrm{rk}(K) + \mathrm{rk}(G/K).$$

Proof.

1. It is clear by definition that the rank of a closed subgroup of G is bounded by r. If N is an open normal subgroup of G then a subgroup of G/N is the image of a subgroup of G under the projection modulo N, hence its minimal number of generators is bounded by r.

2. Let H be a closed subgroup of G. Then $H \cap K$ has a system of generators X with cardinality bounded by $\mathrm{rk}(K)$. Moreover, $H/H \cap K \cong HK/K \leq_{\mathrm{c}} G/K$, hence we can find a generating set Y of $H/H \cap K$ whose cardinality is bounded by the rank of G/K. As the union of X and any lift of Y to H is a generating set for H, we conclude that $\mathrm{d}(H) \leq \mathrm{rk}(K) + \mathrm{rk}(G/K)$.

□

Example 1.1.15. Let G be the direct product of r procyclic groups $G_1, \ldots, G_r$. Then $\mathrm{rk}(G) \leq r$.

We can proceed by induction on r. If $r = 1$ there is nothing to say, so let $r > 1$. For each $i \in \{1, \ldots, r\}$, let g_i be the generator of G_i and let S_i be the (closed) subgroup of G generated by $g_1, \ldots, g_i$. Then we have a series

$$1 \leq S_1 \leq S_2 \leq \cdots \leq S_r = G.$$

Now S_r/S_{r-1} is a procyclic group, hence of rank one, while S_{r-1} has rank bounded by $r - 1$ by induction. By Proposition 1.1.14 we conclude that $\mathrm{rk}(G) \leq r$.

We now introduce the Frattini subgroup of a profinite group, the subgroup of 'non-generators.'

Definition 1.1.16. Let G be a profinite group. For $G \neq 1$, the *Frattini subgroup* $\Phi(G)$ of G is defined as the intersection of all maximal proper open subgroups of G. For $G = 1$ we set $\Phi(G) = G$.

The Frattini subgroup $\Phi(G)$ is by definition a closed normal subgroup of G. Its name of subgroup of non-generators comes from the following result.

Proposition 1.1.17 ([DDMS], Proposition 1.9)**.** *Let G be a profinite group and let X be a subset of G. Then the following are equivalent:*

1. *X generates G;*
2. *$X \cup \Phi(G)$ generates G;*
3. *$X\Phi(G)/\Phi(G)$ generates $G/\Phi(G)$.*

We will see that, when G is a finitely generated pro-p group, we are able to write down explicitly how the Frattini subgroup of G looks like. This will result in a fundamental tool to work with pro-p groups of finite rank.

Let p be a prime number. We now consider a special class of profinite groups, namely the class of pro-p groups.

Definition 1.1.18. A *pro-p group* is a profinite group with the property that the index of every open normal subgroup is a power of p.

Note that finite p-groups are by definition pro-p groups. Pro-p groups are closed under taking subgroups and quotients and under group extensions.

Proposition 1.1.19 ([DDMS], Proposition 1.11)**.** *Let G be a profinite group.*

1. *If G is pro-p and H is a closed subgroup of G then H is a pro-p group.*
2. *Let N be a closed normal subgroup of G. Then G is pro-p if and only if N and G/N are pro-p.*

Also for pro-p groups one can give a characterisation in terms of inverse limits.

Proposition 1.1.20 ([DDMS], Proposition 1.12)**.** *Let G be a topological group. Then G is a pro-p group if and only if G is topologically isomorphic to an inverse limit of finite discrete p-groups.*

Example 1.1.21.

1. Looking back at Example 1.1.3, we see that the pro-p completion of any group is a pro-p group. In the special case of the pro-p completion of the integers, we get the p-adic integers $\mathbb{Z}_p$. Elements of $\mathbb{Z}_p$ can be thought of as formal series $\sum_{i=0}^{\infty} a_i p^i$, where a_i is a natural number with $0 \leq a_i < p$ for every i. Equivalently, an element of $\mathbb{Z}_p$ can be identified with the equivalence class of a sequence of natural numbers $(b_n)_{n\geq 1} = (b_1, b_2, \ldots)$, where $b_n \equiv b_m \pmod{p^m}$ whenever $m \leq n$. Two such sequences $(b_n)_n$ and $(b'_n)_n$ are equivalent when $b_n \equiv b'_n \pmod{p^n}$ for every $n \geq 1$. If $x = \sum_{i=0}^{\infty} a_i p^i$, then $b_n \equiv x \pmod{p^n} = \sum_{i=0}^{n-1} a_i p^i$.

   Note that the open subgroups of $\mathbb{Z}_p$ are exactly the subgroups of the form $p^i\mathbb{Z}_p$ for some integer $i \geq 1$. Indeed, it is clear that such subgroups are open, because they are the kernels of the maps $\mathbb{Z}_p \to \mathbb{Z}_p/p^i\mathbb{Z}_p$. Conversely, if H is an open subgroup of $\mathbb{Z}_p$, then it has index a power of p, say p^i. Therefore, $p^i\mathbb{Z}_p \leq H \leq \mathbb{Z}_p$. But as the index of $p^i\mathbb{Z}_p$ in $\mathbb{Z}_p$ is also p^i, it follows that $H = p^i\mathbb{Z}_p$.
   Moreover, the groups $p^i\mathbb{Z}_p$, for $i \geq 1$, form a base of open neighbourhoods of the identity element (see for example [RZ], Lemma 2.1.1).

   If we consider also multiplication, $\mathbb{Z}_p$ can actually be regarded as a profinite ring, i.e., a topological ring with the profinite topology.

2. Sylow subgroups of profinite groups are pro-p groups. (Recall that a Sylow pro-p subgroup of a profinite group G is, by definition, a maximal pro-p subgroup of G).

3. Consider the group $\mathrm{GL}_d(\mathbb{Z}_p)$ of invertible $d \times d$ matrices over $\mathbb{Z}_p$. $\mathrm{GL}_d(\mathbb{Z}_p)$ is a subset of $\mathrm{Mat}_d(\mathbb{Z}_p)$, the ring of $d \times d$ matrices with entries in $\mathbb{Z}_p$. As $\mathrm{Mat}_d(\mathbb{Z}_p)$ can be identified with $\mathbb{Z}_p^{d^2}$, it can be given the product topology that makes it into a Hausdorff, compact, totally disconnected topological space. Since addition and multiplication in $\mathrm{Mat}_d(\mathbb{Z}_p)$ are induced by the operations in $\mathbb{Z}_p$, they are continuous with respect to the profinite topology, hence $\mathrm{Mat}_d(\mathbb{Z}_p)$ is a profinite ring. Therefore $\mathrm{GL}_d(\mathbb{Z}_p)$ is Hausdorff and totally disconnected with the subspace topology inherited from $\mathrm{Mat}_d(\mathbb{Z}_p)$. Moreover, $\mathrm{GL}_d(\mathbb{Z}_p)$ is the preimage under the determinant map of the closed set $\mathbb{Z}_p \setminus p\mathbb{Z}_p$, hence it is closed in $\mathrm{Mat}_d(\mathbb{Z}_p)$ and therefore it is compact. It follows that $\mathrm{GL}_d(\mathbb{Z}_p)$ is a profinite group.

   For any integer $i \geq 1$, let $\mathrm{GL}_d^i(\mathbb{Z}_p)$ be the kernel of the map $\mathrm{GL}_d(\mathbb{Z}_p) \to \mathrm{GL}_d(\mathbb{Z}/p^i\mathbb{Z})$ that reduces the entries of a matrix modulo p^i; equivalently

$$\mathrm{GL}_d^i(\mathbb{Z}_p) = \{A \in \mathrm{GL}_d(\mathbb{Z}_p) \mid A \equiv \mathrm{I} \bmod p^i\},$$

   where I is the $d \times d$ identity matrix. As a matrix in $\mathrm{Mat}_d(\mathbb{Z}_p)$ is invertible if and only if it is invertible modulo p, we can also write

$$\mathrm{GL}_d^i(\mathbb{Z}_p) = \mathrm{I} + p^i \mathrm{Mat}_d(\mathbb{Z}_p).$$

   Since each $\mathrm{GL}_d(\mathbb{Z}/p^i\mathbb{Z})$ is finite, $\mathrm{GL}_d^i(\mathbb{Z}_p)$ is a closed normal subgroup of finite index in $\mathrm{GL}_d(\mathbb{Z}_p)$, hence an open normal subgroup. As the topology

on $\mathrm{GL}_d(\mathbb{Z}_p)$ is inherited from the product topology on $\mathbb{Z}_p^{d^2}$ and we saw that the open subgroups $p^i\mathbb{Z}_p$ form a base of open neighbourhoods of the identity in $\mathbb{Z}_p$, it follows that a base of neighbourhoods of the identity in $\mathrm{GL}_d(\mathbb{Z}_p)$ is given by the subgroups $\mathrm{GL}_d^i(\mathbb{Z}_p)$. Since, for every $i \geq 1$,

$$|\,\mathrm{GL}_d^1(\mathbb{Z}_p) : \mathrm{GL}_d^i(\mathbb{Z}_p)| = p^{d^2(i-1)},$$

it follows that $\mathrm{GL}_d^1(\mathbb{Z}_p)$ is a pro-p group. Indeed, every open subgroup H of $\mathrm{GL}_d^1(\mathbb{Z}_p)$ is in particular an open set containing the identity, hence it contains $\mathrm{GL}_d^i(\mathbb{Z}_p)$ for some i and therefore the index of H in $\mathrm{GL}_d^1(\mathbb{Z}_p)$ must divide $p^{d^2(i-1)}$.
Similarly, one can also show that the congruence subgroup $\mathrm{SL}_d^1(\mathbb{Z}_p)$ is a pro-p group (see [DDMS], Chapter 1, Exercise 10). Alternatively, one can simply note that $\mathrm{SL}_d^1(\mathbb{Z}_p)$ is a pro-p group as it is a closed subgroup of $\mathrm{GL}_d^1(\mathbb{Z}_p)$.

4. Let d be a natural number. A free object on d generators in the category of pro-p groups is a *free pro-p group* on d generators. It can also be seen as the pro-p completion of an abstract free group on d generators.

5. The Heisenberg group over $\mathbb{Z}_p$ given by the upper unitriangular 3×3 matrices over $\mathbb{Z}_p$ is a pro-p group. More generally, the group of upper triangular $n \times n$ matrices is a pro-p group for any positive integer n.

A *pronilpotent group* is by definition a profinite group that is isomorphic to the inverse limit of finite nilpotent groups. Since finite p-groups are nilpotent, pro-p groups are pronilpotent. The same holds for procyclic groups and abelian profinite groups. (A profinite group is abelian if and only if it is pro-abelian; see [RZ], Exercise 2.1.7). The following result relating pronilpotent groups to their Sylow subgroups holds true.

Proposition 1.1.22 ([W1], Proposition 2.4.3)**.** *Let G be a profinite group. Then G is pronilpotent if and only if it is isomorphic to the direct product of its Sylow subgroups.*

Regarding finitely generated abelian pro-p groups, we have the following structure result.

Proposition 1.1.23. *Let A be a finitely generated abelian pro-p group. Then,*

$$A \cong \mathbb{Z}_p^k \times C_{p^{l_1}} \times \cdots \times C_{p^{l_s}}$$

for some non-negative integers s, k and some positive integers $l_1 \ldots, l_s$, with

$$\mathrm{d}(A) = \mathrm{rk}(A) = s + k.$$

Proof. Let $d := \mathrm{d}(A)$. The abelian pro-p group A can be regarded as a $\mathbb{Z}_p$-module in the following way: using additive notation, if λ belongs to $\mathbb{Z}_p$ and g belongs to A, then $\lambda \cdot g$ is well-defined and gives A the structure of a $\mathbb{Z}_p$-module (compare with [RZ], Lemma 4.1.1 or [W1], Proposition 1.5.3). As a $\mathbb{Z}_p$-module, A is generated by d elements. Since $\mathbb{Z}_p$ is a principal ideal domain, we can write A as the direct product of d cyclic pro-p modules, i.e., d procyclic pro-p groups. Now $\mathrm{d}(A) = \mathrm{rk}(A)$ follows from Example 1.1.15.

□

Remark 1.1.24. From the previous proposition one can deduce the structure theorem of finitely generated abelian profinite groups. Indeed, suppose that G is an abelian profinite group with $\mathrm{d}(G) = d$. By Proposition 1.1.22, G is the direct product of its Sylow subgroups, which are abelian pro-p groups that can be generated by d elements, as a Sylow subgroup of G can be regarded as a quotient of G. Let S_p be a Sylow pro-p subgroup of G. Then, by Proposition 1.1.23 we have $S_p \cong S_{p,1} \times \cdots \times S_{p,d}$, where each $S_{p,i}$ is a procyclic pro-p group, possibly trivial. Therefore, $G \cong \prod_{p \text{ prime}} (\prod_{i=1}^{d} S_{p,i})$.

Remark 1.1.25. Regarding the proof of Proposition 1.1.23, it is possible to prove that for a finitely generated abelian profinite group A one has $\mathrm{d}(A) = \mathrm{rk}(A)$ without making use of the structure theorem for finitely generated modules over principal ideal domains; see [RZ], Proposition 4.3.6.

When dealing with a finitely generated pro-p group, its Frattini subgroup provides information on the number of generators of the group.

Proposition 1.1.26. *Let G be a finitely generated pro-p group. Then the quotient group $G/\Phi(G)$ is an elementary abelian p-group of order $p^{\mathrm{d}(G)}$.*

This result follows from the fact that, if G is a pro-p group, then

$$\Phi(G) = \overline{G^p[G,G]} \tag{1.1}$$

(see for example [DDMS], Proposition 1.13 for a proof). Note that, for any profinite group G, one can define the p-Frattini subgroup of G as

$$\Phi_p(G) := \overline{G^p[G,G]}.$$

The inclusion $\Phi(G) \geq \Phi_p(G)$ always holds, but the equality holds if and only if G is pro-p ([W1], Proposition 2.5.2). Moreover, if G is any profinite group, the p-Frattini quotient $G/\Phi_p(G)$ is the largest elementary abelian pro-p quotient of the group G.

In Section 1.2 we will be able to simplify further the formula (1.1) when G is a finitely generated pro-p group and give an explicit description of the commutator subgroup of G in terms of its generators.

Example 1.1.27. Let

$$A \cong \mathbb{Z}_p^k \times C_{p^{l_1}} \times \cdots \times C_{p^{l_s}}$$

for some non-negative integers s, k and some positive integers $l_1 \ldots, l_s$. We give another proof of the fact that $\mathrm{d}(A) = s + k$.
The Frattini subgroup of A is $\Phi(A) = pA$, hence, using additive notation, we have

$$\Phi(A) = (p\mathbb{Z}_p)^k \times pC_{p^{l_1}} \times \cdots \times pC_{p^{l_s}}.$$

Since for every $i \in \{1, \ldots, s\}$ we have $pC_{p^{l_i}} \cong C_{p^{l_i - 1}}$, we get that $A/\Phi(A)$ has order p^{k+s} and, by Proposition 1.1.26, we conclude that $\mathrm{d}(A) = k + s$.

Another relation between the Frattini subgroup of a pro-p group and the generators of the group is given by the following ([DDMS], Proposition 1.14)

Proposition 1.1.28. *Let G be a pro-p group. Then G is finitely generated if and only if $\Phi(G)$ is open.*

Finally, we introduce the lower p-series of a pro-p group G, that is defined recursively as $P_1(G) := G$ and $P_{i+1}(G) := \overline{P_i(G)^p[P_i(G), G]}$ for $i \geq 1$, where $\bar{\cdot}$ denotes the topological closure.

By definition, $P_2(G) = \Phi(G)$ and $\Phi(P_i(G)) \leq P_{i+1}(G)$. Also in this case, that is, as for the Frattini subgroup, we will give in the next section a simplified formula for the elements of the lower p-series of a finitely generated pro-p group.

Proposition 1.1.29 ([DDMS], Proposition 1.16)**.** *Let G be a pro-p group.*

1. *$[P_i(G), P_j(G)] \leq P_{i+j}(G)$ for all positive integers i and j;*
2. *Let G be finitely generated. Then $P_i(G)$ is open in G for each positive integer i and the set $\{P_i(G) \mid i \geq 1\}$ is a base of neighbourhoods of the identity in G.*

Example 1.1.30. If G is a finitely generated abelian pro-p group, using additive notation we have that $P_{i+1}(G) = \overline{P_i(G)^p} = \overline{P_i(G)^{\{p\}}} = \overline{p^i G}$ for $i \geq 1$ and, from the previous proposition, it follows that this is a base of neighbourhoods for the identity. When G is $\mathbb{Z}_p$ we find again that the subgroups $p^i\mathbb{Z}_p$ are a base of neighbourhoods of the identity (compare with Example 1.1.21).

1.2 Abstract properties of profinite groups

When studying profinite groups, one can ask which properties they have as abstract groups, i.e., when considered without taking into account their topology.

A starting point for this kind of investigation is a result by Serre who established that the topology of a finitely generated pro-p group is entirely determined by the algebraic structure of the group. More precisely, Serre proved that, if G is a finitely generated pro-p group, then every subgroup of finite index of G is open. In other words, in a finitely generated pro-p group a subgroup is open if and only if it has finite index. A profinite group with this property is said to be *strongly complete* or *rigid*. (According to [RZ], Section 4.8, Serre included this result in an unpublished letter to Pletch dated March 26, 1975).

One can see that it is not always the case that a pro-p group is strongly complete. For instance, consider the following example taken from [Se2], Section 6.3 (see also [K2], Section 5.2.1). Let p be a prime and, for each positive integer i, let C_p be the cyclic group of order p. Consider, for each positive integer n, the direct product $G_n = \prod_{i=1}^{n} C_p$ and let $G = \varprojlim G_n$. As an abstract group, G is an $\mathbb{F}_p$-vector space of dimension $2^{\aleph_0}$ and therefore it has $2^{2^{\aleph_0}}$ subgroups of finite index. However, open subgroups of G must contain a subgroup $\ker(G \to G_n)$ for some n ([RZ], Lemma 2.1.1), hence there are only countably many open subgroups in G. More generally, one can construct similar examples with any non-trivial finite group in place of a cyclic group of order p (see [RZ], Example 4.2.12).
As we will see below, the topology of a strongly complete profinite group is completely determined by its group structure. There are indeed examples of profinite groups that are isomorphic as abstract groups but not isomorphic as topological groups, for instance the pro-p groups $G = \prod_{i=1}^{\infty} C_{p^i}$ and $G \times \mathbb{Z}_p$ (see

[K2], Proposition 5.5). In [Ki], Kiehlmann classifies countably-based abelian pro-p groups up to abstract and topological isomorphism.

Serre's theorem on the rigidity of finitely generated pro-p groups is a fundamental result in the theory of finitely generated pro-p groups. Its proof requires some ingredients that are important in their own right and that we will use later on so that we briefly sketch its proof, following the exposition in [DDMS].

The first ingredient of the proof is the following lemma.

Lemma 1.2.1. *Let G be a pro-p group and H a subgroup of finite index of G. Then $|G : H|$ is a power of p.*

Proof. By replacing H by its normal core if necessary, we can assume that H is normal in G. Let $m := p^r m'$, with $(p, m') = 1$, be the index of H in G. Then G/H is a finite group of order m. Therefore, the set $X := G^{\{m\}}$ of m-th powers of elements of G is contained in H and it is closed in G, being the image of the continuous map $g \mapsto g^m$ from the compact space G to the Hausdorff space G.

Now, consider an element $g \in G$; we want to prove that, for some positive integer e, g^{p^e} belongs to H. Indeed, let N be an open normal subgroup of G. By definition of pro-p group, the index of N in G is a power of p, hence there exists k such that g^{p^k} belongs to N. Moreover, we can assume $k \geq r$. Then there exist integers a and b such that $am + bp^k = p^r$. It follows that $g^{p^r} = g^{am+bp^k} = (g^a)^m (g^{p^k})^b \in XN$. Since this is true for every normal open subgroup N and X is closed, we get that $g^{p^r} \in \bigcap_{N \trianglelefteq_o G} XN = X \subseteq H$.

□

The second main ingredient in the proof of Serre's result is the fact that the commutator subgroup of a finitely generated pro-p group is closed.

Proposition 1.2.2. *Let G be a finitely generated pronilpotent group generated by elements $a_1, \ldots, a_d$. Then,*

$$[G, G] = [a_1, G] \cdots [a_d, G].$$

In particular, $[G, G]$ is closed in G.

Recall that $[G, G]$ is the commutator subgroup of G, i.e., the subgroup of G generated by all commutators, while $[a_1, G] \cdots [a_d, G]$ is the set

$$\{[a_1, g_1] \cdots [a_d, g_d] \mid g_1, \ldots, g_d \in G\}.$$

The proof of this proposition relies on a similar result that holds for all finitely generated nilpotent groups. It is proved by induction on the nilpotency class by performing computations with commutators, see [DDMS], Lemma 1.23 or [Se].

Lemma 1.2.3. *Let H be a nilpotent group generated by $a_1, \ldots, a_d$. Then,*

$$[H, H] = [a_1, G] \cdots [a_d, G].$$

With this lemma we can now sketch the proof of Proposition 1.2.2.

Proof of Proposition 1.2.2. Let X be the set $[a_1, G] \cdots [a_d, G] \subseteq [G, G]$. This is the image in G of the compact space $G \times \cdots \times G$ under the continuous map $(g_1, \ldots, g_d) \mapsto [a_1, g_1] \cdots [a_d, g_d]$, hence it is compact. Therefore, since G is Hausdorff, X is closed in G, hence

$$X = \overline{X} = \bigcap_{N \trianglelefteq_o G} XN \tag{1.2}$$

by Proposition 1.1.4. Now for every open normal subgroup N of G, the quotient G/N is a finite nilpotent group. Therefore we can apply Lemma 1.2.3 to G/N to obtain

$$[G/N, G/N] = [\overline{a}_1, G/N] \cdots [\overline{a}_d, G/N].$$

It follows that

$$[G, G]N = XN.$$

Hence, by using (1.2) we obtain:

$$[G, G] \subseteq \bigcap_{N \trianglelefteq_o G} XN = X.$$

As $X \subseteq [G, G]$ the result follows.

□

As a corollary of this proposition we give a simplified formula for the Frattini subgroup and for the lower p-series of a finitely generated pro-p group, as promised in the previous section.

Corollary 1.2.4. *Let G be a finitely generated pro-p group. Then,*

$$\Phi(G) = G^p[G, G]$$

and

$$P_{i+1}(G) = P_i(G)^p[P_i(G), G]$$

for all $i \geq 1$.

Proof. We know from (1.1) that $\Phi(G) = \overline{G^p[G, G]}$. Now, $G^p[G, G] = G^{\{p\}}[G, G]$ and the set $G^{\{p\}}$ is closed, being the image of the p-th power map from G to G. Since also $[G, G]$ is closed by Proposition 1.2.2, from Proposition 1.1.4 we conclude that $G^p[G, G]$ is closed and $\Phi(G) = G^p[G, G]$.

The second claim is proved similarly by induction; see [DDMS], Corollary 1.20 for details. □

Putting everything together we can prove Serre's theorem.

Theorem 1.2.5 (Serre)**.** *Let G be a finitely generated pro-p group. Then every subgroup of finite index of G is open.*

Proof. Let H be a finite index subgroup in G. Replacing H by its core if necessary, one can assume that H is normal in G. We argue by induction on the index (of normal subgroups). If the latter is 1, then $H = G$ is open. Suppose that the index of H is greater than 1. Let $M = H\Phi(G)$. As M contains the open subgroup $\Phi(G)$ (Proposition 1.1.28), M is open in G, hence finitely generated ([DDMS], Proposition 1.7). It is moreover a proper subgroup of G, since G/H is a finite p-group. Hence, $|M : H| < |G : H|$. Therefore, by induction we obtain that H is open in M, hence in G. □

An immediate consequence of this result is that a finitely generated pro-p group is isomorphic to its pro-p completion (use Proposition 1.1.2 and the definition of pro-p completion together with Lemma 1.2.1).

Another consequence is that the topology of a finitely generated pro-p group is completely determined by its group structure.

Corollary 1.2.6. *Any group homomorphism from a finitely generated pro-p group to a profinite group is continuous.*

Proof. Let G be a finitely generated pro-p group, H a profinite group and $\phi : G \to H$ a group homomorphism. Let U be an open subgroup of H (hence of finite index). Then $\phi^{-1}(U)$ has finite index in G, hence it is open. It follows that ϕ is continuous "at the identity " and hence continuous. □

Corollary 1.2.7. *Let G be a finitely generated pro-p group. Then there is no other topology on G that makes G into a profinite group.*

Proof. Assume that $H = G$ as an abstract group but is given a possibly different topology that makes it into a profinite group. Consider the identity map $G \to H$. By the previous corollary this map is continuous. Since G is compact, any closed subset of G is compact hence its image under the identity is compact. Since H, being profinite, is Hausdorff, any compact subset is closed. Therefore the identity map is a continuous closed map, hence a homeomorphism. □

In [NS] Nikolov and Segal extended Theorem 1.2.5 to all finitely generated profinite groups proving the *strong completeness theorem*: every subgroup of finite index in a finitely generated profinite group is open. The proof of this result is significantly more involved than the pro-p case and relies on the classification of finite simple groups; see [K2] for a survey and the book [Se] for another exposition. It is worth to mention that some of the tools related to the finite width of certain words developed by Nikolov and Segal to prove the strong completeness theorem were later used by Jarden and Lubotzky to prove the first-order rigidity of finitely generated profinite groups (see Section 2.2.2).

As important consequences of the strong completeness theorem we obtain that the topology of a finitely generated profinite group is already determined by its algebraic structure and that a finitely generated profinite group is isomorphic to its profinite completion. Finally, the theorem of Nikolov and Segal has also consequences related to the comparison between abstract and continuous cohomology groups of finitely generated profinite groups (see [K2], Section 5.4 and [N], Section 7).

1.3 Pro-p groups of finite rank

In this section we collect some facts regarding pro-p groups of finite rank that will be needed later on. For proofs and more results see [DDMS]. For a concise introduction to pro-p groups of finite rank see [K1].

Recall that, given a pro-p group G, we denote by $\mathrm{d}(G)$ the minimal number of (topological) generators of G and that the rank of G is defined as

$$\mathrm{rk}(G) := \sup\{\mathrm{d}(H) \mid H \leq G \text{ closed}\}.$$

Loosely speaking, a p-adic analytic group (or p-adic Lie group) is a group that has also the structure of a p-adic analytic manifold such that the group operations are analytic (see [DDMS], Section 8.2). One possible interpretation of Hilbert's fifth problem is to determine whether the fact that a group admits a Lie structure has a purely topological characterisation. In the real case this was proven in the affirmative by Montgomery-Zippin and Gleason, who showed that a topological group G admits a (real) Lie structure if and only if G is locally euclidean, i.e., every point of G has a neighbourhood that is homeomorphic to an open subset of $\mathbb{R}^d$, for some positive integer d ([T], Theorem 1.1.9). The answer to Hilbert's fifth problem in the p-adic setting was found in the 1960s by Lazard who, in his seminal paper [La], developed a comprehensive theory of p-adic Lie groups. The group-theoretic aspects of his work were later reconsidered and developed in the 1980s by Lubotzky and Mann and were systematically written down in the book 'Analytic Pro-p Groups' ([DDMS]) by Dixon, du Sautoy, Mann and Segal. One way of expressing Lazard's characterisation of p-adic analytic groups is the following ([DDMS], Theorem 8.1 and Theorem 3.13).

Theorem 1.3.1. *A topological group G has the structure of a p-adic analytic group if and only if G has an open subgroup which is a pro-p group of finite rank.*

Therefore, in the special case when G is a finitely generated profinite group, by the strong completeness theorem, G is a p-adic analytic group if and only if G is virtually a pro-p group of finite rank. In particular, by Proposition 1.1.14, G itself must have finite rank. It follows that the rank is a crucial invariant for pro-p groups. Indeed, one can formulate the following algebraic characterisation of p-adic analytic pro-p groups (see [DDMS], Interlude A):

Theorem 1.3.2. *A pro-p group is p-adic analytic if and only if it has finite rank.*

Example 1.3.3. We saw in Example 1.1.21 that the congruence subgroups $\mathrm{GL}_d^1(\mathbb{Z}_p)$ and $\mathrm{SL}_d^1(\mathbb{Z}_p)$ are pro-p groups. Let $\epsilon = 0$ if $p \neq 2$ and $\epsilon = 1$ if $p = 2$. Then the congruence subgroups $\mathrm{GL}_d^{1+\epsilon}(\mathbb{Z}_p)$ and $\mathrm{SL}_d^{1+\epsilon}(\mathbb{Z}_p)$ are pro-p groups of finite rank, given by d^2 and d^2-1 respectively (see [DDMS], Section 5.1). Therefore $\mathrm{GL}_d^1(\mathbb{Z}_p)$ and $\mathrm{SL}_d^1(\mathbb{Z}_p)$ are pro-p groups of finite rank: this follows immediately if p is odd and from Proposition 1.1.14 if p is even.

Conversely, every pro-p group of finite rank admits a faithful linear representation over $\mathbb{Z}_p$ ([DDMS], Theorem 7.19), which gives, together with the previous example, another characterisation of p-adic analytic pro-p groups: a pro-p group is p-adic analytic if and only if it is isomorphic to a closed subgroup of $\mathrm{GL}_d(\mathbb{Z}_p)$ for some positive integer d.

Yet another characterisation of p-adic analytic pro-p groups is given in terms of powerful subgroups. Loosely speaking, a pro-p group is powerful if it has many p-th powers. This concept generalises the property of being abelian.

Definition 1.3.4. A pro-p group G is *powerful* if $p \neq 2$ and $[G, G] \subseteq G^p$ or $p = 2$ and $[G, G] \subseteq G^4$. More generally, a closed subgroup $N \leq_{\mathrm{c}} G$ is *powerfully embedded* in G if $p \neq 2$ and $[N, G] \subseteq N^p$ or $p = 2$ and $[N, G] \subseteq N^4$.

Note that by G^p, G^4, N^p and N^4 we mean the topological closure of the subgroup of G (respectively of N) generated by all the p-th (respectively 4th)

powers. It follows from the definition that G is powerful if and only if it is powerfully embedded in itself and that, if a closed subgroup N is powerfully embedded in G, then N is a normal subgroup of G and N is powerful. Moreover, it is clear from the definition that the quotients of a powerful pro-p group are again powerful pro-p groups.

With powerful pro-p groups we can give the following characterisation of pro-p groups of finite rank ([DDMS], Theorem 3.13).

Theorem 1.3.5. *Let G be a pro-p group. Then G has finite rank if and only if G is finitely generated and virtually powerful.*

From this theorem and Theorem 1.3.2 it follows that:

Theorem 1.3.6. *A pro-p group is p-adic analytic if and only if it is finitely generated and virtually powerful.*

It is an important fact that for a powerful finitely generated pro-p group the rank coincides with the minimal number of generators of the group ([DDMS], Theorem 3.8):

Theorem 1.3.7. *Let G be a powerful finitely generated pro-p group. Then, for any closed subgroup H of G, $\mathrm{d}(H) \leq \mathrm{d}(G)$.*

Recall from Section 1.1 that the lower p-series of a pro-p group G is defined recursively as

$$\begin{aligned} P_1(G) &:= G \\ P_{i+1}(G) &:= \overline{P_i(G)^p[P_i(G), G]}, \end{aligned}$$

for $i \geq 1$, where $\bar{\cdot}$ denotes the topological closure.

The following proposition collects some important results regarding the lower p-series of a finitely generated powerful pro-p group.

Proposition 1.3.8 ([DDMS], Theorem 3.6)**.** *Let G be a finitely generated powerful pro-p group. Then, for every positive integer i, the following hold:*

1. *$P_i(G)$ is powerfully embedded in G;*
2. *$P_{i+1}(G) = \Phi(P_i(G))$;*
3. *$P_i(G) = G^{p^{i-1}} = \{x^{p^{i-1}} \mid x \in G\}$;*
4. *the map $x \mapsto x^{p^k}$ induces a homomorphism from $P_i(G)/P_{i+1}(G)$ onto $P_{i+k}(G)/P_{i+k+1}(G)$ for each natural number k.*

In particular, it follows from the previous proposition that the lower p-series of a finitely generated powerful pro-p group G coincides with its iterated Frattini series, i.e.,

$$\Phi^i(G) = P_{i+1}(G)$$

for every natural number $i \geq 0$.

When the homomorphism from $P_i(G)/P_{i+1}(G)$ to $P_{i+1}(G)/P_{i+2}(G)$ induced by the map $x \mapsto x^p$ is an isomorphism for every i, we obtain a special kind of powerful group.

Definition 1.3.9. A uniformly powerful (abbreviated as *uniform*) subgroup of a pro-p group G is a finitely generated powerful subgroup U of G such that $|P_i(U) : P_{i+1}(U)| = |G : P_2(G)|$ for all $i \geq 1$.

The last condition is the one that justifies the term uniform. Equivalently, a finitely generated pro-p group is uniform if and only if it is powerful and torsion-free ([DDMS], Theorem 4.5).
Examples of uniform pro-p groups are the congruence subgroups $\mathrm{GL}_d^{1+\epsilon}(\mathbb{Z}_p)$ and $\mathrm{SL}_d^{1+\epsilon}(\mathbb{Z}_p)$ ([DDMS], Section 5.1). For the former group the uniform cardinality of the sections in the lower p-series is given by p^{d^2}, while, for the latter, it is p^{d^2-1}. A relevant fact regarding uniform pro-p groups is contained in the next proposition.

Proposition 1.3.10 ([DDMS], Proposition 4.4)**.** *Let G be a finitely generated powerful pro-p group. Then the following are equivalent:*

1. *G is uniform;*
2. *$\mathrm{d}(H) = \mathrm{d}(G)$ for every powerful open subgroup H of G.*

It turns out that every finitely generated powerful pro-p group has an open characteristic uniform subgroup. From this and the fact that any pro-p group of finite rank contains a powerful characteristic open subgroup ([DDMS], Theorem 3.10) one gets the following:

Corollary 1.3.11 ([DDMS], Corollary 4.3)**.** *A pro-p group of finite rank contains a characteristic open uniform subgroup.*

Finally, uniform pro-p groups allow us to formulate the following structure theorem for powerful pro-p groups.

Theorem 1.3.12 ([DDMS], Theorem 4.20)**.** *Let G be a finitely generated powerful pro-p group. Then the elements of finite order in G form a characteristic subgroup T of G. Moreover, T is a powerful finite p-group and G/T is uniform.*

The fact that a pro-p group has a p-adic analytic structure can be characterised in purely algebraic terms. Also the *dimension* of a p-adic analytic pro-p group, i.e., its dimension as an analytic manifold, can be characterised algebraically in terms of the minimal number of generators of certain subgroups.
We saw before that every pro-p group of finite rank has a normal uniform subgroup of finite index (Corollary 1.3.11). It turns out that the minimal number of generators of any uniform subgroup U of finite index in a pro-p group G is the same, independently of the choice of the uniform subgroup ([DDMS], Lemma 4.6). Hence, if G is a pro-p group of finite rank and U is any uniform subgroup of finite index in G, we can define

$$\dim G := \mathrm{d}(U)$$

and it turns out that this number coincides with the dimension of G as an analytic group (see [DDMS], Theorem 8.36).
For example, since, when p is odd, $\mathrm{GL}_d^1(\mathbb{Z}_p)$ is a uniform pro-p group and

$$|\,\mathrm{GL}_d^1(\mathbb{Z}_p) : \mathrm{GL}_d^2(\mathbb{Z}_p)| = |\,\mathrm{GL}_d^1(\mathbb{Z}_p) : \Phi(\mathrm{GL}_d^1(\mathbb{Z}_p))| = p^{d^2},$$

the dimension of $\mathrm{GL}_d^1(\mathbb{Z}_p)$ is $\mathrm{d}(\mathrm{GL}_d^1(\mathbb{Z}_p)) = d^2$.

The dimension satisfies some good properties, such as that, for any $N \trianglelefteq_{\mathrm{c}} G$,

$$\dim G = \dim G/N + \dim N$$

([DDMS], Theorem 4.8). In particular, a normal subgroup of finite index in G has the same dimension as G.

Recall that a $\mathbb{Z}_p$-Lie lattice is a Lie ring over $\mathbb{Z}_p$ that is also a free module of finite rank over $\mathbb{Z}_p$. To each uniform pro-p group U there is an associated $\mathbb{Z}_p$-Lie lattice $L(U)$ whose underlying set is U and whose addition, scalar multiplication and Lie bracket are defined using the group operation on U (see [DDMS], Chapter 4). Tensoring by $\mathbb{Q}_p$, one obtains the $\mathbb{Q}_p$-Lie algebra associated to G, that is given by

$$\mathfrak{L} := L(U) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p.$$

Similarly to the definition given for powerful pro-p groups, we define a $\mathbb{Z}_p$-lattice L to be *powerful* if $p \neq 2$ and $[L, L] \subseteq pL$ or $p = 2$ and $[L, L] \subseteq 4L$. For example, if L is any $\mathbb{Z}_p$-lattice and p is odd (respectively $p = 2$), then its sublattice pL (respectively $4L$) is powerful. One can verify that the $\mathbb{Z}_p$-lattice associated to a uniform pro-p group is powerful.

Conversely, to a powerful $\mathbb{Z}_p$-Lie lattice L one can associate a uniform group that has L as underlying set and whose operation is defined via the Campbell-Hausdorff formula ([DDMS], Theorem 9.8). This results in an equivalence of categories between uniform pro-p groups and $\mathbb{Z}_p$-powerful lattices ([DDMS], Theorem 9.10). Tensoring by $\mathbb{Q}_p$, this equivalence of categories gives a functor from the category of p-adic analytic pro-p groups to the category of finite-dimensional $\mathbb{Q}_p$-Lie algebras ([DDMS], Theorem 9.11).

Example 1.3.13. Let $\mathfrak{gl}_d(\mathbb{Z}_p)$ be the $\mathbb{Z}_p$-Lie lattice consisting of all $d \times d$ matrices with entries in $\mathbb{Z}_p$ together with the Lie bracket given by the commutator bracket. The Lie lattice $\mathfrak{gl}_d(\mathbb{Z}_p)$ has a congruence filtration given by

$$\mathfrak{gl}_d^i(\mathbb{Z}_p) := \{x \in \mathfrak{gl}_d(\mathbb{Z}_p) \mid x \equiv 0 \pmod{p^i}\},$$

where i runs over the positive integers. Let $\epsilon = 0$ if $p \neq 2$ and $\epsilon = 1$ if $p = 2$. Then the powerful $\mathbb{Z}_p$-Lie lattice associated to the uniform pro-p group $\mathrm{GL}_d^{1+\epsilon}(\mathbb{Z}_p)$ is isomorphic to $\mathfrak{gl}_d^{1+\epsilon}(\mathbb{Z}_p)$ ([K1], Proposition 8.2).

Similarly, if $\mathfrak{sl}_d(\mathbb{Z}_p)$ denotes the $\mathbb{Z}_p$-Lie lattice consisting of all $d \times d$ matrices with entries in $\mathbb{Z}_p$ and zero trace together with the commutator Lie bracket, then the powerful $\mathbb{Z}_p$-Lie lattice associated to the uniform pro-p group $\mathrm{SL}_d^{1+\epsilon}(\mathbb{Z}_p)$ is isomorphic to $\mathfrak{sl}_d^{1+\epsilon}(\mathbb{Z}_p)$.

In general, a closed subgroup of a uniform pro-p group G is not uniform, which makes it difficult to establish a correspondence between closed subgroups of G and $\mathbb{Z}_p$-Lie sublattices of $L(G)$. However, the following result holds true.

Theorem 1.3.14 ([DDMS], Proposition 4.31)**.** *Let G be a uniform pro-p group. Let H be a uniform closed subgroup of G and let N be a closed normal subgroup of G such that G/N is uniform. Then*

1. *$L(H)$ is a $\mathbb{Z}_p$-Lie sublattice of $L(G)$;*

2. N is uniform and $L(N)$ is a $\mathbb{Z}_p$-Lie ideal in $L(G)$.

By $\mathbb{Z}_p$-Lie ideal of $L(G)$ we mean a $\mathbb{Z}_p$-Lie sublattice M of $L(G)$ such that $[L(G), M] \subseteq M$.

Note that, as $[x \otimes \lambda, y \otimes \mu] = [x, y] \otimes (\lambda\mu)$, if $L(H)$ is a $\mathbb{Z}_p$-Lie sublattice of $L(U)$, then $L(H) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is a $\mathbb{Q}_p$-Lie subalgebra of $L(U) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ and, if $L(K)$ is a $\mathbb{Z}_p$-Lie ideal of $L(U)$, then $L(K) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is a $\mathbb{Q}_p$-Lie ideal of $L(U) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$.

Chapter 2

Definability of the rank and the dimension of p-adic analytic pro-p groups

2.1 Introduction

In a recent paper ([NST]), Nies, Segal and Tent started an investigation of the finite axiomatizability of profinite groups. A profinite group is said to be finitely axiomatizable in the class of profinite groups with respect to a language $\mathcal{L}$ if there is a first-order sentence ψ_G in the language $\mathcal{L}$ such that, for every profinite group H the following holds: H satisfies ψ_G if and only if H is isomorphic to G, where the isomorphism is required to be continuous. More generally, one can investigate which properties or invariants of profinite groups belonging to a given class can be described by a single first-order sentence in a certain language. In this case we say that a property $\mathcal{P}$ is finitely axiomatizable in a class $\mathcal{C}$ of profinite groups with respect to a language $\mathcal{L}$ if there exists a first-order sentence $\phi_{\mathcal{P}}$ in $\mathcal{L}$ such that the following holds: a profinite group G belonging to $\mathcal{C}$ has property $\mathcal{P}$ if and only if $\phi_{\mathcal{P}}$ holds true in G.

One of the classes of profinite groups under consideration in [NST] is the one of pro-p groups of finite rank or, equivalently, p-adic analytic pro-p groups. Regarding the rank of pro-p groups, Nies, Segal and Tent state the following

Proposition 1 ([NST], Proposition 5.1)**.** *For each positive integer r, there is a sentence $\rho_{p,r}$ in the language of groups such that, for every pro-p group G,*

$$\mathrm{rk}(G) \leq r \quad \Rightarrow \quad G \models \rho_{p,r} \quad \Rightarrow \quad \mathrm{rk}(G) \leq r(2 + \log_2(r)).$$

As the proof of this proposition is only sketched in the aforementioned paper, we present its proof in Section 2.2.4 for completeness. Then we improve on this result by proving that the rank of a pro-p group is actually determined by a single first-order sentence in the language of groups (compare with Corollary 2.3.6). In other words, given a positive integer r, the property of having rank r is finitely axiomatizable in the class of pro-p groups. To prove this we will establish first the following fact, that is interesting in its own right (see Theorem 2.3.1).

Theorem 2. *Let r be a positive integer and let G be a pro-p group of rank $\mathrm{rk}(G) \leq r$. Suppose that $F \trianglelefteq_{\mathrm{o}} G$ is powerful. Then $\mathrm{rk}(G) = \mathrm{rk}(G/P_{2r+1}(F))$.*

Recall that $P_{2r+1}(F)$ is the $2r+1$ term in the lower p-series of F (see Section 1.1).
More generally, we show that, given a finite set of primes π, the rank of a pro-π group is completely determined by a single first-order sentence (see Theorem 2.6.4):

Theorem 3. *Let $\pi = \{p_1, \dots, p_k\}$ be a finite set of primes and let r be a positive integer. Then the property of having rank r is finitely axiomatizable in the class of pro-π groups.*

Moreover, we prove that this result is the best possible in the class of profinite groups, meaning that the rank of a profinite group involving an infinite number of primes cannot be finitely axiomatizable (Proposition 2.3.9).
We also prove an analogous statement for the dimension of pro-π groups (compare with Theorem 2.7.1):

Theorem 4. *Let $\pi = \{p_1, \dots, p_k\}$ be a finite set of primes and let $\mathbf{d}$ be a k-tuple of natural numbers. Then the property of having dimension $\mathbf{d}$ is finitely axiomatizable in the class of pro-π groups of fixed finite rank.*

Here, by $\dim G = \mathbf{d} = (d_1, \dots, d_k)$, we mean that the pro-$p_i$ Sylow of G has dimension G_i.

We give two different proofs of the previous theorem. The first uses the adjoint representation of a p-adic analytic pro-p group (Section 2.4), while the second relies on the following new description of the dimension of a finitely generated powerful pro-p group (Theorem 2.5.1):

Theorem 5. *Let G be a finitely generated powerful pro-p group with torsion subgroup T. Then*

$$\dim(G) = \mathrm{d}(G) - \mathrm{d}(T).$$

We will first prove both results for pronilpotent groups and then generalize them to pro-π groups.

The chapter is organized as follows. We start with a brief recollection of some preliminaries that will be needed throughout the chapter (Section 2.2). Then we will prove the finite axiomatizability of the rank and the dimension for pronilpotent groups (Sections 2.3, 2.4, 2.5). Along the way we also present some alternative sentences that express the dimension of pronilpotent groups belonging to some special classes of pronilpotent groups of finite rank (Section 2.4.3). Finally, in Sections 2.6 and 2.7 we extend these results to pro-π groups. In Section 2.8 we make an analysis of the quantifier complexity of the sentences that we wrote and, in Section 2.9, we collect some open questions that arise from our work. Finally, in the last section we list some of the main formulas used throughout the chapter for the convenience of the reader.

The material of this chapter led to the preprint [CK] written together my advisor Benjamin Klopsch. In our preprint one can find the main results of this chapter. These results were obtained and written up jointly by the two authors.

2.2 Preliminaries

2.2.1 A few model theoretic facts and notation

In this section we collect some basic facts of model theory, following mostly [M] and [TZ]. We will present the concepts and tools that we will need later on in a rather informal way, mostly with a view towards the use of first-order logic in group theory.

The basic idea of model theory is to use first-order languages to talk about mathematical structures and their properties. By mathematical structure we mean a set with a collection of distinguished functions, relations and elements. For example, a group is a set with a distinguished element (the neutral element), a binary function (the group operation) and a unary function (the inverse operation). Then one chooses a language with which it is possible to talk about these distinguished functions, relations and elements.
Therefore the first concept to be introduced is the one of *language*.

Definition 2.2.1. A language $\mathcal{L}$ is given by the following elements:

1. a set of constant symbols;
2. a set of function symbols where, for each function symbol f, its arity n_f (i.e., the number of variables) is specified;
3. a set of relation symbols where, for each relation symbol R, its arity n_R is specified.

Example 2.2.2.

1. The language of groups is given by
$$\mathcal{L}_{\text{gp}} = \{1, \cdot, ^{-1}\}.$$
Here the constant 1 represents the neutral element of the group, $\cdot$ the (binary) group operation and $^{-1}$ the (unary) inverse function.
2. $$\mathcal{L}_{\text{ordgp}} = \{1, \cdot, ^{-1}, <\}$$
is the language of ordered groups, where $1, \cdot, ^{-1}$ are as above and $<$ is a symbol for a binary relation (order relation).
3. The language of rings $\mathcal{L}_{\text{rings}}$ is given by the set
$$\mathcal{L}_{\text{rings}} = \{0, 1, +, -, \cdot\}.$$

Once we have a language $\mathcal{L}$ we need a structure where we can interpret the symbols of such a language.

Definition 2.2.3. Let $\mathcal{L}$ be a language. An $\mathcal{L}$-structure $\mathcal{M}$ is given by the following data:

1. a non-empty set M, called the *universe* of $\mathcal{M}$;

2. an element $c^{\mathcal{M}} \in M$ for each constant $c \in \mathcal{L}$;

3. a function $f^{\mathcal{M}} : M^{n_f} \to M$ for each function f in $\mathcal{L}$ with n_f variables;

4. a set $R^{\mathcal{M}} \subseteq M^{n_R}$ for each relation symbol R in $\mathcal{L}$ with arity n_R.

For example, if $\mathcal{L}_{\text{gp}}$ is the language of groups, $(\mathbb{Z}, 0, +, -)$ is an $\mathcal{L}_{\text{gp}}$-structure.

Once we have a language $\mathcal{L}$ and an $\mathcal{L}$-structure, we can talk about properties of our structure by means of first-order formulas. Concretely, a first-order *formula* in the language $\mathcal{L}$ is a finite string of symbols built using the symbols of $\mathcal{L}$, variable symbols, the equality symbol $(=)$, the connectives and $(\wedge)$, or $(\vee)$, not $(\neg)$, the existential quantifier $(\exists)$, the universal quantifier $(\forall)$ and parentheses. Note that the implication $(\to)$ can be obtained as a combination of $\neg$ and $\vee$. One then interprets such formulas in the given $\mathcal{L}$-structure.
For instance, if $\mathcal{L} = \mathcal{L}_{\text{gp}}$, examples of formulas are:

1. $\exists x : (x \cdot x \cdot x = 1 \wedge x \neq 1)$;

2. $x^2 = 1$;

3. $x^{-1}yx = z$;

4. $\forall y, z : y^{-1}z^{-1}yz = 1$.

It is important to note that in first-order logic one is allowed to quantify only over elements of the structures and not, for examples, over its substructures. The formal definition of a formula is inductive and can be found in Chapter 1 of [M].

A variable in a formula is said to be *free* if it is not preceded by a (universal or existential) quantifier. A *sentence* is a formula without free variables. This means that one can always tell the truth value of a sentence for each given structure.
Examples 1 and 4 above are examples of sentences. Given any group G we can say whether they hold true in G or not: the sentence in Example 1 holds true in G if and only if G contains an element of order 3, while the sentence in Example 4 is true in G if and only if G is abelian. The truth value of the formulas in Examples 2 and 3 instead depend on the values that we choose for replacing the variables x, y, z. For example, if we take G to be C_4 with additive notation, the sentence in Example 2 is true if we replace x with $\bar{2}$ and false if we replace x with $\bar{3}$.
As a matter of notation, if ϕ is a formula with free variables $v_1, \ldots, v_n$, we will sometimes write $\phi(v_1, \ldots, v_n)$ to underline the fact that $v_1, \ldots, v_n$ are free.

If $\overline{g} := (g_1, \ldots, g_m)$ is an element of the $\mathcal{L}$-structure $\mathcal{M}$ and $\phi(v_1, \ldots, v_m)$ is an $\mathcal{L}$-formula with free variables $v_1, \ldots, v_m$, we write $M \models \phi(\overline{g})$ if $\phi(\overline{g})$ holds true in M and we also say that M *satisfies* $\phi(\overline{g})$. Note that we will often use the algebraists' convention of talking about the universe of a structure, rather than the structure itself, hence writing $M \models \phi(\overline{g})$ rather than $\mathcal{M} \models \phi(\overline{g})$.
For example, if we take $\phi(x)$ to be the formula $x^2 = 1$ in the previous Example 2, we have that $C_4 \models \phi(\bar{2})$ and $C_4 \not\models \phi(\bar{3})$. If instead ψ is the sentence $\forall y, z : y^{-1}z^{-1}yz = 1$ from Example 4, we have that, for every abelian group G, $G \models \psi$.

A set of sentences T is called a *theory*. An $\mathcal{L}$-structure $\mathcal{M}$ is said to be a *model* of T if $\mathcal{M} \models \phi$ for every sentence ϕ in T and we say that a theory is *satisfiable* if it has a model. Two structures are said to be *elementarily equivalent* if they satisfy the same first-order sentences.

Now that we have $\mathcal{L}$-formulas and we can express that a given formula holds true in an $\mathcal{L}$-structure, we can introduce sets that are defined by a formula.

Definition 2.2.4. Let $\mathcal{M}$ be an $\mathcal{L}$-structure. A subset $X \subseteq M^n$ is said to be *definable* if there exist an $\mathcal{L}$-formula $\phi(v_1, \ldots, v_n, w_1, \ldots, w_m)$ and elements $b_1, \ldots, b_m$ in M such that

$$X = \{(a_1, \ldots, a_n) \in M^n : \mathcal{M} \models \phi(a_1, \ldots, a_n, b_1, \ldots, b_m)\}.$$

The elements $b_1, \ldots, b_m$ are called *parameters*.

In this thesis we will always use the language of groups, therefore from now on $\mathcal{L} = \mathcal{L}_{\text{gp}}$, unless otherwise stated.

Example 2.2.5. If G is a group, its center $Z(G)$ is definable without parameters:

$$Z(G) = \{g \in G : G \models (\forall x : gx = xg)\}.$$

Here the formula defining $Z(G)$ is given by $\phi(g) : \forall x : gx = xg$.
Similarly, also the centralizer of an element of G is definable, however by a formula with parameters. If x is an element of G, then

$$C_G(x) = \{g \in G : G \models (gx = xg)\}.$$

In this case the formula is given by $\phi(g, x) : gx = xg$, where g is considered as variable and x as parameter.

Let $\mathcal{C}$ be a class of $\mathcal{L}$-structures. We say that $\mathcal{C}$ is an *elementary class* or an *axiomatizable* class if there exists a theory T such that $\mathcal{C} = \{\mathcal{M} : \mathcal{M} \models T\}$.
For example, the class of groups is axiomatizable in the language of groups by the sentences

$$\begin{aligned} &\forall x : x \cdot 1 = 1 \cdot x = x; \\ &\forall x, y, z : (x \cdot y) \cdot z = x \cdot (y \cdot z); \\ &\forall x : x \cdot x^{-1} = x^{-1} \cdot x = 1. \end{aligned} \tag{2.1}$$

If one adds to these axioms the sentence $\forall x, y : xy = yx$ one gets that also the class of abelian groups is axiomatizable.

One says that a class $\mathcal{C}$ is *finitely axiomatizable* if $\mathcal{C}$ is axiomatizable and the theory that axiomatizes $\mathcal{C}$ is finite. Note that this is equivalent to the fact that $\mathcal{C}$ is axiomatized by a single sentence, that we can take to be the conjunction of the finitely many sentences of the theory.

One fundamental result in model theory, that can be used to prove that a given property is not (finitely) axiomatizable, is the compactness theorem (see [M], Theorem 2.1.4).

Theorem 2.2.6 (Compactness)**.** *Let T be an $\mathcal{L}$-theory. Then T is satisfiable if and only if every finite subset of T is satisfiable.*

Example 2.2.7 ([Ba], Proposition 2.3)**.** The property of 'being torsion' for a group is not axiomatizable (in the language of groups), i.e., the class of torsion groups is not axiomatizable. By torsion group we mean a group where every

element has finite order, i.e., for every g there exists a natural number $n \geq 1$ such that $g^n = 1$ (in additive notation, $ng = 0$).

To prove our claim, we assume by contradiction that the class of torsion groups is axiomatized by a theory T. By using compactness, we will find a model of T that is not a torsion group. We use additive notation. Fix a new constant symbol c and consider the language $\mathcal{L} \cup \{c\}$ that extends the language of groups with the new constant c. Write ψ_n for the sentence $nc \neq 0$ for $n \geq 1$ and set $T' := T \cup \{\psi_n | n \geq 1\}$. Any finite subset S of T' is satisfiable: if $\psi_{i_1}, \ldots, \psi_{i_m}$ are the elements from $\{\psi_n | n \geq 1\}$ belonging to S, with $i_1 \leq i_2 \leq \cdots \leq i_m$, and $N > i_m$, then the finite cyclic group C_N of order N is a model of S, if we interpret the constant c as a generator of C_N. It follows by compactness that T' is satisfiable, hence there exists a non-torsion group that satisfies the theory T.

One of the proofs of the compactness theorem uses Łoś's theorem on ultraproducts (see [E], Section 5). We just recall very briefly the main definitions.

Definition 2.2.8. Let I be a non-empty set. A *filter* over I is a subset $\mathcal{U}$ of the power set of I such that:

1. the empty set does not belong to $\mathcal{U}$ and I belongs to $\mathcal{U}$;
2. if X and Y belong to $\mathcal{U}$, then $X \cap Y$ belongs to $\mathcal{U}$;
3. if $X \in \mathcal{U}$ and $X \subseteq Y \subseteq I$, then $Y \in \mathcal{U}$.

If $Y \subseteq I$ is non-empty, then $\mathcal{U} = \{X \subseteq I \mid Y \subseteq X\}$ is called the *principal filter* generated by Y. A filter $\mathcal{U}$ is called an *ultrafilter over* I if, for every $X \subseteq I$, either $X \in \mathcal{U}$ or $I \setminus X \in \mathcal{U}$.

Given a language $\mathcal{L}$ and a family of $\mathcal{L}$-structures, we can define their ultraproduct in the following way.

Definition 2.2.9. Let I be a non-empty set, $(\mathcal{A}_i \mid i \in I)$ a family of $\mathcal{L}$-structures and $\mathcal{U}$ an ultrafilter on I. Then we can define the *ultraproduct* $\prod_{i \in I} \mathcal{A}_i / \mathcal{U}$ by considering the cartesian product $\prod_{i \in I} \mathcal{A}_i$ modulo the equivalence relation $\sim_{\mathcal{U}}$ given by

$$(a_i)_{i \in I} \sim_{\mathcal{U}} (b_i)_{i \in I} \quad \Leftrightarrow \quad \{i \in I \mid a_i = b_i\} \in \mathcal{U}.$$

One can see that the ultraproduct $\prod_{i \in I} \mathcal{A}_i / \mathcal{U}$ can be made into an $\mathcal{L}$-structure (see [E], Section 2, or [TZ], Exercise 1.2.4).

We will just use the following corollary of Łoś's theorem.

Theorem 2.2.10 (Łoś; see [E], Corollary 3.2)**.** *Let $\mathcal{L}$ be a language, I an infinite set and $\mathcal{U}$ an ultrafilter on I. Let $(\mathcal{A}_i \mid i \in I)$ be a family of $\mathcal{L}$-structures. Then, for any $\mathcal{L}$-sentence ϕ, the ultraproduct $\prod_{i \in I} \mathcal{A}_i / \mathcal{U}$ satisfies ϕ if and only if $\{i \in I \mid \mathcal{A}_i \models \phi\} \in \mathcal{U}$.*

A consequence of Łoś's theorem is that, if each member of a family of groups satisfies a sentence, then also their ultraproduct satisfies the same sentence ([E], Corollary 3.3). It follows that a class of groups that is not closed under ultraproducts cannot be axiomatizable. For example, one can prove that the class of torsion groups is not axiomatizable also by showing that this class is not closed under ultraproducts (see [E], Corollary 3.4).

A consequence of the compactness Theorem is the Löwenheim-Skolem Theorem (see [TZ], Theorem 2.3.1), from which one can deduce the following ([TZ], Corollary 2.3.2):

Theorem 2.2.11. *A theory that has an infinite model has a model in every cardinality* $\kappa \geq \max(|\mathcal{L}|, \aleph_0)$.

From this result it follows, for example, that the class of finitely generated groups is not axiomatizable: finitely generated groups have at most countable cardinality but, if there was a theory axiomatizing this class, this theory would also have an uncountable model. Even more, from this it follows that no theory can axiomatize the property of being isomorphic to a given infinite group, again for cardinality reasons.

Finally, another result that we will use to prove the non-axiomatizability of a property is the following theorem proved by Feferman and Vaught ([FV], Corollary 6.7).

Theorem 2.2.12. *If the class of all models of a set of first-order sentences is closed under finite direct products, then it is closed under arbitrary direct products.*

As a matter of example, we list here some common properties of groups and state whether they are (finitely) axiomatizable or not in the first-order language of groups. See also [Ba] and [W] for more examples and explanations.

Property	**A**	**FA**	**Reason/Formula(s)**
group	yes	yes	axioms (2.1) in definition
abelian	yes	yes	axioms (2.1) $\wedge\ \forall x, y : xy = yx$
divisible	yes	no	$(\forall x \exists y : y^n = x)_{n\geq 1}$ / Compactness Theorem
finite	no	no	Łoś Theorem
finite p-group	no	no	Łoś Theorem
torsion-free	yes	no	$(\forall x : x \neq 1 \rightarrow x^n \neq 1)_{n\geq 1}$ / Compactness Theorem
torsion group	no	no	Compactness Theorem (see Example 2.2.7)
finitely generated	no	no	Löwenheim-Skolem Theorem
simple	no	no	Łoś Theorem
nilpotent	no	no	Łoś Theorem
nilpotent of class 2	yes	yes	$\forall x, y, z : [x, y, z] = 1$
soluble	no	no	Łoś Theorem

Sometimes a certain class of $\mathcal{L}$-structures is not axiomatizable but it is still axiomatizable *within* another class of $\mathcal{L}$-structures: we say that the class of $\mathcal{L}$-structures $\mathcal{C}$ is axiomatizable in the class of $\mathcal{L}$-structures $\mathcal{D}$ if there exists a theory T such that, for every $G \in \mathcal{D}$, G belongs to $\mathcal{C}$ if and only if G satisfies T.
This will be relevant to our discussion because we will always deal with axiomatizability with respect to a given class, for example the class of pro-p groups with p a fixed prime.

Example 2.2.13. Any class of groups $\mathcal{C}$ is axiomatizable in the class $\mathcal{D}$ of finite groups. Indeed, for each finite group G we can consider the sentence ϕ_G that one obtains from the multiplication table of G. Then $\mathcal{C}$ is axiomatized by the theory $\{\neg\phi_G : G \notin \mathcal{C}\}$.

The previous example shows that, when dealing with axiomatizability in the class of finite groups, the question becomes whether a certain subclass is finitely axiomatizable. Some results in this direction are:

- Simple groups are not FA within the class of finite groups ([W]);
- Non-abelian simple groups are FA within the class of finite groups ([W]);
- Soluble groups are FA within the class of finite groups ([W2]);
- Nilpotent groups are not FA within the class of finite groups ([CW]).

We conclude this section recalling some of the facts and notation frequently used in [NST] that we will often use; see [NST], Section 2.
Let G be a group and let H be a definable subgroup of G, i.e., there exists a formula $\kappa(x)$ (possibly with parameters $\overline{g}$) such that $H = \kappa(G) = \kappa(\overline{g}, G) = \{x \in G \mid G \models \kappa(\overline{g}, x)\}$.
Then, H satisfies a formula ϕ if and only if G satisfies the corresponding restricted formula, that is obtained by replacing expressions of the form $\forall x : \psi(x)$ with $\forall x : (\kappa(x) \to \psi(x))$ and expressions of the form $\exists x : \psi(x)$ with $\exists x : \kappa(x) \wedge \psi(x)$. In symbols, for any formula $\phi(y_1, \ldots, y_k)$ there is a restriction formula $\mathrm{res}(\kappa, \phi)(y_1, \ldots, y_k)$ such that

$$G \models \mathrm{res}(\kappa, \phi)(\overline{b}) \Leftrightarrow H \models \phi(\overline{b}).$$

For example, let H be a definable subgroup of G by means of a formula $\kappa(x)$. If we want to express that H is abelian we can use the formula

$$\forall g_1, g_2 : (\kappa(g_1) \wedge \kappa(g_2)) \to g_1 g_2 = g_2 g_1.$$

In a similar way, if $N = \kappa(G)$ is a definable normal subgroup of G, then there exists a lifted formula $\mathrm{lift}(\kappa, \phi)$ which satisfies

$$G \models \mathrm{lift}(\kappa, \phi)(\overline{b}) \Leftrightarrow G/N \models \phi(\tilde{b}_1, \ldots, \tilde{b}_k),$$

where, for each $i = 1, \ldots, k$, $\tilde{b}_i$ is the image of b_i under the projection map $G \to G/N$. Such a formula is obtained by replacing each atomic formula $x = y$ in ϕ with $\kappa(x^{-1}y)$.
Moreover, $\kappa(G)$ is a subgroup of G if and only if $G \models s(\kappa)$, where

$$s(\kappa) := \exists x : \kappa(x) \ \wedge \ \forall x, y : (\kappa(x) \wedge \kappa(y) \to \kappa(x^{-1}y))$$

and $\kappa(G)$ is a normal subgroup if and only if $G \models s_\triangleleft(\kappa)$, where

$$s_\triangleleft(\kappa) := s(\kappa) \ \wedge \ \forall x, y : (\kappa(x) \to \kappa(y^{-1}xy)).$$

2.2.2 A brief overview on the finite axiomatizability of profinite groups

The concept of finite axiomatizability used in [NST] is a generalization of the concept of *quasi-finite-axiomatizability* introduced in [N1] by Nies. This stems from the study of which properties of a group are axiomatizable by a set of sentences

in first-order logic. We already saw in the previous section that some properties of groups are not axiomatizable but they become such if we restrict the class of groups under consideration. One of the strongest properties of a group G is being isomorphic to G. Hence the following question naturally arises: given a group G, does there exist a set of sentences T such that, for any given group H, the theory of H is T if and only if H is isomorphic to G? We already noted that, given an infinite finitely generated group G, the property of being isomorphic to G cannot be axiomatizable because of the Löwenheim-Skolem Theorem. Therefore one sees immediately that some kind of restriction on the class of groups under consideration is necessary. Moreover, in [N1], Nies observes that even restricting to the class of countable groups is not enough. Indeed, for any finitely generated group G there exists a countable group that has the same theory as G but is not isomorphic to G. Therefore he considers the class of finitely generated groups and defines a finitely generated group G to be *quasi-axiomatizable* if, given any finitely generated group H with the same theory as G, H is isomorphic to G. In the same spirit, working in the realm of profinite groups, Jarden and Lubotzky proved that, if two profinite groups have the same theory and one of them is finitely generated, then the two groups are isomorphic ([JL], Theorem A). However, the situation for abstract groups is more complicated. For example, in [N1], Nies points out that there exists a finitely generated torsion-free nilpotent group of class 3 that is not quasi-axiomatizable. This follows from an example of Hirshon of such a group G for which there exists a group H with $G \times \mathbb{Z} \cong H \times \mathbb{Z}$ but $G \ncong H$ (see [H], Section 3, page 154). By a result of Oger ([O]), two finitely generated nilpotent groups G and H have the same theory if and only if $G \times \mathbb{Z} \cong H \times \mathbb{Z}$ and therefore G and H from Hirshon's example are elementarily equivalent but not isomorphic. However, Nies observes that there are classes of quasi-axiomatizable groups, such as finitely generated abelian groups and torsion-free finitely generated nilpotent groups of class 2. Even more, in his investigation he finds out that there are finitely generated groups that are completely determined (among finitely generated groups) by a single first-order sentence. This leads him to the following definition:

Definition 2.2.14. A finitely generated group G is *quasi-finitely axiomatizable* (QFA) if there exists a first-order sentence ϕ such that, for every finitely generated group H, H satisfies ϕ if and only if H is isomorphic to G.

For example, he proves that, if p is a prime number, then the restricted wreath product $C_p \wr \mathbb{Z}$ is quasi-finitely axiomatizable ([N1], Theorem 2.3). See [N2], Section 7, for more examples and results.

In [NST], Nies, Segal and Tent extend the previous definition in the following way:

Definition 2.2.15. Let $\mathcal{C}$ be a class of groups and $\mathcal{L}$ a language. We say that a group G belonging to $\mathcal{C}$ is *finitely axiomatizable* (FA) in $\mathcal{C}$ with respect to $\mathcal{L}$ if there is a sentence ϕ in the language $\mathcal{L}$ such that, for any group $H \in \mathcal{C}$, H satisfies ϕ if and only if H is isomorphic to G.

If the class of groups under consideration is a class of topological groups, such as the class of profinite groups or pro-p groups, the isomorphism in the definition is required to be a continuous map.
Observe that QFA just means FA in the class $\mathcal{C}$ of finitely generated groups.

To give some examples of FA profinite groups, regarding p-adic analytic groups, in [NST] the authors prove, among many other results, that a pro-p group of finite rank given by the pro-p completion of an (abstractly) finitely presented group is finitely axiomatizable in the class of pro-p groups ([NST], Theorem 1.6) and that, if $d \geq 2$ and p is an odd prime with $p \nmid d$, then each of the groups $\mathrm{SL}_d^1(\mathbb{Z}_p)$, $\mathrm{SL}_d(\mathbb{Z}_p)$ and $\mathrm{PSL}_d(\mathbb{Z}_p)$ is finitely axiomatizable in the class of profinite groups. It is an open question to establish whether a finitely generated non-abelian free pro-p group is finitely axiomatizable in the class of profinite groups ([NST], Section 1.5, Problem 3).

By abuse of notation we will also say that a property $\mathcal{P}$ is finitely axiomatizable for groups of a certain class $\mathcal{C}$ if there exists a single first-order sentence ϕ such that a group G in $\mathcal{C}$ has property $\mathcal{P}$ if and only if G satisfies ϕ.

2.2.3 Some model theory of $\mathcal{C}_\pi$ groups

Given a finite set of primes $\pi := \{p_1, \dots, p_k\}$, we follow [NST] in calling groups of the form $G_1 \times \cdots \times G_k$, where each G_i is a pro-p_i group, $\mathcal{C}_\pi$ *groups*; equivalently, a $\mathcal{C}_\pi$ group is a pronilpotent group whose Sylow subgroups are pro-p_i groups, with $p_i \in \pi$ (Proposition 1.1.22).

The class of finitely generated $\mathcal{C}_\pi$ groups is particularly nice from a first-order point of view. To start with, as we will explain below, one can express the fact that d elements of a $\mathcal{C}_\pi$ group G are generators of G.
To avoid repetition, from now on π will denote a finite set of primes $\{p_1, \dots, p_k\}$ and we will denote as usual with $\mathrm{d}(G)$ the minimal number of generators of G.

We start by recalling a crucial fact established in [NST], Section 5.1.

Lemma 2.2.16 ([NST])**.** *If G is a finitely generated $\mathcal{C}_\pi$ group and $q(\pi) := p_1 \cdots p_k$, then its Frattini subgroup*

$$\Phi(G) := [G, G]G^{q(\pi)}$$

is definable.

Proof. If G is generated by elements $a_1, \dots, a_d$, then

$$[G, G] = [a_1, G] \cdots [a_d, G]$$

(see Proposition 1.2.2). Recall that $G^{q(\pi)}$ denotes the group generated by the $q(\pi)$-th powers of the elements of G, while $G^{\{q(\pi)\}}$ denotes the subset of G consisting of the $q(\pi)$-th powers of the elements of G. Since $[G, G]G^{q(\pi)} = [G, G]G^{\{q(\pi)\}}$, we can define $\Phi(G)$ by means of the formula with parameters $\phi_1 = \phi_1(a_1, \dots, a_d, G)$ given by

$$\phi_1(a_1, \dots, a_d, x) \ := \ \exists z, y_1, \dots, y_d : x = [a_1, y_1] \cdots [a_d, y_d] z^{q(\pi)}.$$

□

Thanks to the fact that the Frattini subgroup of a finitely generated $\mathcal{C}_\pi$ group is definable, for each integer $d \geq 1$, we can write a formula β_d (depending on π) with parameters $a_1, \dots, a_d$ that expresses the fact that a $\mathcal{C}_\pi$ group is generated by $a_1, \dots, a_d$ ([NST], Proposition 5.3). As the existence of such a formula is a crucial part in being able to express properties of $\mathcal{C}_\pi$ groups and as we will need it later to study the complexity of our sentences, we recall the precise statement and its proof here.

Lemma 2.2.17 ([NST]). *Given a positive integer d, there exists a formula (with parameters) β_d such that, for a $\mathcal{C}_\pi$ group G,*

$$G \models \beta_d(a_1, \dots, a_d) \Leftrightarrow G = \overline{\langle a_1, \dots, a_d \rangle}.$$

Proof. The idea to write this formula is to use the fact that the quotient $G/\Phi(G)$ is a finite direct product of elementary abelian groups, each of order dividing $q(\pi)$. Since $\Phi(G)$ is definable in a finitely generated $\mathcal{C}_\pi$ group, we just need to write that each element of G belongs to one of the finitely many cosets of $G/\Phi(G)$.
We first need to express the fact that, if G is d-generated, then the commutator word has width d in G. To do so, given $a_1, \dots, a_d$ generators of G, we say that the product of any $d+1$ commutators belongs to $[a_1, G] \cdots [a_d, G]$ by means of the formula $w(a_1, \dots, a_d)$:

$$\forall x_1, y_1, \dots, x_{d+1}, y_{d+1} \exists z_1, \dots, z_d : [x_1, y_1] \cdots [x_{d+1}, y_{d+1}] = [a_1, z_1] \cdots [a_d, z_d].$$

Note that, if G satisfies $w(a_1, \dots, a_d)$, then it follows automatically that the set $[a_1, G] \cdots [a_d, G]$ is a subgroup of G. Moreover, G satisfies $w(a_1, \dots, a_d)$ if and only if $[G, G] = [a_1, G] \cdots [a_d, G]$.
We now write that every element x in G belongs to one of the finitely many cosets of $G/\Phi(G)$, that are of the form $a_1^{s(1)} \cdots a_d^{s(d)} \Phi(G)$ for $s(1), \dots, s(d)$ belonging to the set $S := \{0, 1, \dots, q(\pi) - 1\}$. This can be done by saying that $x^{-1} a_1^{s(1)} \cdots a_d^{s(d)}$ belongs to $\Phi(G)$, i.e., that G satisfies $\phi_1(a_1, \dots, a_d, x^{-1} a_1^{s(1)} \cdots a_d^{s(d)})$. In conclusion, let $\beta_d(a_1, \dots, a_d)$ be the formula

$$w(a_1, \dots, a_d) \wedge \forall x : \bigvee_{s(1), \dots, s(d) \in S} \phi_1(a_1, \dots, a_d, x^{-1} a_1^{s(1)} \cdots a_d^{s(d)}).$$

Then, from the previous considerations, it is clear that if G is generated by $a_1, \dots, a_d$ then G satisfies $\beta_d(a_1, \dots, a_d)$. Conversely, if G is a $\mathcal{C}_\pi$ group that satisfies $\beta(a_1, \dots, a_d)$, then $G' = [a_1, G] \cdots [a_d, G]$ and every element x in G belongs to $a_1^{s(1)} \cdots a_d^{s(d)} [a_1, G] \cdots [a_d, G] G^{q(\pi)}$ for some $s(1), \dots, s(d)$ in S. It follows that

$$G \subseteq \langle a_1, \dots, a_d \rangle [a_1, G] \cdots [a_d, G] G^{q(\pi)} = \langle a_1, \dots, a_d \rangle G' G^{q(\pi)} = \langle a_1, \dots, a_d \rangle \Phi(G),$$

i.e., G is (topologically) generated by $a_1, \dots, a_d$.

□

From β_d one can easily obtain sentences $\tilde{\beta}_d$ and β_d^* (depending on π) such that, for a $\mathcal{C}_\pi$ group G,

$$G \models \tilde{\beta}_d \Leftrightarrow \mathrm{d}(G) \leq d,$$
$$G \models \beta_d^* \Leftrightarrow \mathrm{d}(G) = d.$$

These sentences are given by

$$\tilde{\beta}_d := \exists a_1, \dots, a_d : \beta_d(a_1, \dots, a_d)$$

and

$$\beta_d^* := \tilde{\beta}_d \wedge \neg \tilde{\beta}_{d-1}.$$

Therefore, the property of a $\mathcal{C}_\pi$ group of being d-generated can be expressed by one single first-order sentence, i.e., it is a finitely axiomatizable property.

It is interesting to note that the same is not true for profinite groups, i.e., in the class of profinite groups the property of being d-generated, as well as the property of being finitely generated, cannot be expressed by a single first-order sentence ([NST], Proposition 5.4).

If the $\mathcal{C}_\pi$ group G has finite rank, by iteration also the higher Frattini subgroups $\Phi^m(G)$ $(m \geq 1)$, defined recursively by $\Phi^m(G) := \Phi(\Phi^{m-1}(G))$, can be characterized by a first-order formula (with parameters) ϕ_m.
More precisely, let $\mathrm{rk}(G) = r$ and define ϕ_1 and β_r as before, taking $d = r$. Then $\Phi(G)$ has rank bounded by r and therefore there exist elements $b_1^{(1)}, \ldots, b_r^{(1)}$ in $\Phi(G)$ such that $\Phi(G) = \overline{\langle b_1^{(1)}, \ldots, b_r^{(1)} \rangle}$. It follows that

$$\Phi(\Phi(G)) = \{x \in \Phi(G) | \ \exists w, t_1, \ldots, t_r \in \Phi(G) : x = [b_1^{(1)}, t_1] \cdots [b_r^{(1)}, t_r] w^{q(\pi)}\}.$$

Hence, $\Phi(\Phi(G))$ is defined in G by the formula

$$\phi_2 = \phi_2(b_1^{(1)}, \ldots, b_r^{(1)}, x) := \mathrm{res}(\phi_1, \phi_1(b_1^{(1)}, \ldots, b_r^{(1)}, x)),$$

where the parameters $b_1^{(1)}, \ldots, b_r^{(1)}$ can be described implicitly by the formula

$$\mathrm{res}(\phi_1, \beta_r(b_1^{(1)}, \ldots, b_r^{(1)})),$$

which describes the fact that $\Phi(G)$ is generated by $b_1^{(1)}, \ldots, b_r^{(1)}$.

In the same way one can find generators $b_1^{(2)}, \ldots, b_r^{(2)}$ of $\Phi(\Phi(G))$ and iterate the process just described, thus finding, for each $m \geq 1$, the formula $\phi_m(b_1^{(m-1)}, \ldots, b_r^{(m-1)}, x)$.

Note that when we want to talk about properties of the Frattini subgroup of a pro-p group G with rank r by means of a formula ψ, we need to include $\tilde{\beta}_r$ in ψ, since the generators of G are needed in the formula ϕ_1. The same is true for the iterated Frattini subgroup $\Phi^m(G)$ for $m \geq 2$ and moreover, in this case, we also need the generators of all the iterated Frattini subgroups $\Phi^k(G)$ for $k \in \{1, \ldots, m-1\}$, i.e., we have to add, for $k \in \{1, \ldots, m-1\}$, all the sentences $\exists b_1^{(k)}, \ldots, b_r^{(k)} : \bigwedge_{i=1}^r \phi_k(b_i^{(k)}) \wedge \Phi^k(G) \models \beta_r(b_1^{(k)}, \ldots, b_r^{(k)})$, where $\Phi^k(G) \models \beta_r(b_1^{(k)}, \ldots, b_r^{(k)})$ is given by $\mathrm{res}(\phi_k, \beta_r(b_1^{(k)}, \ldots, b_r^{(k)}))$. As we will often need to speak of the iterated Frattini subgroup and writing such a sentence would be rather long, we make the following shortcuts.
If G is a pro-p group of finite rank r we will denote by ϕ_m^G the formula defining $\Phi^m(G)$ in G, that is given by

$$\phi_0^G = \phi_0 \ := \ \exists b_1^{(0)}, \ldots, b_r^{(0)} : \beta_r(b_1^{(0)}, \ldots, b_r^{(0)})$$

for $m = 0$ and, for $m \geq 1$, by

$$\begin{aligned}
\phi_m^G(x) \ := \ & \exists b_1^{(0)}, \ldots, b_r^{(0)} : \beta_r(b_1^{(0)}, \ldots, b_r^{(0)}) \ \wedge \bigwedge_{k=1}^{m-1} \exists b_1^{(k)}, \ldots, b_r^{(k)} : \\
& \bigwedge_{k=1}^{m-1} \bigwedge_{i=1}^{r} \phi_k(b_1^{(k-1)}, \ldots, b_r^{(k-1)}, b_i^{(k)}) \ \wedge \bigwedge_{k=1}^{m-1} \mathrm{res}(\phi_k, \beta_r(b_1^{(k)}, \ldots, b_r^{(k)})) \\
& \wedge \ \exists w, t_1, \ldots, t_r : \phi_{m-1}(b_1^{(m-1)}, \ldots, b_r^{(m-1)}, w) \\
& \wedge \bigwedge_{i=1}^{r} \phi_{m-1}(b_1^{(m-1)}, \ldots, b_r^{(m-1)}, t_i) \ \wedge \ x = [b_1^{(m-1)}, t_1] \cdots [b_r^{(m-1)}, t_r] w^{q(\pi)}.
\end{aligned}$$

The first term of the formula expresses the fact that $b_1^{(0)}, \dots, b_r^{(0)}$ generate G, the second and third terms say that, for each $k \in \{1, \dots, m-1\}$, the elements $b_1^{(k)}, \dots, b_r^{(k)}$ belong to $\Phi^k(G)$ and generate $\Phi^k(G)$ and the last three terms are the definition of $\Phi^m(G)$. Note that with these last three terms, that form the last two lines of the formula $\phi_m^G(x)$, we are just explicitly writing out $\mathrm{res}(\phi_{m-1}, \phi_m(b_1^{(m-1)}, \dots, b_r^{(m-1)}, x))$.

Remark 2.2.18. Note that the previous sentence ϕ_m^G that defines $\Phi^m(G)$ implicitly states also that $\mathrm{d}(\Phi^i(G)) \leq r$ for each $0 \leq i \leq m-1$.

Finally, it is worth noting that, when we want to express something of the form

$$\Phi^m(G) \models \psi_1 \ \wedge \ \Phi^m(G) \models \psi_2 \ \wedge \ G/\Phi^m(G) \models \psi_3 \ \wedge \ ...$$

we will write it as

$$\mathrm{res}(\phi_m^G, \psi_1) \ \wedge \ \mathrm{res}(\phi_m^G, \psi_2) \ \wedge \ \mathrm{lift}(\phi_m^G, \psi_3) \ \wedge \ ...$$

but, if needed, we can assume that we are choosing the same sets of generators at each step in the formulas for ϕ_m^G.

Even if we will not make use of it, note that a similar argument can be used to define the iterated Frattini subgroups when it is known that G is d-generated but the rank of G is not known. In this case one can use the Schreier formula to bound the number of generators at each step (see Proposition 1.1.10).

Later we will also need the following fact, of which we briefly sketch the proof.

Lemma 2.2.19. *If $G = G_1 \times \cdots \times G_k$, then*

$$\Phi(G) \cong \Phi(G_1) \times \cdots \times \Phi(G_k).$$

Proof. Recall that this isomorphism holds for a finite group ([Mi]) and that, if $\{G_i\}_{i \in I}$ is an inverse system of finite groups, then $\Phi(\varprojlim_{i \in I}(G_i)) = \varprojlim_{i \in I}(\Phi(G_i))$ ([RZ], Proposition 2.8.2, (c)). It follows that, if we denote by $\mathcal{U}$ the set of open normal subgroups of G,

$$\begin{aligned}\Phi(G) &= \Phi(\varprojlim_{U \in \mathcal{U}}(G/U)) = \varprojlim_{U \in \mathcal{U}} \Phi(G/U) = \varprojlim_{U \in \mathcal{U}} \Phi(\frac{G_1}{G_1 \cap U} \times \cdots \times \frac{G_k}{G_k \cap U}) \\ &= \Phi(\varprojlim_{U \in \mathcal{U}}(\frac{G_1}{G_1 \cap U})) \times \cdots \times \Phi(\varprojlim_{U \in \mathcal{U}}(\frac{G_k}{G_k \cap U})) = \Phi(G_1) \times \cdots \times \Phi(G_k).\end{aligned}$$

By induction, we obtain, for every $m \geq 1$,

$$\Phi^m(G) \cong \Phi^m(G_1) \times \cdots \times \Phi^m(G_k).$$

□

Finally, if G is a $\mathcal{C}_\pi$ group, we say, as in [NST], that G is *semi-powerful* (respectively *semi-uniform*) if each direct factor of G is powerful (respectively uniform). If G is a $\mathcal{C}_\pi$ group of finite rank r, for each $i \in \{1, \dots, k\}$ we set $r_i := \mathrm{rk}(G_i)$ and

$$m(r_i) := \lceil \log_2(r_i) + \varepsilon_{p_i} \rceil,$$

with

$$\varepsilon_{p_i} := \begin{cases} 0, & \text{if } p_i \neq 2 \\ 1, & \text{if } p_i = 2 \end{cases}.$$

If $m(r) := \max_{i=1,\dots,k} m_i$, then $\Phi^{m(r)}(G)$ is semi-powerful ([NST], Theorem 5.7) and being (semi)powerful is a first-order property: a finitely generated $\mathcal{C}_\pi$ group P is semi-powerful if and only if

$$P \models \text{pow} := \forall x, y \, \exists z : ([x, y] = z^{q'(\pi)}),$$

where $q'(\pi) := 2^{\varepsilon_\pi} q(\pi)$, with $\varepsilon_\pi = 0$ if $2 \notin \pi$ and $\varepsilon_\pi = 1$ if $2 \in \pi$ ([NST], Section 5.2).
Note that

$$m(r) \leq \lceil \log_2(r) + \varepsilon_\pi \rceil. \tag{2.2}$$

Let F be a definable semi-powerful subgroup of G defined by a formula θ; then each term $P_i(F)$ $(i \geq 1)$ of the lower $q(\pi)$-series of F is definable in G. Indeed, since F is semi-powerful, we have that

$$P_i(F) = F^{q(\pi)^{i-1}} = \{x^{q(\pi)^{i-1}} | x \in F\}$$

for all $i \geq 1$ ([DDMS], Theorem 3.6). Hence $P_i(F)$ is defined in F by the formula $\widetilde{\pi_i^F}(z) := \exists x : z = x^{q(\pi)^{i-1}}$ and it is defined in G by the formula $\pi_i^F := \text{res}(\theta, \widetilde{\pi_i^F})$.

2.2.4 The problem of the finite axiomatizability of the rank

As stated in the introduction of this chapter, the problem of the finite axiomatizability of the rank of a p-adic analytic pro-p group has its origin in the paper [NST] and has a natural place in the general framework of studying first-order properties of profinite groups, in this case in particular of pro-p groups. In the already mentioned paper, Nies, Segal and Tent state Proposition 1, that we write here again for convenience.

Proposition 2.2.20. *For each positive integer r, there is a sentence $\rho_{p,r}$ in the language of groups such that, for a pro-p group G,*

$$\text{rk}(G) \leq r \quad \Rightarrow \quad G \models \rho_{p,r} \quad \Rightarrow \quad \text{rk}(G) \leq r(2 + \log_2(r)).$$

They observe that, at a first glance, the property of having fixed rank r does not seem to be axiomatizable. Indeed, if one uses the definition of rank to write a sentence axiomatizing the fact that a given pro-p group G has rank r, one needs to quantify over subgroups of G, which is not allowed in first-order logic.

We will prove in this thesis that the property of having a fixed finite rank is actually finitely axiomatizable in the class of pro-p groups. What will allow us to do so is a result that states that we can read the rank of a pro-p group G in a finite definable quotient of G.

Before illustrating our results we spell out in some detail the proof of Proposition 2.2.20, as it is just sketched in the paper [NST]. Contrary to most of the proofs that will follow, here we just describe the sentence without writing it out in detail.

Proof of Proposition 2.2.20. Let G be a pro-p group with rank at most r and let

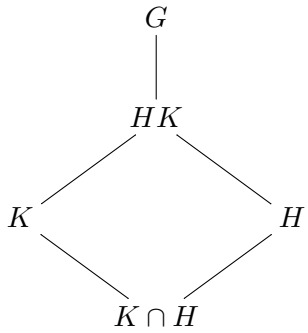
$$m := m(r) := \lceil \log_2(r) + \varepsilon_p \rceil,$$

with

$$\varepsilon_p := \begin{cases} 0, & \text{if } p \neq 2 \\ 1, & \text{if } p = 2 \end{cases}.$$

By [NST], Theorem 5.7, and the previous considerations in Section 2.2.3, the iterated Frattini group $\Phi^m(G)$ is a definable powerful normal subgroup of G whose index is bounded by p^{rm}. The latter bound is obtained considering that each quotient $\Phi^i(G)/\Phi^{i+1}(G)$, for $i \geq 0$, is an elementary abelian p-group with rank bounded by r. Therefore, $G/\Phi^m(G)$ is a definable quotient of G and a finite p-group with order bounded by p^{rm}. Moreover, since $\Phi^m(G)$ is powerful, $\mathrm{d}(\Phi^m(G)) = \mathrm{rk}(\Phi^m(G)) \leq r$ and we can express this fact with the first-order sentence $\tilde{\beta}_r$. Hence, let $\rho_{p,r}$ be the first-order sentence that expresses the fact that $\Phi^m(G)$ is powerful with $\mathrm{d}(\Phi^m(G)) \leq r$ and that the quotient $G/\Phi^m(G)$ is a finite group with order bounded by p^{rm}. It is clear that any pro-p group of rank bounded by r satisfies $\rho_{p,r}$.

Assume now that G is a pro-p group satisfying $\rho_{p,r}$ and set $H := \Phi^m(G)$. Let K be a closed subgroup of G and consider $K \cap H$.



Since G satisfies $\rho_{p,r}$, we know that the rank of H is r and, therefore, $\mathrm{d}(K \cap H) \leq r$. Now $\mathrm{d}(K) \leq \mathrm{d}(K \cap H) + \mathrm{d}(K/K \cap H) = \mathrm{d}(K \cap H) + \mathrm{d}(HK/H)$. Thus we want an upper bound for $\mathrm{d}(HK/H)$. By remark 2.2.18 we know that $\mathrm{d}(\Phi^i(G)) \leq r$ for each $0 \leq i \leq m-1$. Hence $\mathrm{d}(\Phi^i(G)/\Phi^{i+1}(G)) \leq r$ for each $0 \leq i \leq m-1$. As each factor $\Phi^i(G)/\Phi^{i+1}(G)$ is an elementary abelian group also $\mathrm{rk}(\Phi^i(G)/\Phi^{i+1}(G)) \leq r$ and therefore $\mathrm{d}((K \cap \Phi^i(G))\Phi^{i+1}(G)/\Phi^{i+1}(G)) \leq r$ for each $0 \leq i \leq m-1$. From this it follows that $\mathrm{d}(HK/H) = \mathrm{d}(\Phi^m(G)K/\Phi^m(G)) \leq rm$. Therefore, $\mathrm{d}(K) \leq r(1+m) \leq r(2+\log_2 r)$. Since K is an arbitrary closed subgroup of G, the result follows.

□

Remark 2.2.21. As $G/\Phi^m(G)$ has bounded order, we can add to $\rho_{p,r}$ a term stating that $G/\Phi^m(G)$ is one of the finitely many possible groups of rank at most r. In this way we can improve the upper bound $r(2+\log_2(r))$ in the previous proposition to $2r$.

Finally, it is interesting to note that, because of the result of Feferman and Vaught (Proposition 2.2.12), it is not possible to axiomatize the property of

'having finite rank'. Indeed, by using the fact that an extension of two pro-p groups of finite rank has again finite rank (Proposition 1.1.14) and induction on the number of factors, one sees that every finite cartesian product of pro-p groups of finite rank is again a pro-p group of finite rank. However, an infinite cartesian product of non-trivial pro-p groups of finite rank does not have finite rank.

Example 2.2.22. The pro-p group $C_p^{\aleph_0}$ given by the direct product of countably many copies of C_p has not finite rank as it is not even finitely generated. However every finite direct product C_p^n has finite rank.

Observe that the same example shows that also the property of being finitely generated cannot be axiomatized within the class of pro-p groups.

Then the question arises: is it possible to find a class of pro-p groups in which the property of having finite rank is axiomatizable? For example, fix a positive integer d and consider the class $\mathcal{C}$ of pro-p groups with minimal number of generators bounded by d. Assume that there exists a sentence ϕ that expresses the fact that a group in $\mathcal{C}$ has finite (unbounded) rank. Then the previous example ceases to be an issue as $C_p^{\aleph_0}$ is a model of ϕ not belonging to the class $\mathcal{C}$ under consideration (see Section 2.9 for a list of questions).

2.3 Finite axiomatizability of the rank of $\mathcal{C}_\pi$ groups

In this section we prove that the rank of a p-adic analytic pro-p group is finitely axiomatizable. This result follows immediately from the slightly more general fact that the rank of any pronilpotent group of finite rank is finitely axiomatizable.

The main tool that we need is a result that allows us to detect the rank of a p-adic analytic pro-p group G in a finite quotient of G. More precisely, assume that we have an upper bound λ on the rank of G. We will then find a normal subgroup H_λ with finite index in G bounded by $p^{f(\lambda)}$ for a certain function f, such that $\mathrm{rk}(G) = \mathrm{rk}(G/H_\lambda)$. This will help us in the following way. In the first part of the proof of the finite axiomatizability of the rank we will write a sentence that is satisfied by any pro-p group of a given rank r and that gives us an upper bound $\lambda := \lambda(r)$ for the rank of any pro-p group satisfying it, similarly to what happens in Proposition 2.2.20. We will then add a term to our sentence which states that $\mathrm{rk}(G/H_\lambda) = r$. Then, thanks to our main tool, every pro-p group that satisfies the sentence that we produced has rank r.

Let G be a pro-p group of finite rank. We start by recalling that, if F is a powerful pro-p subgroup of G, then the lower p-series of F forms a base of neighbourhoods of the identity in G (see Section 1.3) and therefore, by Remark 1.1.13,

$$\mathrm{rk}(G) = \sup\{\mathrm{rk}(G/P_j(F)) \mid j \geq 1, j \in \mathbb{N}\} = \max\{\mathrm{rk}(G/P_j(F)) \mid j \geq 1, j \in \mathbb{N}\}.$$

It is then natural to look for the smallest positive integer j such that $\mathrm{rk}(G) = \mathrm{rk}(G/P_j(F))$. In the following result we find a positive integer k that is dependent on a bound on $\mathrm{rk}(G)$ such that $\mathrm{rk}(G) = \mathrm{rk}(G/P_k(F))$. Example 2.3.3 shows that the approach used in the proof of this result is not suitable for finding an index independent of $\mathrm{rk}(G)$; it remains open to determine if such an index exists.

Theorem 2.3.1. *Let R be a positive integer and let G be a pro-p group of rank $\mathrm{rk}(G) \leq R$. Suppose that $F \trianglelefteq_o G$ is powerful. Then $\mathrm{rk}(G) = \mathrm{rk}(G/P_{2R+1}(F))$.*

Before starting with the proof we need a lemma.

Lemma 2.3.2. *Let G be a (not necessarily infinite) pro-p group with $\mathrm{d}(G) = d$ and let N be a normal subgroup of G. Let $m := \mathrm{d}(G/N)$ and $\bar{y}_1, \ldots, \bar{y}_m$ a minimal generating set for this quotient. Then there exist $z_1, \ldots, z_{d-m}$ in N such that $y_1, \ldots, y_m, z_1, \ldots, z_{d-m}$ form a minimal generating set for G.*

Proof. The quotient $(G/N)/\Phi(G/N)$ is a finite dimensional $\mathbb{F}_p$-vector space of dimension $\mathrm{d}(G/N) = m$ with basis given by the images of $\bar{y}_1, \ldots, \bar{y}_m$. By abuse of notation we write again $\bar{y}_1, \ldots, \bar{y}_m$ to denote the images of these elements in the quotient $(G/N)/\Phi(G/N)$. Since G is a pro-p group, $\Phi(G/N) \cong \Phi(G)N/N$ and therefore $(G/N)/\Phi(G/N) \cong G/\Phi(G)N$. The latter group is in turn isomorphic to the quotient of $G/\Phi(G)$ by $\Phi(G)N/\Phi(G)$. It follows that we can lift the images of the basis $\bar{y}_1, \ldots, \bar{y}_m$ of $(G/N)/\Phi(G/N)$ to $\tilde{y}_1, \ldots, \tilde{y}_m$ in $G/\Phi(G)$ and extend to a basis of $G/\Phi(G)$ by means of elements $\tilde{z}_1, \ldots, \tilde{z}_{d-m}$ in $\Phi(G)N/\Phi(G)$. Lifting to G we obtain a minimal system of generators $y_1, \ldots, y_m, z_1, \ldots, z_{d-m}$ with the required properties. □

Proof of Theorem 2.3.1. For convenience, write $F_i = P_i(F)$ for the terms of the lower p-series of the powerful group F. For a contradiction, we assume that $\mathrm{rk}(G) > \mathrm{rk}(G/F_{2R+1})$. Consider $H \leq_{\mathrm{o}} G$ with $\mathrm{rk}(G) = \mathrm{d}(H) =: r$. Since the sequence $\{F_j\}_j$ is decreasing and $\bigcap_j F_j = 1$, the sequence $\mathrm{d}(HF_j/F_j)$, $j \in \mathbb{N}$, is non-decreasing and eventually constant, with final constant value $\mathrm{d}(H)$. Since $\mathrm{d}(H) \leq R < 2R+1$, we conclude that $\mathrm{d}(HF_j/F_j)$, $j \in \mathbb{N}$, cannot be strictly increasing until it becomes constant. Indeed, if this sequence was strictly increasing, there would be an index i_0, with $1 \leq i_0 \leq r = \mathrm{d}(H) \leq R < 2R+1$, such that $\mathrm{d}(HF_{i_0}/F_{i_0}) = \mathrm{d}(H) = r$, contradicting the fact that $r = \mathrm{rk}(G) > \mathrm{rk}(G/F_{2R+1})$. Consequently, we may choose H such that $j = j(H) \in \mathbb{N}$ is minimal with regard to the following property:

$$\begin{aligned}\mathrm{d}(HF_j/F_j) = \mathrm{d}(HF_{j+1}/F_{j+1}) < \mathrm{d}(HF_{j+2}/F_{j+2}) \\ < \ldots < \mathrm{d}(HF_{j+k+1}/F_{j+k+1}) = \mathrm{d}(H)\end{aligned} \quad (2.3)$$

for suitable $k = k(H)$ with $1 \leq k \leq r \leq R$.

In particular, this set-up implies that $j + k + 1 > 2R + 1$, for otherwise we would contradict the assumption $\mathrm{d}(H) = \mathrm{rk}(G) > \mathrm{rk}(G/F_{2R+1})$. Hence $j > R$ and $2j \geq j + R + 1 \geq j + k + 1$. Consequently,

$$[F_j, F_j] \subseteq F_{2j} \subseteq F_{j+k+1}. \quad (2.4)$$

We set $m = \mathrm{d}(HF_{j+1}/F_{j+1})$, choose $y_1, \ldots, y_m \in H$ such that $\langle y_1, \ldots, y_m \rangle \leq_{\mathrm{c}} H$ satisfies $\langle y_1, \ldots, y_m \rangle F_{j+1} = HF_{j+1}$ and set

$$L := \langle y_1, \ldots, y_m \rangle.$$

As $\mathrm{d}(HF_j/F_j) = \mathrm{d}(HF_{j+1}/F_{j+1})$, we gain for free the extra information $LF_j = HF_j$. Next we put $\ell = \mathrm{d}(H) - m$ and, by using Lemma 2.3.2, we complement $y_1, \ldots, y_m$ to a minimal generating system for H, by choosing successively suitable $w_1, \ldots, w_\ell \in F_{j+1}$: the first few elements $w_1, \ldots, w_{l(1)}$ are chosen in F_{j+1} to obtain a minimal generating system $y_1, \ldots, y_m, w_1, \ldots, w_{l(1)}$ modulo F_{j+2}, the

next elements $w_{l(1)+1}, \ldots, w_{l(2)}$ are chosen from F_{j+2} to obtain a minimal generating system $y_1, \ldots, y_m, w_1, \ldots, w_{l(2)}$ modulo F_{j+3} et cetera. We write $l(0) = 0$ and deduce from (2.3) that $0 = l(0) < l(1) < l(2) < \ldots < l(k) = \ell$.

As F is powerful, $F_{j+1} = \{x^p \mid x \in F_j\}$. Thus we find $z_1, \ldots, z_\ell \in F_j$ with $w_i = z_i^p$ for $1 \leq i \leq \ell$. Observe that $w_{l(i-1)+1}, \ldots, w_{l(i)} \in F_{j+i} \setminus F_{j+i+1}$ for $1 \leq i \leq k$ and therefore $z_{l(i-1)+1}, \ldots, z_{l(i)} \in F_{j+i-1} \setminus F_{j+i}$ for $1 \leq i \leq k$: if, without loss of generality, $z_{l(i-1)+1}$ was in F_{j+i}, then $z_{l(i-1)+1}^p = w_{l(i-1)+1}$ would be in F_{j+i+1}, in contradiction with our choice of $w_{l(i-1)+1}$.

We claim that $y_1, \ldots, y_m, z_1, \ldots, z_\ell$ is a minimal generating system for the group

$$\widetilde{H} = \langle y_1, \ldots, y_m, z_1, \ldots, z_\ell \rangle \leq_{\mathrm{c}} G,$$

(hence $\widetilde{H} \leq_{\mathrm{o}} G$ and $\mathrm{d}(\widetilde{H}) = m + \ell = \mathrm{d}(H) = \mathrm{rk}(G) = r$), and correspondingly that

$$\mathrm{d}(\widetilde{H}F_j/F_j) < \mathrm{d}(\widetilde{H}F_{j+1}/F_{j+1}) < \ldots < \mathrm{d}(\widetilde{H}F_{j+k}/F_{j+k}) = \mathrm{d}(\widetilde{H}), \tag{2.5}$$

in contradiction to our initial choice of H with the aim of minimising $j = j(H)$.

In order to prove these claims we may work in the group $G_0 = HF_j = \widetilde{H}F_j = LF_j \leq_{\mathrm{o}} G$. First note that we can quotient by F_{2j} because, by (2.4), the minimal number of generators of the image of H in G_0/F_{2j} remains r. Also, we know that F_j/F_{2j} is abelian; hence, from now on we will consider $F_{2j} = 1$ and write A for the abelian group F_j. Now observe that $L \cap A$ is normal in $G_0 = HA = LA$: if $u \in L \cap A$, $l \in L$ and $a \in A$ then $a^{-1}ua = u$, since A is abelian, and $l^{-1}ul$ is an element of L that belongs to A because A is normal in G_0. Moreover, we observe that $\mathrm{d}(H/L \cap A) = \mathrm{d}(H)$, i.e., taking this quotient does not affect the minimal number of generators of H. Indeed, since by construction

$$\mathrm{d}(\frac{L}{L \cap A}) = \mathrm{d}(\frac{LA}{A}) = \mathrm{d}(\frac{HA}{A}) = \mathrm{d}(\frac{H}{H \cap A}) = m = \mathrm{d}(L),$$

$L \cap A$ is contained in the Frattini subgroup of L, hence in the Frattini subgroup of H. It follows that from now on we can consider the quotient $G_0/(L \cap A)$, thus assuming that the intersection $L \cap A$ is trivial.

With these simplifications, G_0 is a finite p-group and splits as a semidirect product $G_0 = L \ltimes A$.

We note that the minimal number of generators of the $\mathbb{Z}L$-module $H \cap A = \langle w_{m+1}, \ldots, w_r \rangle^L$ is $\mathrm{d}_L(H \cap A) = \ell$, as $H \cap A$ can be generated by $w_{m+1}, \ldots, w_r$ as an L-module. Indeed, an element v of $H \cap A$ can be written as a product

$$y_{i_1}^{k_{i_1}} w_{j_1}^{l_{j_1}} \cdots y_{i_s}^{k_{i_s}} w_{j_s}^{l_{j_s}}$$

for some integer s, some indices $i_1, \ldots, i_s$ in $\{1, \ldots, m\}$ and $j_1, \ldots, j_s$ in $\{1, \ldots, \ell\}$ and some exponents $k_{i_1}, \ldots, k_{i_s}, l_{j_1}, \ldots, l_{j_s}$. Rearranging terms if necessary, we can rewrite such product as

$$\prod_t y_{\iota_t}^{\kappa_{\iota_t}} \cdot \prod_n (w_{\gamma_n}^{\lambda_{\gamma_n}})^{y_{\mu_n}^{\kappa_{\mu_n}}}$$

for some indices ι_t, μ_n in $\{1, \ldots, m\}$, γ_n in $\{1, \ldots, \ell\}$ and exponents $\kappa_{\iota t}, \lambda_{\gamma_n}, \kappa_{\mu_n}$. Now the first factor of this product belongs to L and the second one to $H \cap A$.

Since this product represents an element in $H \cap A$, it follows that also the factor $\prod_t y_{\iota t}^{\kappa_{\iota t}}$ must belong to A. But $L \cap A = 1$ by assumption, hence $\prod_t y_{\iota t}^{\kappa_{\iota t}}$ is trivial and $v = \prod_n (w_{\gamma_n}^{\lambda_{j_n}})^{y_{\iota_n}^{\kappa_{\iota_n}}}$, which proves that $H \cap A$ can be generated by $w_{m+1}, \dots, w_r$ as an L-module. It is now clear that ℓ is the minimal number of generators of such module, because otherwise one would get $\mathrm{d}(H) < r$.
It follows that $\mathrm{d}(H) = r = \mathrm{d}(L) + \mathrm{d}_L(H \cap A) = m + \ell$.
In a similar way, $\mathrm{d}(\widetilde{H}) = \mathrm{d}(L) + \mathrm{d}_L(\widetilde{H} \cap A)$, where $\widetilde{H} \cap A = \langle z_1, \dots, z_\ell \rangle^L$ is the relevant $\mathbb{Z}L$-module, whence $\mathrm{d}_L(\widetilde{H} \cap A) = \mathrm{d}(\widetilde{H}) - m \leq r - m = \ell$. Finally, we notice that, since A is abelian, the p-power map $x \mapsto x^p$ induces an epimorphism of $\mathbb{Z}L$-modules $\widetilde{H} \cap A \to H \cap A$ and shifts the elements $z_1, \dots, z_\ell$ of $F_j \setminus F_{j+k}$ each one term down in the given filtration $A = F_j \supseteq F_{j+1} \supseteq \dots \supseteq F_{j+k+1}$. Therefore, $\mathrm{d}_L(\widetilde{H} \cap A) \geq \mathrm{d}_L(H \cap A) = \ell$ and we can conclude that $\mathrm{d}_L(\widetilde{H} \cap A) = \mathrm{d}(\widetilde{H}) - m = \ell$. Therefore the minimal number of generators of $\widetilde{H}$ modulo $(L \cap F_j)F_{2j}$ is at least r and hence also $\mathrm{d}(\widetilde{H}) \geq r$. But since r is the rank of G, the minimal number of generators of $\widetilde{H}$ is exactly r, which proves the claim.

□

Example 2.3.3.

1. Let G be an abelian pro-p group, i.e.,

$$G \cong \mathbb{Z}_p^k \times C_{p^{l_1}} \times \cdots \times C_{p^{l_s}}$$

for some natural numbers s, k and some positive integers $l_1 \dots, l_s$. We use additive notation for the group operation. Since G is abelian it is in particular powerful, hence we can take F to be G in the previous theorem. By Proposition 1.1.23 the rank of G is given by the number of factors of the direct product, i.e., $\mathrm{rk}(G) = k + s$. If we want to use the previous theorem,

$$P_{2(k+s)+1}(G) = p^{2(k+s)+1}\mathbb{Z}_p^k \times p^{2(k+s)+1}C_{p^{l_1}} \times \cdots \times p^{2(k+s)+1}C_{p^{l_s}}$$

and taking the quotient $G/P_{2(k+s)+1}(G)$ we get

$$C_{p^{2(k+s)+1}}^k \times \frac{C_{p^{l_1}}}{p^{2(k+s)+1}C_{p^{l_1}}} \times \cdots \times \frac{C_{p^{l_s}}}{p^{2(k+s)+1}C_{p^{l_s}}}.$$

Since, for every $i \in \{1, \dots, s\}$, the group $p^{2(k+s)+1}C_{p^{l_i}}$ is either trivial or a finite p-group of order $p^{l_i - 2(k+s)-1}$, it follows that the quotient $G/P_{2(k+s)+1}(G)$ is a finite p-group of rank $k + s$.

Note that we could have taken the quotient of G by $P_2(G)$ obtaining the same result.

2. Let n be a positive integer and consider the metabelian pro-p group

$$G = C \ltimes A, \qquad \text{where } C = \langle c \rangle \cong \mathbb{Z}_p, \quad A = \langle a_1, \dots, a_n \rangle \cong \mathbb{Z}_p^n$$

and the action of C on A is given by

$$a_i^c = a_i a_{i+1} \quad \text{for } 1 \leq i < n, \qquad \text{and} \quad a_n^c = a_n.$$

Then $G = \langle c, a_1 \rangle$ is 2-generated, nilpotent of class n and has rank $\mathrm{rk}(G) = n+1$. For instance,

$$H = \langle c, a_1^{p^{n-1}}, a_2^{p^{n-2}}, \ldots, a_{n-1}^{p}, a_n \rangle \leq_{\mathrm{o}} G$$

requires $n+1$ generators.

Suppose that $p > n \geq 2$. Then $F = \langle c^p \rangle \ltimes A \trianglelefteq_{\mathrm{o}} G$ is powerful, and $\Phi^j(F) = \langle c^{p^j} \rangle \ltimes A^{p^{j-1}}$ for $j \geq 1$. Thus any subgroup $\widetilde{H} \leq_{\mathrm{o}} G$ with $\widetilde{H}F = HF = \langle c \rangle F$ and $\mathrm{d}(\widetilde{H}) = \mathrm{d}(\widetilde{H}\Phi^n(F)/\Phi^n(F))$ requires less than $\mathrm{d}(H) = n+1$ generators, but nevertheless $\mathrm{rk}(G) = \mathrm{rk}(G/\Phi(F))$. For example, the group

$$K = \langle c^p, a_1, \ldots, a_n \rangle,$$

which is unrelated to H, requires $n+1$ generators, even modulo $\Phi(F) = P_2(F)$.

Note that the previous example shows that one would have to follow a different approach to eliminate the dependency on R from the number of iterations of the Frattini subgroup of F. (Recall that, if F is a finitely generated powerful pro-p group, then its lower p-series coincides with its iterated Frattini series, with $\Phi^j(F) = P_{j+1}(F)$ for all natural numbers j; see Proposition 1.3.8).

Remark 2.3.4. Even if we presented the previous theorem in the pro-p case for clarity of exposition and because this is the result that we will need in this section, we want to mention that the same result holds more generally for profinite groups of finite rank that are virtually pro-p, more or less with the same proof. As later on, in Section 2.6, we will need this more general result, we state it here indicating the changes needed in the proof. Recall that, if G is a profinite group and p is a prime, we denote with $\mathrm{rk}_p(G)$ the rank of a Sylow pro-p subgroup of G.

Theorem 2.3.5. *Let R be a positive integer and let G be a profinite group that is virtually pro-p. Assume that $F \trianglelefteq_{\mathrm{o}} G$ is a powerful pro-p open normal subgroup of G. If $\mathrm{rk}_p(G) \leq R$, then*

$$\mathrm{rk}_p(G) = \mathrm{rk}_p\big(G/P_{2R+1}(F)\big).$$

Proof. The proof is almost the same as the proof of Theorem 2.3.1. Here are the few modifications needed. First of all, when considering the rank, we are always talking about the p-rank rk_p. We therefore assume by contradiction that $\mathrm{rk}_p(G) > \mathrm{rk}_p(G/F_{2R+1})$, with $F_{2R+1} = P_{2R+1}(F)$. When choosing the open subgroup H, we take it to be a pro-p subgroup of G of *minimal index* among the open pro-p subgroups of G with $\mathrm{d}(H) = \mathrm{rk}_p(G)$. Instead, we do not make any assumption of minimality on the index $j = j(H)$ in the filtration (2.3). Finally, when dealing with $\tilde{H}$ we need to observe that this group is pro-p, as it is a closed subgroup of the pro-p group HF_j. The result is then obtained by observing that $\mathrm{d}(\tilde{H}) = \mathrm{rk}_p(G)$ (as before) and that $|G : \tilde{H}| < |G : H|$, that contradicts the minimality of the index of H. The last inequality is obtained by extending the p-power map to a surjective homomorphism from $\tilde{H}$ to H. □

Now let $\pi = \{p_1, \ldots, p_k\}$ be a finite set of primes and $G = G_1 \times \cdots \times G_k$ a $\mathcal{C}_\pi$ group. Then, since the primes in π are all distinct, the rank of G is related to the ranks of the factors in the direct product by

$$\mathrm{rk}(G) = \max_{i=1,\ldots,k} \mathrm{rk}(G_i). \tag{2.6}$$

This formula is well known but we provide a proof for completeness.

Proof of (2.6). To prove the formula we show that, for any $\mathcal{C}_\pi$ group $H = H_1 \times \cdots \times H_k$, the minimal number of generators of H is given by $\mathrm{d}(H) = m := \max_{i=1,\dots,k} \mathrm{d}(H_i)$. We start with the case where H is a finite $\mathcal{C}_\pi$ group. Then clearly $\mathrm{d}(H) \geq m$ as the projection $H \to H_i$ is surjective for every i. Conversely, for every $i \in \{1,\dots,k\}$ let $h_{1,i},\dots,h_{m,i}$ be generators of H_i and consider the subgroup T of H generated by all tuples $(h_{j,1},\dots,h_{j,k})$ with $j \in \{1,\dots,m\}$. Each projection homomorphism $T \to H_i$ is surjective because its image contains the generators $h_{1,i},\dots,h_{m,i}$ of H_i. It follows that, for each $i \in \{1,\dots,k\}$, the order of H_i divides the order of T. Since the orders of the groups H_i are pairwise coprime we get that also their product divides the order of T. Therefore we conclude that

$$|H| = |H_1| \cdots |H_k| \leq |T| \leq |H|,$$

hence $T = H$ and H is generated by m elements, i.e., $\mathrm{d}(H) \leq m$.

Let now H be any $\mathcal{C}_\pi$ group, not necessarily finite, and let again $m := \max_{i=1,\dots,k} \mathrm{d}(H_i)$. As before, clearly $\mathrm{d}(H) \geq m$. Conversely, by [DDMS], Proposition 1.5,

$$\begin{aligned} \mathrm{d}(H) &= \sup\{\mathrm{d}(H/N) | N \trianglelefteq_{\mathrm{o}} H\} \\ &= \sup\{\max\{\mathrm{d}(H_1/N \cap H_1),\dots,\mathrm{d}(H_k/N \cap H_k)\} | N \trianglelefteq_{\mathrm{o}} H\} \end{aligned}$$

thanks to the finite case. Therefore, $\mathrm{d}(H) = \mathrm{d}(H_i/N \cap H_i)$ for some $N \trianglelefteq_{\mathrm{o}} H$ and some $i \in \{1,\dots,k\}$ and $\mathrm{d}(H_i/N \cap H_i) \leq \mathrm{d}(H_i) \leq m$.

We now look at the rank. Let $G = G_1 \times \cdots \times G_k$ be a $\mathcal{C}_\pi$ group. Then, by definition of rank, $\max_{i=1,\dots,k} \mathrm{rk}(G_i) \leq \mathrm{rk}(G)$. Conversely,

$$\begin{aligned} \mathrm{rk}(G) &= \sup\{\mathrm{d}(H) | H <_{\mathrm{o}} G\} \\ &= \sup \max\{\mathrm{d}(H_i) | H = H_1 \times \cdots \times H_k <_{\mathrm{o}} G\} \\ &\leq \max \mathrm{rk}(G_i). \end{aligned}$$

□

Note that in the previous proof we also showed that, if $G = G_1 \times \ldots \times G_k$ is a $\mathcal{C}_\pi$ group, then

$$\mathrm{d}(G) = \max_{i=1,\dots,k} \mathrm{d}(G_i).$$

Finally, note that also in the case of a semi-powerful group F we have

$$\mathrm{d}(F) = \max_{i=1,\dots,k} \mathrm{d}(F_i) = \max_{i=1,\dots,k} \mathrm{rk}(F_i) = \mathrm{rk}(F).$$

Recall that the direct factors of a $\mathcal{C}_\pi$ group $G = G_1 \times \cdots \times G_k$ are Sylow subgroups of G. If $\pi = \{p_1,\dots,p_k\}$, by rearranging the factors of G if necessary, we can assume that G_i is the Sylow pro-p_i subgroup of G for each $i \in \{1,\dots,k\}$. Given a prime p, from now on we will call p-rank the common rank of all Sylow pro-p subgroups of G and we will denote it by $\mathrm{rk}_p(G)$.

From (2.6) it follows that a $\mathcal{C}_\pi$ group G has finite rank if and only if each direct factor of G has finite rank and in this case we have the following:

Corollary 2.3.6. *Let $\pi := \{p_1, \dots, p_k\}$ be a finite set of primes. For each positive integer r and each tuple $\mathbf{r} = (r_i)_{i\in\{1,\dots,k\}}$ of natural numbers in $\{0, 1, \dots, r\}$ with $\max r_i = r$ there is a sentence $\sigma_{\pi,r,\mathbf{r}}$ in the language of groups $\mathcal{L}_{gp}$ such that, for every $\mathcal{C}_\pi$ group G, the following are equivalent:*

1. *$\mathrm{rk}(G) = r$ and $\mathrm{rk}_{p_i}(G) = r_i$ for every $i \in \{1, \dots, k\}$,*
2. *G is a model of $\sigma_{\pi,r,\mathbf{r}}$.*

We remark that the case of a p-adic analytic pro-p group can be recovered from the pronilpotent case by considering $\pi = \{p\}$ and G consisting of a single pro-p factor.

Proof of Corollary 2.3.6. Recall that $\pi := \{p_1, \dots, p_k\}$ is a finite set of primes and let $G = G_1 \times \cdots \times G_k$ be a $\mathcal{C}_\pi$ group of rank r. Set $m := m(r) = \lceil \log_2(r) + \varepsilon_\pi \rceil$, with

$$\varepsilon_\pi := \begin{cases} 0, & \text{if } 2 \notin \pi \\ 1, & \text{if } 2 \in \pi \end{cases}.$$

For the considerations made in Section 2.2.3, the iterated Frattini group $\Phi^m(G)$ is a semi-powerful subgroup of G of rank bounded by r, definable via the formula ϕ_m^G. Moreover, the quotient $G/\Phi^m(G)$ is a finite π-group with order bounded by $\prod_{i=1,\dots k} p_i^{mr}$ and rank bounded by r. Let $\lambda_1, \dots, \lambda_N$ be the finitely many formulas that can describe such groups. Then $G/\Phi^m(G) \models \lambda := \lambda_1 \vee \dots \vee \lambda_N$.
It follows that a $\mathcal{C}_\pi$ group G of rank r satisfies the sentence

$$\mathrm{res}(\phi_m^G, \mathrm{pow}) \wedge \mathrm{res}(\phi_m^G, \tilde{\beta}_r) \wedge \mathrm{lift}(\phi_m^G, \lambda).$$

Conversely, if a $\mathcal{C}_\pi$ group $G = G_1 \times \cdots \times G_k$ satisfies the previous sentence, then its rank is bounded by $2r$:

$$\mathrm{rk}(G) \leq \mathrm{rk}(\Phi^m(G)) + \mathrm{rk}(G/\Phi^m(G)) \leq 2r$$

(see Proposition 1.1.14 for the first inequality).
We know that G has rank r if and only if the maximum of the ranks of the factors G_i is r. Let $R := 2r$, $F := P_{2R+1}(\Phi^m(G))$ and $F_i := P_{2R+1}(\Phi^m(G_i))$ for every $i = 1, \dots, k$. By Theorem 2.3.1, the rank of each factor G_i is equal to the rank of G_i/F_i and, in order for G to have rank r, it is enough to require that one of the quotients G_i/F_i has rank r and the others have rank bounded by r. This is what we are going to express with a first-order sentence.
Given $i \in \{1, \dots, k\}$, consider the quotient G_i/F_i. This finite group has order bounded by $p_i^{2r(2R+1+m)}$ and it is isomorphic to $G/(F \cdot G^{p_i^{2r(2R+1+m)}})$. Recall that each r_i is a natural number in $\{0, \dots, r\}$ and that $\max r_i = r$ by assumption. Let $\nu_1^{p_i,r_i}, \dots, \nu_{M_{p_i,r_i}}^{p_i,r_i}$ be the finitely many formulas describing finite groups of order bounded by $p_i^{2r(2R+1+m)}$ and with rank r_i and set $\nu_{p_i,r_i} := \nu_1^{p_i,r_i} \vee \dots \vee \nu_{M_{p_i,r_i}}^{p_i,r_i}$.
Let ξ_i be the formula describing $F \cdot G^{p_i^{2r(2R+1+m)}}$ (such a formula exists because the word $x^{p_i^{2r(2R+1+m)}}$ has finite width; see [NST], Proposition 5.12.) Then the $\mathcal{C}_\pi$ group G has rank r and p_i-rank r_i for each $i \in \{1, \dots, k\}$ if and only if it satisfies the sentence

$$\sigma_{\pi,r,\mathbf{r}} := \mathrm{res}(\phi_m^G, \mathrm{pow}) \wedge \mathrm{res}(\phi_m^G, \tilde{\beta}_r) \wedge \mathrm{lift}(\phi_m^G, \lambda) \wedge \bigwedge_{i=1}^{k} \mathrm{lift}(\xi_i, \nu_{p_i,r_i}).$$

□

Remark 2.3.7. In the case where π consists of a single prime p, the last term of $\sigma_{\pi,r,\mathbf{r}}$ can be simplified to $\mathrm{lift}(\pi_{2R+1}^{\Phi^m(G)}, \nu)$, where $\pi_{2R+1}^{\Phi^m(G)}$ is the formula defining $P_{2R+1}(\Phi^m(G))$ and ν is the formula describing finite groups of order bounded by $p^{r(2R+1+m)}$ and with rank r.

Remark 2.3.8. In Section 2.6 we will prove a more general result than Theorem 2.3.5, that holds true for all virtually pronilpotent profinite groups (see Theorem 2.6.1). By using this result we could simplify the previous sentence by simply imposing in the last step that $\mathrm{rk}(G/F) = r$ and that, for each $p_i \in \pi$, the p_i-rank of G/F is r_i, where $F := P_{2R+1}(\Phi^m(G))$. However, since Theorem 2.6.1 will depend on the classification of finite simple groups, it is worth recording the previous proof that is independent of the classification.

We conclude this section by showing that it is necessary that the set of primes π under consideration is finite. The situation would not change even if the language $\mathcal{L}_{\mathrm{gp}}$ was to be enlarged by an extra function to be interpreted as the p-power map $x \mapsto x^p$ in pro-p groups. We sketch a proof for completeness; it relies on a standard ultraproduct construction and a well-known quantifier elimination result in model theory. More precisely, we will use the fact that, given a field K, the theory of infinite K-vector spaces is complete, i.e., any two models of this theory are elementarily equivalent (see [TZ], Theorem 3.3.3).

Proposition 2.3.9. *Let $\tilde{\pi}$ be an infinite set of primes and let r be a positive integer. Then there is no $\mathcal{L}_{\mathrm{gp}}$-sentence $\vartheta_{\tilde{\pi},r}$ such that, for every $p \in \tilde{\pi}$ and every finite elementary abelian p-group G, the following are equivalent:*

1. $\mathrm{rk}(G) = r$.
2. *$\vartheta_{\tilde{\pi},r}$ holds in G, i.e., $G \models \vartheta_{\tilde{\pi},r}$.*

Proof. For a contradiction, assume that the $\mathcal{L}_{\mathrm{gp}}$-sentence $\vartheta = \vartheta_{\tilde{\pi},r}$ has the desired property. Then $C_p^r \models \vartheta$ and $C_p^{r+1} \models \neg\vartheta$ for all $p \in \tilde{\pi}$. We regard C_p^r and C_p^{r+1} as the additive groups of the vector spaces $\mathbb{F}_p^r$ and $\mathbb{F}_p^{r+1}$ over the prime field $\mathbb{F}_p$.

Let $\mathcal{U}$ be a non-principal ultrafilter on the infinite index set $\tilde{\pi}$. By Łoś's theorem (Theorem 2.2.10),

$$\mathcal{K} = \left(\prod_{p\in\tilde{\pi}} \mathbb{F}_p\right)/\mathcal{U}$$

is a field of characteristic 0 (see [E], Theorem 5.3), and

$$\mathcal{V} = \left(\prod_{p\in\tilde{\pi}} \mathbb{F}_p^r\right)/\mathcal{U} \qquad \text{and} \qquad \mathcal{W} = \left(\prod_{p\in\tilde{\pi}} \mathbb{F}_p^{r+1}\right)/\mathcal{U}$$

are non-zero $\mathcal{K}$-vector spaces. Let $\mathcal{L}_{\mathcal{K}\text{-vs}}$ denote the language of $\mathcal{K}$-vector spaces, which comprises the language of groups (for the additive group of vectors) and,

for each scalar $c \in \mathcal{K}$, a 1-ary operation f_c (to denote scalar multiplication by c). Clearly, the $\mathcal{L}_{\text{gp}}$-sentence ϑ gives rise to an $\mathcal{L}_{\mathcal{K}\text{-vs}}$-sentence θ, not involving scalar multiplication at all, such that, again by Łoś's theorem,

$$\mathcal{V} \models \theta \qquad \text{and} \qquad \mathcal{W} \models \neg\theta,$$

in contradiction to the known fact that the infinite $\mathcal{K}$-vector spaces $\mathcal{V}$ and $\mathcal{W}$ have the same theory. □

2.4 Finite axiomatizability of the dimension of $\mathcal{C}_\pi$ groups

In this section we prove that the dimension of a pro-p group of fixed finite rank r is axiomatizable by a single first-order sentence in $\mathcal{L}_{\text{gp}}$. Also in this case we will prove the result in the slightly more general case of pronilpotent pro-π groups, i.e., $\mathcal{C}_\pi$ groups. Given a $\mathcal{C}_\pi$ group with finite rank $G = G_1 \times \cdots \times G_k$, let $d_i := \dim(G_i)$ for all $i \in \{1, \ldots, k\}$; then we call the k-tuple $\mathbf{d} := (d_1, \ldots, d_k)$ the *dimension* of G. Recall that the factors G_i of G are Sylow subgroups of G. As in the previous section, if $\pi = \{p_1, \ldots, p_k\}$, we assume that G_i is a Sylow pro-p_i subgroup of G for each $i \in \{1, \ldots, k\}$.

We deal first with the case of abelian $\mathcal{C}_\pi$ groups of finite rank and then we make use of it to deduce the result in the general case.

2.4.1 The abelian case

Let $G = G_1 \times \cdots \times G_k$ be an abelian $\mathcal{C}_\pi$ group of rank $r = \max_{i=1,\ldots,k} r_i$, where r_i is the rank of G_i for all $i \in \{1, \ldots, k\}$.
Given a k-tuple $\mathbf{d} := (d_1, \ldots, d_k)$ of natural numbers, we want to write a sentence $\delta^{\text{ab}}_{\pi,r,\mathbf{d}}$ such that $G \models \delta^{\text{ab}}_{\pi,r,\mathbf{d}}$ if and only if G has dimension $\mathbf{d}$.
By the structure theorem of finitely generated abelian pro-p groups, for every $i \in \{1, \ldots, k\}$,

$$G_i \cong \mathbb{Z}_{p_i}^{d_i} \times C_{p_i^{l_{i,1}}} \times \cdots \times C_{p_i^{l_{i,s_i}}}$$

for some non-negative integers d_i, s_i and some positive integers $l_{i,1}, \ldots, l_{i,s_i}$, where $r_i = d_i + s_i$. Therefore

$$G \cong \prod_{i=1}^{k} \mathbb{Z}_{p_i}^{d_i} \times C_{p_i^{l_{i,1}}} \times \cdots \times C_{p_i^{l_{i,s_i}}}.$$

Hence we see that an abelian pro-p_i group G_i of rank r_i has dimension d_i if and only if G_i has a finite subgroup isomorphic to the direct product of $r_i - d_i = s_i$ copies of C_{p_i} and G_i does not have a subgroup isomorphic to the direct product of $r_i - d_i + 1$ copies of C_{p_i}.
Let $\gamma_{p_i,s_i} = \gamma_{p_i,s_i}(v_1, \ldots, v_{p_i^{s_i}})$ be a formula with free variables $v_1, \ldots, v_{p_i^{s_i}}$ describing the direct product of s_i copies of the cyclic group C_{p_i}; such a formula can be written by using the multiplication table of said group.
Hence, we can define the sentence $\overline{\delta}^{\text{ab}}_{p_i,r_i,d_i}$ as follows:

$$\exists\, x_1, \ldots, x_{p_i^{s_i}} : \gamma_{p_i,s_i}(x_1, \ldots, x_{p_i^{s_i}}) \ \wedge\ \neg\exists\, y_1, \ldots, y_{p_i^{s_i+1}} : \gamma_{p_i,s_i+1}(y_1, \ldots, y_{p_i^{s_i+1}}).$$

Moreover, we can detect the ranks r_i of the direct factors of G thanks to the fact that

$$G/G^{p_1\cdots p_k} \cong C_{p_1}^{r_1} \times \cdots \times C_{p_k}^{r_k}. \tag{2.7}$$

According to (2.7), in order to specify the ranks r_i it is enough to write a sentence that states that the quotient $G/G^{p_1\cdots p_k}$ contains a direct product isomorphic to $C_{p_i}^{r_i}$ for every $i \in \{1, \ldots, k\}$.
Let $\chi_\pi(z)$ be the formula $\exists x : z = x^{p_1\cdots p_k}$ that defines $G^{p_1\cdots p_k}$ and consider the sentence $\tau_{r_1,\ldots,r_k}$ given by

$$\bigwedge_{i=1}^{k} \Big(\exists\, x_1, \ldots, x_{p_i^{r_i}} : \gamma_{p_i,r_i}(x_1, \ldots, x_{p_i^{r_i}}) \wedge \neg\exists\, y_1, \ldots, y_{p_i^{r_i+1}} : \gamma_{p_i,r_i+1}(y_1, \ldots, y_{p_i^{r_i+1}})\Big).$$

Then we can express the isomorphism (2.7) by the sentence

$$\overline{\tau}_{r_1,\ldots,r_k} := \mathrm{lift}(\chi_\pi, \tau_{r_1,\ldots,r_k}).$$

By using $\overline{\delta}^{\mathrm{ab}}_{p_i,r_i,d_i}$ and $\overline{\tau}_{r_1,\ldots,r_k}$ we get:

Proposition 2.4.1. *For every positive integer r and every k-tuple of natural numbers $\mathbf{d} := (d_1, \ldots, d_k)$, with $d_i \leq r$ for each $i \in \{1, \ldots, k\}$, there is a sentence $\delta^{\mathrm{ab}}_{\pi,r,\mathbf{d}}$ in the language of groups $\mathcal{L}_{gp}$ such that for every abelian $\mathcal{C}_\pi$ group G the following are equivalent:*

1. *G has rank r and dimension $\mathbf{d}$,*
2. *G is a model of $\delta^{\mathrm{ab}}_{\pi,r,\mathbf{d}}$.*

Proof. Let $\delta^{\mathrm{ab}}_{\pi,r,\mathbf{d}}$ be the sentence

$$\bigvee_{\substack{r_1,\ldots,r_k \\ \max_i r_i = r}} \overline{\tau}_{r_1,\ldots,r_k} \wedge \bigwedge_{j=1}^{k} \overline{\delta}^{\mathrm{ab}}_{p_j,r_j,d_j}.$$

Then, according to the previous discussion, an abelian $\mathcal{C}_\pi$ group $G = G_1 \times \ldots \times G_k$ satisfies $\delta^{\mathrm{ab}}_{\pi,r,\mathbf{d}}$ if and only if, for every $i \in \{1, \ldots, k\}$, $\mathrm{rk}\, G_i = r_i$ (this is assured by $\overline{\tau}_{r_1,\ldots,r_k}$) and, for every $i \in \{1, \ldots, k\}$, the dimension of G_i is d_i (this follows from $\overline{\delta}^{\mathrm{ab}}_{p_j,r_j,d_j}$).
Note that when the group has a single factor, i.e., when we are dealing with an abelian pro-p group G of rank r, the sentence

$$\mathrm{lift}(\chi_p, \tau_r) \wedge \overline{\delta}^{\mathrm{ab}}_{p,r,d}$$

is enough to ensure that G has dimension d.
Note also that we might use the sentence $\sigma_{\pi,r,\mathbf{r}}$ from the previous section to determine the ranks r_i of the factors. □

Remark 2.4.2. Letting $\alpha := \forall x, y : x^{-1}y^{-1}xy = 1$, then $G \models \alpha$ if and only if G is abelian. Thus, by setting $\tilde{\delta}^{\mathrm{ab}}_{\pi,r,\mathbf{d}} := \alpha \wedge \delta^{\mathrm{ab}}_{\pi,r,\mathbf{d}}$ we can reformulate the previous proposition as:

Proposition 2.4.3. *For every positive integer r and every k-tuple of natural numbers $\mathbf{d} := (d_1, \ldots, d_k)$, with $d_i \leq r$ for each $i \in \{1, \ldots, k\}$, there is a sentence $\tilde{\delta}^{\mathrm{ab}}_{\pi,r,\mathbf{d}}$ in the language of groups $\mathcal{L}_{gp}$ such that, for every $\mathcal{C}_\pi$ group G, the following are equivalent:*

1. *G is abelian and has rank r and dimension $\mathbf{d}$,*
2. *G is a model of $\tilde{\delta}^{\mathrm{ab}}_{\pi,r,\mathbf{d}}$.*

2.4.2 The general case

Let $G = G_1 \times \ldots \times G_k$ be a C_π group of finite rank and, for every $i \in \{1, \ldots, k\}$, let H_i be an open normal uniform subgroup of the p_i-adic analytic pro-p_i group G_i. Set $H := H_1 \times \cdots \times H_k$.
Recall that, if we denote by $\mathrm{L}(H_i)$ the Lie lattice corresponding to H_i, the Lie algebra of G_i is given by

$$\mathcal{L}(G_i) := \mathbb{Q}_{p_i} \otimes_{\mathbb{Z}_{p_i}} \mathrm{L}(H_i)$$

(see Section 1.3). From these Lie algebras we obtain an abelian group given by

$$\mathcal{L}(G) := \bigoplus_{i=1}^{k} \mathbb{Q}_{p_i} \otimes_{\mathbb{Z}_{p_i}} \mathrm{L}(H_i) = \bigoplus_{i=1}^{k} \mathcal{L}(G_i).$$

Let $g := (g_1, \ldots, g_k) \in G$. The inner automorphism ϕ_g sending an element $x := (x_1, \ldots, x_k)$ in G to $x^g := g^{-1}xg = (g_1^{-1}x_1g_1, \ldots, g_k^{-1}x_kg_k)$ induces an automorphism $\phi_g^* : \mathcal{L}(G) \to \mathcal{L}(G)$ defined as

$$\phi_g^* := \bigoplus_{i=1}^{k} 1 \otimes \phi_{g_i|_{\mathrm{L}(H_i)}}$$

(see [DDMS], Section 9.5).

Denote as usual by Ad the adjoint representation of G:

$$\mathrm{Ad} : G \to \mathrm{Aut}(\mathcal{L}(G)), \qquad g \mapsto \phi_g^*.$$

Lemma 2.4.4. *Let K be the kernel of* Ad.
Then $K = C_G(H) = C_{G_1}(H_1) \times \ldots \times C_{G_k}(H_k)$.

Proof. Let g be an element of K. Then $\phi_g^* = \mathrm{id}_{\mathcal{L}(G)}$. In particular, for every $i \in \{1, \ldots, k\}$, for every λ_i in $\mathbb{Q}_{p_i}$ and every h_i in H_i we have $\lambda_i \otimes g_i^{-1}h_ig_i = \lambda_i \otimes h_i$, hence $g_i \in C_{G_i}(H_i)$.

Conversely, if g is in $C_{G_1}(H_1) \times \ldots \times C_{G_k}(H_k)$, then, given $i \in \{1, \ldots, k\}$, for every $\lambda_1, \ldots, \lambda_s$ in $\mathbb{Q}_{p_i}$ and every $h_1, \ldots, h_s$ in H_i one has

$$\begin{aligned}\phi_{g_i}^*(\lambda_1 \otimes h_1 + \ldots + \lambda_s \otimes h_s) &= (\lambda_1 \otimes g_i^{-1}h_1g_i) + \ldots + (\lambda_k \otimes g_i^{-1}h_kg_i) \\ &= (\lambda_1 \otimes h_1) + \ldots + (\lambda_k \otimes h_k),\end{aligned}$$

i.e., $\phi_{g_i}^*$ is the identity. Since this holds for every $i \in \{1, \ldots, k\}$, ϕ_g^* is the identity. □

Assume now that G has rank r and dimension $\mathbf{d}$, that K has dimension $\mathbf{d}_1$ and G/K has dimension $\mathbf{d}_2$, with $\mathbf{d}_1 + \mathbf{d}_2 = \mathbf{d}$.
We will show that G satisfies a first-order sentence in the language of groups that expresses the fact that G has dimension $\mathbf{d}$.
In order to do so we will first consider K and G/K separately.
We need a (well known) lemma to begin with.

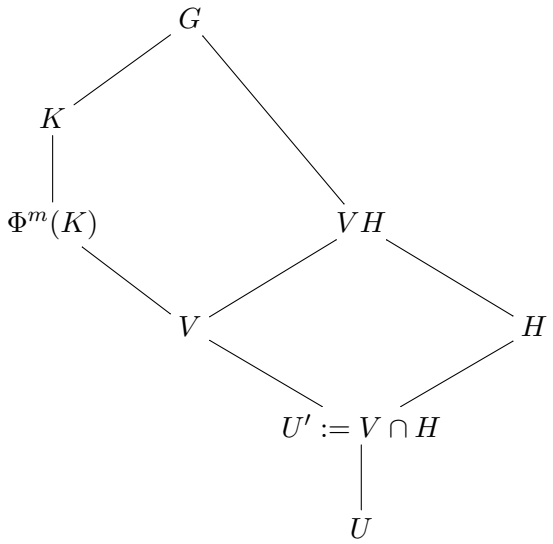
Lemma 2.4.5. *Let U be an abelian subgroup of G and let $C_G(U)$ be the centralizer of U in G. Then $C_G(C_G(U))$ is abelian and $U \subseteq C_G(C_G(U))$.*

Proof. It is clear that $U \subseteq C_G(C_G(U))$.
Moreover, since $U \subseteq C_G(U)$, then $C_G(C_G(U)) \subseteq C_G(U)$.
We claim that $C_G(C_G(U)) = Z(C_G(U))$.
Indeed, $Z(C_G(U)) = C_G(C_G(U)) \cap C_G(U) = C_G(C_G(U))$.
It follows that $C_G(C_G(U))$ is abelian. □

1. dim K

Since K is a closed subgroup of G and G has rank r, the rank of K is less than or equal to r.
It follows that, setting $m := m(r)$ as defined in Section 2.3, the iterated Frattini subgroup $\Phi^m(K)$ is semi-powerful.

We claim that $\Phi^m(K)$ has an open semi-uniform abelian subgroup U.
Indeed, since $\Phi^m(K)$ has finite rank, it has an open semi-uniform normal subgroup V. Let $U' := V \cap H$, where H is the open normal semi-uniform subgroup of G that we chose above. Now from $V/U' \cong VH/H$ it follows that U' has finite index in V, hence in $\Phi^m(K)$. Moreover, U' is torsion-free, being contained in the torsion-free group V.
Let U be a semi-powerful open subgroup of U'; then U is a semi-uniform open subgroup of $\Phi^m(K)$ by construction.



Finally, since $U \subseteq H$, $C_G(H) \subseteq C_G(U)$, i.e., $K \subseteq C_G(U)$. But by definition U is contained in K and therefore U is abelian.

It follows by Lemma 2.4.5 that $C_K(C_K(U))$ is abelian and that $U \subseteq C_K(C_K(U))$. In particular, since U has finite index in K, also $C_K(C_K(U))$ has finite index in K and $\dim K = \dim C_K(C_K(U))$.

Now note that $K = C_G(H)$ is definable in G in the language of groups. Indeed, since G has rank r, there exist $h_1, \ldots, h_r$ in G with $H = \overline{\langle h_1, \ldots, h_r \rangle}$. Therefore, $K = C_G(H) = \{x \in G \mid [x, h_i] = 1 \text{ for } i = 1, \ldots, r\}$.

Moreover, $C_K(C_K(U))$ is definable in K (hence in G).
Indeed, consider $C_K(U)$. Since K has rank bounded by r, there exist elements $a_1, \ldots, a_r$ in K such that $C_K(U) = \overline{\langle a_1, \ldots, a_r \rangle}$.
Now consider $C_K(C_K(U)) = C_K(a_1) \cap \ldots \cap C_K(a_r)$ and let $\zeta(a, x)$ be the formula $ax = xa$. Then $C_K(C_K(U)) = \{x \in K \mid G \models \zeta(a_1, x) \wedge \ldots \wedge \zeta(a_r, x)\}$ is a definable abelian subgroup of G containing U.
Denote by $\tilde{\alpha} := \tilde{\alpha}(a_1, \ldots, a_r, x)$ the formula (with parameters) $\zeta(a_1, x) \wedge \ldots \wedge \zeta(a_r, x)$ that defines $C_K(C_K(U))$ in K and let $\overline{r}_1 \leq r$ be the rank of $C_K(C_K(U))$. From the abelian case, we know that $\dim(C_K(C_K(U))) = \mathbf{d}_1$ if and only if $C_K(C_K(U)) \models \delta^{\mathrm{ab}}_{\pi, \overline{r}_1, \mathbf{d}_1}$. Let $\mathbf{d}_1^{\max}$ be the maximal entry of the vector $\mathbf{d}_1$.
Since $\mathbf{d}_1^{\max} \leq \overline{r}_1 \leq r$, we have a finite number of possibilities for the value of the rank of $C_K(C_K(U))$. Write $\overline{\delta}_{\mathbf{d}_1}$ for the sentence given by the corresponding union of $r - \mathbf{d}_1^{\max} + 1$ sentences, one for each possible value of $\overline{r}_1$:

$$\overline{\delta}_{\mathbf{d}_1} := \delta^{\mathrm{ab}}_{\pi, \mathbf{d}_1^{\max}, \mathbf{d}_1} \vee \delta^{\mathrm{ab}}_{\pi, \mathbf{d}_1^{\max}+1, \mathbf{d}_1} \vee \ldots \vee \delta^{\mathrm{ab}}_{\pi, r, \mathbf{d}_1}$$

Then clearly $C_K(C_K(U)) \models \overline{\delta}_{\mathbf{d}_1}$.

Furthermore, we can express the fact that $C_K(C_K(U))$ is an abelian subgroup of maximal dimension in K, meaning that each direct factor $C_K(C_K(U))_i$ of $C_K(C_K(U))$ has maximal dimension in the direct factor K_i of K.
Indeed, suppose that there is an abelian subgroup $\overline{B} := B_1 \times \ldots \times B_k$ one of whose components B_i has dimension greater than $(\mathbf{d}_1)_i$, the i^{th} component of $\mathbf{d}_1$, and assume that $C_K(\overline{B})$ is generated by the elements $b_1, \ldots, b_r$. Then $\overline{B}$ is contained in $B := C_K(C_K(\overline{B}))$, that, by Lemma 2.4.5, is a definable abelian subgroup of K defined in K by the formula (with parameters) $\beta := \zeta(b_1, x) \wedge \ldots \wedge \zeta(b_r, x)$.
Then we can express the maximality of the dimension of $C_K(C_K(U))$ by means of the following sentence μ (holding true in K)

$$\neg\exists\, b_1, \ldots, b_r : (\mathrm{res}(\beta(b_1, \ldots, b_r), \bigvee_{\substack{\mathbf{m} \in \{0, \ldots, r\}^k \\ \mathbf{m} \neq (0, \ldots, 0)}} \overline{\delta}_{\mathbf{d}_1 + \mathbf{m}}) \wedge\ \mathrm{res}(\beta(b_1, \ldots, b_r), \alpha)),$$

where $\alpha := \forall x, y : xy = yx$ is the formula defining being abelian.

Therefore, $K \models \delta_{\mathbf{d}_1}$, where

$$\delta_{\mathbf{d}_1} := \exists\, a_1, \ldots, a_r : \mathrm{res}(\tilde{\alpha}(a_1, \ldots a_r), \overline{\delta}_{\mathbf{d}_1}) \wedge \mathrm{res}(\tilde{\alpha}(a_1, \ldots, a_r), \alpha) \wedge \mu.$$

In the previous sentence, $\mathrm{res}(\tilde{\alpha}(a_1, \ldots a_r), \overline{\delta}_{\mathbf{d}_1})$ states that $C_K(C_K(U))$ has dimension $\mathbf{d}_1$, $\mathrm{res}(\tilde{\alpha}(a_1, \ldots, a_r), \alpha)$ states that $C_K(C_K(U))$ is abelian and μ ensures that $\mathbf{d}_1$ is the maximal dimension among the dimensions of abelian subgroups of K.

Finally, let κ be the formula (with parameters) $\zeta(h_1, x) \wedge \ldots \wedge \zeta(h_r, x)$ that defines K.
Then $G \models \delta^s_{\mathbf{d}_1}$, where $\delta^s_{\mathbf{d}_1}$ is the formula with parameters

$$\delta^s_{\mathbf{d}_1} := \mathrm{res}(\kappa(h_1, \ldots h_r), \delta_{\mathbf{d}_1}) \wedge s_{\lhd}(\kappa(h_1, \ldots, h_r)),$$

where $s_{\lhd}(\kappa(h_1, \ldots, h_r))$ ensures that K is a normal subgroup of G.

2. dim G/K

Recall that $\mathbf{d} = \dim G$. Since K is the kernel of the adjoint representation of G, the quotient G/K embeds into $\mathrm{GL}_{d_1}(\mathbb{Q}_{p_1}) \times \ldots \times \mathrm{GL}_{d_k}(\mathbb{Q}_{p_k})$. Consider the semi-powerful group $\Phi^m(G/K)$. It is known ([DDMS], Theorem 4.20) that the torsion elements of $\Phi^m(G/K)$ form a finite $\mathcal{C}_\pi$ group $\mathrm{T}(\Phi^m(G/K))$ that is characteristic in $\Phi^m(G/K)$. Since this group is isomorphic to a finite subgroup of $\mathrm{GL}_{d_1}(\mathbb{Q}_{p_1}) \times \ldots \times \mathrm{GL}_{d_k}(\mathbb{Q}_{p_k})$, it follows that its order is bounded by $p_1^{f_1(d_1)} \cdots p_k^{f_k(d_k)}$, where $f_i : \mathbb{N} \to \mathbb{N}$ is the function given by

$$f_i(n) := \begin{cases} \lfloor \frac{n}{\varphi(p_i-1)} \rfloor + \mathrm{v}_{p_i}(n!) & \text{if } p_i \neq 2 \\ 2\lfloor \frac{n}{\varphi(2)} \rfloor + \mathrm{v}_{p_i}(n!) & \text{if } p_i = 2 \end{cases}. \tag{2.8}$$

Here $\mathrm{v}_{p_i}(n!)$ is the p_i-valuation of $n!$ and φ is the Euler function (see [Serre2], Theorem 5).[1]

It follows that $\mathrm{T}(\Phi^m(G/K)) = \{x \in \Phi^m(G/K) : x^{p_1^{f_1(d_1)} \cdots p_k^{f_k(d_k)}} = 1\}$ is a definable subgroup of $\Phi^m(G/K)$.

Let $\mathrm{bound}_{\mathbf{d}}$ be the formula

$$x^{p_1^{f_1(d_1)} \cdots p_k^{f_k(d_k)}} = 1$$

that defines $\mathrm{T}(\Phi^m(G/K))$.

Now the quotient $\Phi^m(G/K)/\mathrm{T}(\Phi^m(G/K))$ is a semi-uniform group ([DDMS], Theorem 4.20) whose dimension is the same as the dimension of $\Phi^m(G/K)$, i.e., $\mathbf{d}_2$. In order to define this dimension with a sentence we use the fact that the dimension of a uniform group coincides with its rank. Therefore it is enough to express the rank of each factor of the pronilpotent group $Q := \Phi^m(G/K)/\mathrm{T}(\Phi^m(G/K))$, which we can do similarly to what we did in Section 2.3. Namely, for every $i \in \{1, \ldots, k\}$, we can describe with a sentence the rank of the quotient $Q/P_{2r+1}(Q)Q^{{p_i}^{r(2r+1)}}$, that is equal to the rank of the direct factor Q_i by Theorem 2.3.1. To this aim let $\tilde{\xi}_i$ be the formula describing $P_{2r+1}(Q)Q^{{p_i}^{r(2r+1)}}$ and let $\tilde{\nu}^i_1, \ldots, \tilde{\nu}^i_{M_i}$ be the finitely many formulas describing finite groups of order bounded by ${p_i}^{r(2r+1)}$ and with rank $(\mathbf{d}_2)_i$ and set $\tilde{\nu}_{(\mathbf{d}_2)_i} := \nu^i_1 \vee \ldots \vee \nu^i_{M_i}$. Hence we can express the fact that Q has dimension $\mathbf{d}_2$ with the sentence

$$\mathfrak{q}_{\mathbf{d}_2} := \bigwedge_{i=1}^{k} \mathrm{lift}(\tilde{\xi}_i, \tilde{\nu}_{(\mathbf{d}_2)_i})$$

that is satisfied by Q.

(Alternatively, one might use directly the sentence $\sigma_{\pi,\max(\mathbf{d}_2)_i,\mathbf{d}_2}$ established in Section 2.3 to define the rank of a $\mathcal{C}_\pi$ group and of its factors).

[1] Alternatively, one can use the following elementary fact to find a bound for the order of the elements of the torsion subgroup $\mathrm{T}(\Phi^m(G/K))$. Let g be a torsion element in $\mathrm{GL}_d(\mathbb{Q}_p)$, i.e., there exists a non-negative integer n such that $g^{p^n} = 1$. The minimal polynomial of g over $\mathbb{Q}_p$ has degree bounded by d and divides the polynomial $X^{p^n} - 1$. It is therefore a cyclotomic polynomial, say the p^k-th cyclotomic polynomial, with degree $\varphi(p^k) = (p-1)p^{k-1} \leq d$. Let p^l be the least common multiple of the finite set $\{p^k \mid \varphi(p^k) \leq d\}$. Then every torsion element in $\mathrm{GL}_d(\mathbb{Q}_p)$ has order bounded by p^l.

We can therefore conclude that $\Phi^m(G/K)$ has dimension $\mathbf{d}_2$ if and only if it satisfies the sentence

$$\widetilde{\widetilde{\delta_{\mathbf{d}_2}}} := s_{\triangleleft}(\text{bound}_{\mathbf{d}}) \wedge \text{lift}(\text{bound}_{\mathbf{d}}, \mathfrak{q}_{\mathbf{d}_2}) \wedge \forall x : \left(\bigvee_{i=1}^{k} x^{p_i^{f(d_i)+1}} = 1 \to x^{p_i^{f(d_i)}} = 1 \right).$$

Note that the last part of the sentence guarantees that the torsion of $\Phi^m(G/K)$ is exactly given by $\mathrm{T}(\Phi^m(G/K)) = \{x \in \Phi^m(G/K) : x^{p_1^{f_1(d_1)} \cdots p_k^{f_k(d_k)}} = 1\}$.

Since $\Phi^m(G/K)$ is of finite index in G/K, they have the same dimension and therefore G/K has dimension $\mathbf{d}_2$ if and only if G/K satisfies the sentence

$$\widetilde{\delta}_{\mathbf{d}_2} := \text{res}(\phi_m^{G/K}, \widetilde{\widetilde{\delta_{\mathbf{d}_2}}}).$$

Finally, G/K has dimension $\mathbf{d}_2$ if and only if $G \models \delta^q_{\mathbf{d}_2}$, where $\delta^q_{\mathbf{d}_2}$ is the formula with parameters

$$\delta^q_{\mathbf{d}_2} := \text{lift}(\kappa(h_1, \ldots, h_r), \widetilde{\delta}_{\mathbf{d}_2}).$$

Remark 2.4.6. When dealing with a pronilpotent group of finite rank with just one factor (i.e., a p-adic analytic pro-p group) one can simplify the previous sentence by considering that, thanks to the fact that the dimension of a uniform group coincides with the minimal number of its generators, we can express the dimension of Q by means of the sentence $\beta^*_{\mathbf{d}_2} = \beta^*_{d_2}$.
In this case we can write that $\Phi^m(G/K)$ has dimension d_2 by means of the sentence (satisfied in $\Phi^m(G/K)$)

$$\widetilde{\widetilde{\delta'_{d_2}}} := s_{\triangleleft}(\text{bound}_d) \wedge \text{lift}(\text{bound}_d, \beta^*_{d_2}) \wedge \forall x : (\neg \text{bound}_d(x) \to x^{p^{f(d)+1}} \neq 1).$$

The same argument cannot be directly used in the case of multiple direct factors because we cannot single out the factors since they are not definable (see [NST], Remark after Proposition 5.12.) However, for each prime $p_i \in \pi$, the p_i-Frattini subgroup of Q, defined as $\Phi_{p_i}(Q) = [Q, Q]Q^{p_i}$, is definable. Since $|Q : \Phi_{p_i}(Q)| = p_i^{\mathrm{d}(Q_i)}$ and, as Q_i is uniform, $\mathrm{d}(Q_i) = (\mathbf{d}_2)_i$, one could write a sentence expressing the fact that the quotient $Q/\Phi_{p_i}(Q)$ has prescribed order $p_i^{(\mathbf{d}_2)_i}$ for each $p_i \in \pi$.

Conclusion

At this point we can conclude that a $\mathcal{C}_\pi$ group of rank r has dimension $\mathbf{d}$ if and only if it satisfies the sentence $\delta_{\pi,r,\mathbf{d}}$ given by

$$\begin{aligned} \exists h_1, \ldots, h_r : & \bigvee_{\mathbf{d}_1+\mathbf{d}_2=\mathbf{d}} \left(\delta^{\mathrm{s}}_{\mathbf{d}_1}(h_1, \ldots, h_r) \wedge \delta^{\mathrm{q}}_{\mathbf{d}_2}(h_1, \ldots, h_r) \right) \\ \wedge \neg \exists h_1, \ldots, h_r : & \bigvee_{\substack{\mathbf{m} \in \{0,\ldots,r\}^k \\ \mathbf{m} \neq (0,\ldots,0)}} \left(\bigvee_{\mathbf{d}_1+\mathbf{d}_2=\mathbf{d}+\mathbf{m}} (\delta^{\mathrm{s}}_{\mathbf{d}_1}(h_1, \ldots, h_r) \wedge \delta^{\mathrm{q}}_{\mathbf{d}_2}(h_1, \ldots, h_r)) \right). \end{aligned}$$

Indeed, it follows from the previous discussion that a $\mathcal{C}_\pi$ group of rank r and dimension $\mathbf{d}$ satisfies the formula

$$\exists h_1, \dots, h_r : \bigvee_{\mathbf{d}_1+\mathbf{d}_2=\mathbf{d}} \Big(\delta^{\mathrm{s}}_{\mathbf{d}_1}(h_1, \dots, h_r) \wedge \delta^{\mathrm{q}}_{\mathbf{d}_2}(h_1, \dots, h_r)\Big).$$

Conversely, if a $\mathcal{C}_\pi$ group G of rank r satisfies this formula, then its dimension is at least $\mathbf{d}$. Indeed, if G satisfies $\delta^{\mathrm{s}}_{\mathbf{d}_1} \wedge \delta^{\mathrm{q}}_{\mathbf{d}_2}$ with $\mathbf{d}_1 + \mathbf{d}_2 = \mathbf{d}$, then G has a normal subgroup N of dimension at least $\mathbf{d}_1$ (since the maximal dimension of the abelian subgroups of N is $\mathbf{d}_1$) such that the quotient G/N has dimension $\mathbf{d}_2$.

With the second half of the sentence,

$$\neg\exists h_1, \dots, h_r : \bigvee_{\substack{\mathbf{m}\in\{0,\dots,r\}^k \\ \mathbf{m}\neq(0,\dots,0)}} \left(\bigvee_{\mathbf{d}_1+\mathbf{d}_2=\mathbf{d}+\mathbf{m}} (\delta^{\mathrm{s}}_{\mathbf{d}_1}(h_1, \dots, h_r) \wedge \delta^{\mathrm{q}}_{\mathbf{d}_2}(h_1, \dots, h_r)) \right)$$

we rule out the possibility that the dimension is strictly greater than $\mathbf{d}$.

With the previous considerations we therefore obtained:

Theorem 2.4.7. *For every natural number r and every k-tuple of natural numbers $\mathbf{d} := (d_1, \dots, d_k)$, with $d_i \leq r$ for each $i \in \{1, \dots, k\}$, there is a sentence $\delta_{\pi,r,\mathbf{d}}$ in the language of groups $\mathcal{L}_{gp}$ such that, for every $\mathcal{C}_\pi$ group G of rank r, the following are equivalent:*

1. *G has dimension $\mathbf{d}$,*
2. *G is a model of $\delta_{\pi,r,\mathbf{d}}$.*

Corollary 2.4.8. *For every positive integer r, every k-tuple of natural numbers $\mathbf{d} := (d_1, \dots, d_k)$, with $d_i \leq r$ for each $i \in \{1, \dots, k\}$, and every k-tuple $\mathbf{r} := (r_1, \dots, r_k)$ satisfying $r = \max r_i$, there is a sentence $\overline{\delta}_{\pi,r,\mathbf{r},\mathbf{d}}$ in the language of groups $\mathcal{L}_{gp}$ such that, for every $\mathcal{C}_\pi$ group G, the following are equivalent:*

1. *G has rank r and dimension $\mathbf{d}$ and each factor G_i has rank r_i,*
2. *G is a model of $\overline{\delta}_{\pi,r,\mathbf{r},\mathbf{d}}$.*

Proof. Take

$$\overline{\delta}_{\pi,r,\mathbf{r},\mathbf{d}} := \sigma_{\pi,r,\mathbf{r}} \wedge \delta_{\pi,r,\mathbf{d}},$$

where $\sigma_{\pi,r,\mathbf{r}}$ is as in Corollary 2.3.6. □

2.4.3 Alternative sentences for the dimension for special classes of $\mathcal{C}_\pi$ groups of finite rank

In this section we provide alternative sentences for the dimension of $\mathcal{C}_\pi$ groups of finite rank belonging to special classes, namely soluble $\mathcal{C}_\pi$ groups of finite rank, $\mathcal{C}_\pi$ groups in which each factor is a just-infinite pro-p_i group of finite rank and pro-p groups of finite rank whose associated Lie algebra is non-abelian simple.

The approaches used for proving the finite axiomatizability of the dimension in this section differ from the one used in the general case, thus leading to different sentences.

For all this section fix $\pi := \{p_1, \dots, p_k\}$ to be a finite set of primes.

Soluble $\mathcal{C}_\pi$ groups

We prove the following:

Proposition 2.4.9. *Let r be a positive integer. For every k-tuple of natural numbers $\mathbf{d} := (d_i)_{i\in\{1,\dots,k\}}$ with $d_i \leq r$ for each $i \in \{1,\dots,k\}$, there is a sentence $\delta^{\mathrm{sol}}_{\pi,r,\mathbf{d}}$ in the language of groups $\mathcal{L}_{gp}$ such that for every soluble $\mathcal{C}_\pi$ group G of rank r the following are equivalent:*

1. *G has dimension $\mathbf{d}$;*
2. *G is a model of $\delta^{\mathrm{sol}}_{\pi,r,\mathbf{d}}$.*

We will need the following:

Lemma 2.4.10. *Let G be a soluble pro-p group of finite rank and positive dimension. Then G has a closed normal abelian subgroup of positive dimension.*

Proof. Let U be a normal uniform subgroup of finite index in G and let

$$\{1\} = U^{(n+1)} \lhd U^{(n)} \lhd \dots \lhd U^{(0)} = U$$

be the derived series of U.
The group $U^{(n)}$ is a closed normal abelian subgroup of G (see Proposition 1.2.2) and it has positive dimension. Indeed, it is a finitely generated abelian pro-p group, hence of the form $\mathbb{Z}_p^{d_n} \times F_n$, where $d_n \geq 0$ is a natural number and F_n is a finite abelian p-group. Since U is uniform, it is torsion-free, therefore F_n is trivial and necessarily $d_n > 0$.

□

Proof of Proposition 2.4.9. Let G be a soluble $\mathcal{C}_\pi$ group of finite rank r.
Since G is soluble, it contains a closed abelian normal subgroup A_0. Moreover, by Lemma 2.4.5 we can choose A_0 in such a way that $A_1 := C_G(C_G(A_0))$ is an abelian normal subgroup of maximal dimension among the abelian normal subgroups of G, by this meaning that each factor of A_1 has maximal dimension. Note that, thanks to Lemma 2.4.10, if G has at least one factor of positive dimension, then the dimension vector of A_1 has at least one positive entry.
Let $\widetilde{A_1} := C_G(A_0)$. Since G has rank r, there exist elements $a_1,\dots,a_r$ in G such that $\widetilde{A_1} = \langle a_1,\dots,a_r\rangle$.
Now consider $A_1 = C_G(\widetilde{A_1}) = C_G(a_1)\cap\dots\cap C_G(a_r)$ and let $\zeta(a,x)$ be the formula $ax = xa$.
Then $A_1 = \{x \in G \mid G \models \zeta(a_1,x) \wedge \dots \wedge \zeta(a_r,x)\}$ is a definable closed normal abelian subgroup of G containing A_0. Note that a subgroup of G defined by this formula is automatically closed.
Let $\overline{r}_1 \leq r$ be the rank of A_1 and let $\mathbf{d}_1$ be the dimension of A_1.
From the abelian case, we know that $\dim A_1 = \mathbf{d}_1$ if and only if $A_1 \models \delta^{\mathrm{ab}}_{\pi,\overline{r}_1,\mathbf{d}_1}$.
Since $\mathbf{d}_1^{\max} \leq \overline{r}_1 \leq r$, we have a finite number of possibilities for the value of the rank of A_1. Write $\overline{\delta}^{\mathrm{sol}}_{\mathbf{d}_1}$ for the sentence given by the corresponding union of $r - \mathbf{d}_1^{\max} + 1$ sentences, one for each possible value of $\overline{r}_1$:

$$\overline{\delta}^{\mathrm{sol}}_{\mathbf{d}_1} := \delta^{\mathrm{ab}}_{\pi,\mathbf{d}_1^{\max},\mathbf{d}_1} \vee \delta^{\mathrm{ab}}_{\pi,\mathbf{d}_1^{\max}+1,\mathbf{d}_1} \vee \dots \vee \delta^{\mathrm{ab}}_{\pi,r,\mathbf{d}_1}.$$

Then clearly $A_1 \models \overline{\delta}^{\mathrm{sol}}_{\mathbf{d}_1}$.
Similarly to what we did in the proof of Theorem 2.4.7, we can express the fact that A_1 is a normal abelian subgroup of maximal dimension in G.
Indeed, suppose that there is a normal abelian group $\overline{B}$ of dimension greater than $\mathbf{d}_1$ and assume that $C_G(\overline{B})$ is generated by the elements $b_1, \ldots, b_r$. Then $\overline{B}$ is contained in $B := C_G(C_G(\overline{B}))$, that, by Lemma 2.4.5, is a definable abelian normal subgroup of G defined by the formula $\beta := \zeta(b_1, x) \wedge \ldots \wedge \zeta(b_r, x)$. Then we can express the maximality of the dimension of A_1 by means of the sentence μ defined as

$$\neg\, \exists\, b_1, \ldots, b_r : (\mathrm{res}(\beta(b_1, \ldots, b_r), \bigvee_{\substack{\mathbf{m} \in \{0,\ldots,r\}^k \\ \mathbf{m} \neq (0,\ldots,0)}} \overline{\delta}_{\mathbf{d}_1 + \mathbf{m}} \wedge \alpha) \wedge s_{\lhd}(\beta(b_1, \ldots, b_r)),$$

where α is the formula defining being abelian.
Let $\alpha_1 := \alpha_1(a_1, \ldots, a_r, x)$ be the formula $\zeta(a_1, x) \wedge \ldots \wedge \zeta(a_r, x)$ that defines A_1. Then $G \models \delta^{\mathrm{sol}}_{\mathbf{d}_1}$, where

$$\delta^{\mathrm{sol}}_{\mathbf{d}_1} := \exists\, a_1, \ldots, a_r : \mathrm{res}(\alpha_1(a_1, \ldots a_r), \overline{\delta}^{\mathrm{sol}}_{\mathbf{d}_1}) \wedge \mathrm{res}(\alpha_1(a_1, \ldots, a_r), \alpha) \wedge \mu \wedge s_{\lhd}(\alpha_1(a_1, \ldots, a_r)).$$

In the previous sentence, $\mathrm{res}(\alpha_1(a_1, \ldots a_r), \overline{\delta}^{\mathrm{sol}}_{\mathbf{d}_1})$ states that A_1 has dimension $\mathbf{d}_1$, $\mathrm{res}(\alpha_1(a_1, \ldots, a_r), \alpha)$ states that A_1 is abelian, μ ensures that $\mathbf{d}_1$ is the maximal dimension among the dimensions of normal abelian subgroups of G and $s_{\lhd}(\alpha_1)$ implies that A_1 is a normal subgroup.

Now consider the quotient G/A_1. This is again a soluble $\mathcal{C}_\pi$ group of finite rank bounded by r and we can repeat the same reasoning as above. Proceeding as before we can find in G/A_1 a definable closed normal abelian subgroup A_2 of maximal dimension $\mathbf{d}_2$ with $\mathbf{d}_2^{\max} \leq r$. Note that, by Lemma 2.4.10, if the dimension of G is strictly greater than $\mathbf{d}_1$ (meaning that at least one entry of $\mathbf{d}$ is strictly greater than the corresponding entry of $\mathbf{d}_1$), then $\mathbf{d}_2$ has at least one positive entry.
With the same argument we get that $G/A_1 \models \overline{\overline{\delta}}^{\mathrm{sol}}_{\mathbf{d}_2}$, where

$$\overline{\overline{\delta}}^{\mathrm{sol}}_{\mathbf{d}_2} := \exists a'_1, \ldots, a'_r : \mathrm{res}(\alpha_2(a'_1, \ldots, a'_r), \overline{\delta}^{\mathrm{sol}}_{\mathbf{d}_2}) \wedge \mathrm{res}(\alpha_2(a'_1, \ldots, a'_r), \alpha) \wedge \mu' \wedge s_{\lhd}(\alpha_2),$$

where α_2 is the formula defining A_2 in G/A_1 and μ' is the formula establishing the maximality of the dimension of A_2 among the dimensions of normal abelian subgroups of G/A_1.
Hence, $G \models \delta^{\mathrm{sol}}_{\mathbf{d}_1} \wedge \delta^{\mathrm{sol}}_{\mathbf{d}_2}$, where $\delta^{\mathrm{sol}}_{\mathbf{d}_2} := \mathrm{lift}(\alpha_1, \overline{\overline{\delta}}^{\mathrm{sol}}_{\mathbf{d}_2})$.

Since G has rank r, we have to iterate this process for at most r times.
At the end of the process we find that G satisfies the sentence $\delta^{\mathrm{sol}}_{\mathbf{d}_1} \wedge \ldots \wedge \delta^{\mathrm{sol}}_{\mathbf{d}_r}$, where $\mathbf{d} := \dim G = \mathbf{d}_1 + \ldots + \mathbf{d}_r$.
Note that it is possible that there is an index i with $r \geq i \geq 1$ such that $\mathbf{d}_j = \mathbf{0}$ for every $i \leq j \leq r$.
We see that G satisfies also the sentence

$$\delta^{\mathrm{sol}}_{\pi,r,\mathbf{d}} := \bigvee_{\mathbf{d}_1 + \ldots + \mathbf{d}_r = \mathbf{d}} \delta^{\mathrm{sol}}_{\mathbf{d}_1} \wedge \ldots \wedge \delta^{\mathrm{sol}}_{\mathbf{d}_r}.$$

Conversely, if a soluble $\mathcal{C}_\pi$ group G of rank r satisfies $\delta^{\mathrm{sol}}_{\pi,r,\mathbf{d}}$, then G has dimension $\mathbf{d}$. Indeed, this sentence states that we can find a closed normal abelian subgroup of G of maximal dimension $\mathbf{d}_1$, then a closed normal abelian subgroup of G/A_1 of maximal dimension $\mathbf{d}_2$ and so on up to dimension $\mathbf{d}_r$. Because of the requirement of maximality of the dimension at each step and considering that the rank of G is r, we can conclude that $\dim G = \mathbf{d} = \mathbf{d}_1 + \ldots + \mathbf{d}_r$.

□

Corollary 2.4.11. *For every positive integer r and every k-tuple of natural numbers $\mathbf{d} := (d_i)_{i\in\{1,\ldots,k\}}$ and $\mathbf{r} := (r_i)_{i\in\{1,\ldots,k\}}$ with $d_i \leq r$ for each $i \in \{1,\ldots,k\}$ and $\max r_i = r$, there is a sentence $\overline{\delta}^{\mathrm{sol}}_{\pi,r,\mathbf{r},\mathbf{d}}$ in the language of groups $\mathcal{L}_{gp}$ such that, for every soluble $\mathcal{C}_\pi$ group G, the following are equivalent:*

1. *G has dimension $\mathbf{d}$ and rank r and each factor G_i has rank r_i;*
2. *G is a model of $\overline{\delta}^{\mathrm{sol}}_{\pi,r,\mathbf{r},\mathbf{d}}$.*

Proof. Take

$$\overline{\delta}^{\mathrm{sol}}_{\pi,r,\mathbf{r},\mathbf{d}} := \sigma_{\pi,r,\mathbf{r}} \wedge \delta^{\mathrm{sol}}_{\pi,r,\mathbf{d}},$$

where $\sigma_{\pi,r,\mathbf{r}}$ is as in Corollary 2.3.6.

□

Observe that, if one wants a sentence that is satisfied by a soluble $\mathcal{C}_\pi$ group G if and only if G has dimension $\mathbf{d}$ and rank r without imposing any restriction on the individual ranks of the factors G_i, it is enough to take the sentence

$$\left(\bigvee_{\mathbf{r}:\max r_i = r} \sigma_{\pi,r,\mathbf{r}}\right) \wedge \delta^{\mathrm{sol}}_{\pi,r,\mathbf{d}}.$$

$\mathcal{C}_\pi$ groups whose factors are just-infinite p-adic analytic pro-p groups

We start by recalling a definition.

Definition 2.4.12. A pro-p group is said to be *just-infinite* if it is an infinite pro-p group all of whose proper quotients are finite.

A non-soluble just-infinite p-adic analytic pro-p group G acts faithfully on its Lie algebra $\mathcal{L}(G)$ (see [KLGP], Proposition III.6). By using this fact, the argument used for proving the finite axiomatizability of the dimension of $\mathcal{C}_\pi$ groups can be slightly simplified in this case.

Let $G = G_1 \times \ldots \times G_k$ be a $\mathcal{C}_\pi$ group with rank r whose factors G_i are non-soluble just-infinite p_i-adic analytic pro-p_i groups of dimension d_i, for $i \in \{1,\ldots,k\}$.
Since each factor of G acts faithfully on its Lie algebra, G embeds into $\mathrm{GL}_{d_1}(\mathbb{Q}_{p_1}) \times \ldots \times \mathrm{GL}_{d_k}(\mathbb{Q}_{p_k})$. As we remarked in the proof of Theorem 2.4.7, setting $m := \lceil \log_2(r) + \varepsilon_\pi \rceil$, the torsion elements of $\Phi^m(G)$ form a finite $\mathcal{C}_\pi$ group $\mathrm{T}(\Phi^m(G))$ that is characteristic in $\Phi^m(G)$ and has order bounded by $p_1^{f_1(d_1)} \cdots p_k^{f_k(d_k)}$, where the f_i are the functions (2.8) defined in the proof of Theorem 2.4.7. Following

the proof of Theorem 2.4.7 we find that the fact that G has dimension $\mathbf{d} = (d_i)$ can be expressed by the sentence (holding true in the definable group $\Phi^m(G)$)

$$s_{\triangleleft}(\text{bound}_{\mathbf{d}}) \wedge \text{lift}(\text{bound}_{\mathbf{d}}, \mathfrak{q}_{\mathbf{d}}) \wedge \forall x : \left(\bigvee_{i=1}^{k} x^{p_i^{f(d_i)+1}} = 1 \to x^{p_i^{f(d_i)}} = 1 \right),$$

that expresses the fact that the formula $\text{bound}_{\mathbf{d}}$ describes the group $\mathrm{T}(\Phi^m(G))$ and that $\mathrm{T}(\Phi^m(G))$ is a normal subgroup of G such that $\dim(G/\mathrm{T}(\Phi^m(G)))(= \dim(G)) = \mathbf{d}$.

However, in our case the previous sentence can be simplified further. Indeed, consider the sentence

$$\delta^*_{\pi,\mathbf{d}} := s_{\triangleleft}(\text{bound}_{\mathbf{d}}) \wedge \text{lift}(\text{bound}_{\mathbf{d}}, \mathfrak{q}_{\mathbf{d}}),$$

from which, recalling that ϕ^G_m is the formula describing $\Phi^m(G)$, we obtain the sentence

$$\delta^{\text{j.i.}}_{\pi,r,\mathbf{d}} := \text{res}(\phi^G_m, \delta^*_{\pi,\mathbf{d}}).$$

Now, if a $\mathcal{C}_\pi$ group of rank r with non-soluble just-infinite p_i-adic analytic pro-p_i factors has dimension $\mathbf{d}$, then clearly it satisfies $\delta^{\text{j.i.}}_{\pi,r,\mathbf{d}}$ by the previous discussion.

Conversely, if such a group G satisfies $\delta^{\text{j.i.}}_{\pi,r,\mathbf{d}}$, then its dimension is at most $\mathbf{d}$. Indeed, let $\mathrm{T}(\Phi^m(G))$ be the torsion subgroup of $\Phi^m(G)$ and let

$$\mathrm{T}_{\mathbf{d}}(\Phi^m(G)) := \{x \in \Phi^m(G) : x^{p_1^{f(d_1)} \cdots p_k^{f(d_k)}} = 1\}.$$

Then clearly $\mathrm{T}_{\mathbf{d}}(\Phi^m(G)) \triangleleft \mathrm{T}(\Phi^m(G))$ and therefore, for each $i \in \{1, \ldots, k\}$,

$$\dim G_i = \mathrm{d}(\Phi^m(G)/\mathrm{T}(\Phi^m(G)))_i \leq \mathrm{d}(\Phi^m(G)/\mathrm{T}_{\mathbf{d}}(\Phi^m(G)))_i = d_i,$$

where the last equality is ensured by the sentence $\delta^{\text{j.i.}}_{\pi,r,\mathbf{d}}$ satisfied by G.

Since each G_i is a non-soluble just-infinite p_i-adic analytic pro-p_i group, if its dimension is less than d_i, then G_i embeds in $\mathrm{GL}_{k_i}(\mathbb{Q}_{p_i})$ with $k_i \leq d_i$. Therefore also $\Phi^m(G_i)$ embeds in $\mathrm{GL}_{k_i}(\mathbb{Q}_{p_i})$ and its torsion subgroup has order bounded by $p_i^{f(k_i)}$. Since each f_i is a monotone function, $p_i^{f(k_i)} \leq p_i^{f(d_i)}$ and thus $\mathrm{T}(\Phi^m(G)) \subseteq \mathrm{T}_{\mathbf{d}}(\Phi^m(G))$. It follows that $\mathrm{T}(\Phi^m(G)) = \mathrm{T}_{\mathbf{d}}(\Phi^m(G))$ and we can conclude that, for each $i \in \{1, \ldots, k\}$,

$$\dim G_i = \mathrm{d}(\Phi^m(G)/\mathrm{T}(\Phi^m(G)))_i = \mathrm{d}(\Phi^m(G)/\mathrm{T}_{\mathbf{d}}(\Phi^m(G)))_i = d_i,$$

hence $\dim G = \mathbf{d}$.

We therefore proved:

Proposition 2.4.13. *For every positive integer r and every k-tuple of natural numbers $\mathbf{d} := (d_i)_{i \in \{1,\ldots,k\}}$ with $d_i \leq r$ for each $i \in \{1, \ldots, k\}$, there is a sentence $\delta^{\text{j.i.}}_{\pi,r,\mathbf{d}}$ in the language of groups $\mathcal{L}_{gp}$ such that, for a $\mathcal{C}_\pi$ group G of rank r with non-soluble just-infinite p_i-adic analytic pro-p_i factors, the following are equivalent:*

1. *G has dimension $\mathbf{d}$;*
2. *G is a model of $\delta^{\text{j.i.}}_{\pi,r,\mathbf{d}}$.*

As usual, taking the sentence $\delta^{\text{j.i.}}_{\pi,r,\mathbf{d}} \wedge \sigma_{\pi,r,\mathbf{r}}$ we get the following variation:

Corollary 2.4.14. *For every positive integer r and every k-tuple of natural numbers $\mathbf{d} := (d_i)_{i\in\{1,\dots,k\}}$ and $\mathbf{r} := (r_i)_{i\in\{1,\dots,k\}}$ with $d_i \leq r$ for each $i \in \{1,\dots,k\}$ and $\max r_i = r$, there is a sentence $\overline{\delta}^{\text{j.i.}}_{\pi,r,\mathbf{r},\mathbf{d}}$ in the language of groups $\mathcal{L}_{gp}$ such that, for a $\mathcal{C}_\pi$ group G with non-soluble just-infinite p_i-adic analytic pro-p_i factors, the following are equivalent:*

1. *G has dimension $\mathbf{d}$ and rank r and each factor G_i has rank r_i;*
2. *G is a model of $\overline{\delta}^{\text{j.i.}}_{\pi,r,\mathbf{r},\mathbf{d}}$.*

Remark 2.4.15. When $\pi = \{p\}$, one has that a just-infinite pro-p group G of finite rank r has dimension d if and only if it satisfies $\delta^{\text{sol}}_{p,r,d} \vee \delta^{\text{j.i.}}_{p,r,d}$.

$\mathcal{C}_\pi$ groups whose factors have non-abelian simple Lie algebras

In this subsection we show that we can find an alternative formula to define the rank, as well as the rank and dimension vectors, of $\mathcal{C}_\pi$ groups $G = G_1 \times \cdots \times G_k$ all of whose factors G_i have non-abelian simple Lie algebra and that satisfy the following condition $(\star)_\upsilon$, involving a fixed first-order formula $\upsilon = \upsilon(z; x_1, \dots, x_l)$ in $l+1$ variables, which needs to be chosen carefully.

$(\star)_\upsilon$ The formula (with l parameters) υ defines a family of closed subsets of G such that every semi-uniform open normal subgroup N of G contains a non-trivial closed normal subgroup H_N that is definable in G by the formula $\upsilon(z) = \upsilon(z; a_1, \dots, a_l)$, where $a_1, \dots, a_l \in G$ are suitable parameters that depend on N.

Ideally, we would like to identify υ, depending only on π and r, such that $(\star)_\upsilon$ holds for all $\mathcal{C}_\pi$ groups G of rank at most r (all of whose factors have non-abelian simple Lie algebra), but currently it is not clear how this could be done; see Remark 2.4.20.

As usual, let $m := \lceil \log_2(r) + \varepsilon_\pi \rceil$. We will need the following:

Lemma 2.4.16. *Let G be a $\mathcal{C}_\pi$ group with rank r such that each factor G_i of G has non-abelian simple Lie algebra. Let N be a semi-uniform open normal subgroup of G and let H_N be a non-trivial closed subgroup of N that is normal in G. Then $\dim(G) = \dim(\Phi^m(H_N))$.*

Proof. We claim that, for each i, the closed uniform subgroup $\Phi^m(H_N)_i$ is of finite index in G_i. In our setting, G_i is a p_i-adic analytic pro-p_i group with non-abelian simple algebra and the open uniform subgroup N_i has the same Lie algebra as G_i. Assume by contradiction that $\Phi^m(H_N)_i$ has infinite index in G_i, hence in N_i. If $T/\Phi^m(H_N)_i$ denotes the torsion subgroup of the powerful group $N_i/\Phi^m(H_N)_i$, then, by Theorem 1.3.12, we have that $T/\Phi^m(H_N)_i$ is finite and that $N_i/T \cong N_i/\Phi^m(H_N)_i/T/\Phi^m(H_N)_i$ is uniform. Hence, by Theorem 1.3.14, T is a uniform normal subgroup of infinite index in N_i and therefore its corresponding Lie algebra is a non-trivial Lie ideal in the simple Lie algebra of N, which gives the required contradiction (compare also with the proof of Proposition 3.4.6).

Therefore, as, for each i, the closed subgroup $\Phi^m(H_N)_i$ is of finite index in G_i, we can conclude that the dimension of each G_i is the same as the dimension of $\Phi^m(H_N)_i$ and hence that the dimension of G is the same as the dimension of $\Phi^m(H_N)$. □

Proposition 2.4.17. *For every positive integer r and every k-tuple of natural numbers $\mathbf{d} := (d_i)_{i\in\{1,\dots,k\}}$ with $d_i \leq r$ for each $i \in \{1,\dots,k\}$, there is a sentence $\delta^{\mathrm{sim}}_{\pi,r,\mathbf{d}}$ in the language of groups $\mathcal{L}_{gp}$ such that, for a $\mathcal{C}_\pi$ group G with rank r satisfying $(\star)_\upsilon$ and all of whose factors have non-abelian simple Lie algebra, the following are equivalent:*

1. *G has dimension $\mathbf{d}$;*
2. *G is a model of $\delta^{\mathrm{sim}}_{\pi,r,\mathbf{d}}$.*

Proof. By $H_{\mathbf{a}}$ we will denote the closed subgroup of G defined by $\upsilon(a_1,\dots,a_l)$. Consider the sentence $\delta^{\mathrm{sim}}_{\pi,r,\mathbf{d}}$ defined as

$$\begin{aligned}
&\exists\, a_1,\dots,a_l :\ \mathrm{res}\Big(\upsilon(a_1,\dots,a_l),\ s_\lhd \wedge \forall x : x^{p_1\cdots p_k} = 1 \to x = 1\Big)\\
&\qquad\qquad \wedge\ \mathrm{res}\Big(\phi_m^{H_{\mathbf{a}}}, \sigma_{\pi,\max d_i,\mathbf{d}}\Big)\\
\wedge\, \neg\exists\, b_1,\dots,b_l :\ &\mathrm{res}\Big(\upsilon(b_1,\dots,b_l),\ s_\lhd \wedge \forall x : x^{p_1\cdots p_k} = 1 \to x = 1\Big)\\
&\qquad\qquad \wedge \bigvee_{\substack{\mathbf{u}\in\{0,\dots,r\}^k\\ \mathbf{u}\neq(0,\dots,0)}} \mathrm{res}\Big(\phi_m^{H_{\mathbf{b}}}, \sigma_{\pi,\max(d_i+u_i),\mathbf{d}+\mathbf{u}}\Big).
\end{aligned}$$

that expresses that there exist elements $a_1,\dots,a_l$ in G such that the group $H_{\mathbf{a}}$ defined by $\upsilon(a_1,\dots,a_l)$ is a normal torsion-free subgroup of G of dimension $\mathbf{d}$ and that there are no elements $b_1,\dots,b_l$ such that the group $H_{\mathbf{b}}$ is a normal torsion-free subgroup of dimension greater than $\mathbf{d}$. For the assertions on the dimension recall that, in a uniform group, the rank coincides with the minimal number of generators and with the dimension. Here, $\phi_m^{H_{\mathbf{a}}}$ defines the semi-uniform group $\Phi^m(H_{\mathbf{a}})$ and the sentence $\sigma_{\pi,\max d_i,\mathbf{d}}$ from Corollary 2.3.6 expresses the fact that $\Phi^m(H_{\mathbf{a}})$ has rank vector $\mathbf{d}$, which coincides with its dimension vector.

By Lemma 2.4.16, it follows that a $\mathcal{C}_\pi$ group satisfying $(\star)_\upsilon$ with rank r, dimension $\mathbf{d}$ and factors with non-abelian simple Lie algebras satisfies this sentence. Indeed, such a group contains an open normal semi-uniform subgroup N that, by condition $(\star)_\upsilon$, contains a non-trivial closed normal subgroup $H_{\mathbf{a}}$, defined by $\upsilon(a_1,\dots,a_l)$, for some $a_1,\dots a_l$ in G. Now, by Lemma 2.4.16, the dimension of $\Phi^m(H_{\mathbf{a}})$ is the same as the dimension of G, which is $\mathbf{d}$.

Conversely, let G be a $\mathcal{C}_\pi$ group satisfying $(\star)_\upsilon$, with rank r and factors with non-abelian simple Lie algebras, that satisfies the sentence $\delta^{\mathrm{sim}}_{\pi,r,\mathbf{d}}$. Then certainly G has dimension at least $\mathbf{d}$ (i.e., each factor G_i has dimension at least d_i).
Suppose by contradiction that G has dimension $\mathbf{d}+\mathbf{u}$, where each u_i is a non-negative integer and at least one d_i is positive. For any semi-uniform open normal subgroup U of G, let H_U be a non-trivial closed normal subgroup defined by υ and contained in U, according to condition $(\star)_\upsilon$. Then, by Lemma 2.4.16, the dimension of $\Phi^m(H_U)$ would be equal to $\mathbf{d}+\mathbf{u}$, the dimension of G. However, this would contradict the sentence $\delta^{\mathrm{sim}}_{\pi,r,\mathbf{d}}$.

□

Remark 2.4.18. For a pro-p group we can simplify the previous sentence to

$$\exists\, a_1,\dots,a_l : \mathrm{res}(\upsilon(a_1,\dots,a_l), s_\triangleleft \wedge \forall x : x^p = 1 \to x = 1) \wedge \mathrm{res}(\phi_m^{H_{\mathbf{a}}}, \beta_d^*)$$

$$\wedge\neg\exists\, b_1,\dots,b_l : \mathrm{res}(\upsilon(b_1,\dots,b_l), s_\triangleleft \wedge \forall x : x^p = 1 \to x = 1) \wedge \mathrm{res}(\phi_m^{H_{\mathbf{b}}}, \bigvee_{i=1}^{r-d} \beta_{d+i}^*),$$

as β_d^* expresses the fact that $\Phi^m(H_{\mathbf{a}})$, which is defined by $\phi_m^{H_{\mathbf{a}}}$, has minimal number of generators d.

Corollary 2.4.19. *For every positive integer r and every k-tuple of natural numbers $\mathbf{d} := (d_i)_{i\in\{1,\dots,k\}}$ and $\mathbf{r} := (r_i)_{i\in\{1,\dots,k\}}$ with $d_i \le r$ for each $i \in \{1,\dots,k\}$ and $\max r_i = r$, there is a sentence $\overline{\delta}^{\mathrm{sim}}_{\pi,r,\mathbf{r},\mathbf{d}}$ in the language of groups $\mathcal{L}_{gp}$ such that, for a $\mathcal{C}_\pi$ group G satisfying $(\star)_\upsilon$ and whose factors have non-abelian simple Lie algebra, the following are equivalent:*

1. *G has dimension $\mathbf{d}$ and rank r and each factor G_i has rank r_i;*
2. *G is a model of $\overline{\delta}^{\mathrm{sim}}_{\pi,r,\mathbf{r},\mathbf{d}}$.*

Remark 2.4.20. Let G be a $\mathcal{C}_\pi$ group and let N be a semi-uniform open normal subgroup of G. A natural candidate for the closed subgroups H_N in condition $(\star)_\upsilon$ would be the group $[G,N]$. Indeed, if N is a semi-uniform open normal subgroup of G, then $[G,N]$ is a closed normal subgroup of G contained in N. Moreover, it is non-trivial. Indeed, as the Lie algebra of each direct factor G_i of G is non-abelian, for each $i \in \{1,\dots,k\}$ we have that $[G_i,N_i] \neq 1$. This holds true because, if $[G_i,N_i] = 1$, in particular N_i would be abelian, in contradiction with the fact that its Lie algebra, that coincides with the Lie algebra of G_i, is not abelian. Therefore, $[G,N]$ is a non-trivial closed normal subgroup of G. However, it is currently not clear to us whether the groups $[G,N]$ are definable in the required way by a single formula υ, depending only on π and the rank $\mathrm{rk}(G)$.

The following example shows that, unfortunately, it is not possible to imitate directly the formula in Proposition 1.2.2: for a pronilpotent group G and N a closed normal subgroup of G generated by elements $a_1,\dots,a_r$, in general one cannot expect to have an equality of the form

$$[G,N] = [G,a_1]\cdot\dots\cdot[G,a_r].$$

Example 2.4.21. Let p be an odd prime and let $F = \mathbb{Q}_p(\zeta)$ be the cyclotomic extension of the field of p-adic numbers, obtained by adjoining a primitive p-th root of the identity. The valuation ring of F takes the form $\mathcal{O} = \mathbb{Z}_p[\zeta]$ and the additve group $(\mathcal{O},+)$ is isomorphic to $\mathbb{Z}_p^{p-1}$ and generated by $1,\zeta,\dots,\zeta^{p-2}$.

Now let m be a positive integer and let $N := \mathcal{O}/p^m\mathcal{O}$. Then N is a finite abelian group of order $p^{(p-1)m}$. Let C_p be the cyclic group of order p and let x be a generator. Consider the group $G := N \rtimes C_p$, where x acts as multiplication by ζ. The group operation in G is given by:

$$\begin{aligned}&(\overline{a}_1 + \overline{a}_2\zeta + \dots + \overline{a}_{p-1}\zeta^{p-2}, x^i)(\overline{b}_1 + \overline{b}_2\zeta + \dots + \overline{b}_{p-1}\zeta^{p-2}, x^j) = \\ &(\overline{a}_1 + \overline{a}_2\zeta + \dots + \overline{a}_{p-1}\zeta^{p-2} + \overline{b}_1\zeta^i + \overline{b}_2\zeta^{i+1} + \dots + \overline{b}_{p-1}\zeta^{i+p-2}, x^{i+j}),\end{aligned} \tag{2.9}$$

where the coefficients $\overline{a}_h$ and $\overline{b}_k$ are classes of elements of $\mathbb{Z}_p$ for each $h,k \in \{1,\dots,p-1\}$. The neutral element of the group is $(\overline{0},1)$.

By using the group operation (2.9) and the fact that every element of N has the form $(\overline{a}_1 + \overline{a}_2\zeta + \cdots + \overline{a}_{p-1}\zeta^{p-2}, 1)$, one can verify that $[G, N]$ is isomorphic to $(1-\zeta)N$. Therefore, if we choose m big enough, $[G, N]$ can have arbitrarily large order.
However, if x is any fixed element of N, the centraliser $C_G(x)$ of x in G is isomorphic to N if x is non-trivial and it is isomorphic to G if x is trivial. Hence, the conjugacy class of x in G can have cardinality p or 1, and the number of commutators of the form $[g, x]$, where x is a fixed element in N and g runs over G, is also p or 1.

Now suppose that we can write

$$[G, N] = \{[g_1, x_1] \cdots [g_l, x_l] \mid g_1, \ldots, g_l \in G\}$$

for some fixed positive integer l and some fixed elements $x_1, \ldots, x_l$ in N. Then one can obtain at most p^l elements of this form, which, for m big enough, contradicts the fact that the order of $[G, N]$ is bigger than p^l.

2.5 Finite axiomatizability of the dimension of $\mathcal{C}_\pi$ groups: another proof

In this section we present another proof for the finite axiomatizability of the dimension of $\mathcal{C}_\pi$ groups, following an approach that was suggested by Jon González-Sánchez. This proof is shorter than the previous one and leads to a formula with lower quantifier complexity. Moreover, the preliminary Theorem 2.5.1 is of independent interest.

We begin by establishing this very result, that is a new description of the dimension of a finitely generated powerful pro-p group. Recall that, by Theorem 1.3.12, the elements of finite order in a finitely generated powerful pro-p group G form a characteristic powerful finite subgroup T and the quotient G/T is uniform. Therefore, intuitively, $\dim G = \mathrm{d}(G/T)$ should equal $\mathrm{d}(G) - \mathrm{d}(T)$. In our result we prove that this is exactly what happens.

Theorem 2.5.1. *Let G be a finitely generated powerful pro-p group with torsion subgroup T and let $\Omega_{\{1\}}(G) = \{g \in G \mid g^p = 1\}$ denote the set of all elements of order 1 or p. Then*

$$\dim(G) = \mathrm{d}(G) - \log_p|\Omega_{\{1\}}(G)| = \mathrm{d}(G) - \mathrm{d}(T).$$

This theorem is a consequence of a result of Héthelyi and Lévai ([HL]); compare also with [Wi] and [FA].

Theorem 2.5.2 (Héthelyi, Lévai; [HL], Theorem 1)**.** *Let P be a powerful finite p-group. Given a subset $S \subseteq P$, let $\Omega_{\{1\}}(S)$ be the set of elements of S of order at most p. Then:*

$$|\Omega_{\{1\}}(P)| = |P : P^p| = p^{\mathrm{d}(P)}.$$

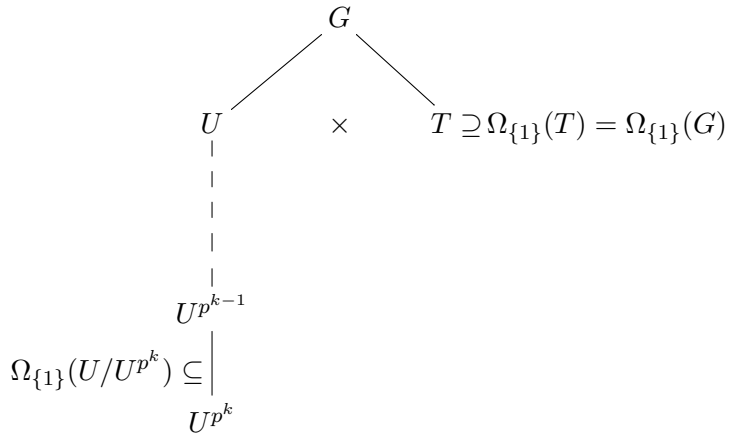
The idea of the proof of Theorem 2.5.1 is the following. We choose a positive integer k and an open uniform normal subgroup U of G such that $U \times T \trianglelefteq G$,

$$\mathrm{d}(G) = \mathrm{d}(G/U^{p^k}) \tag{2.10}$$

and

$$\Omega_{\{1\}}(G/U^{p^k}) \overset{1:1}{\longleftrightarrow} U^{p^{k-1}}/U^{p^k} \times \Omega_{\{1\}}(T), \tag{2.11}$$

thus obtaining the following diagram:



Considering the order of all the groups in (2.11) and taking $\log_p$ we obtain

$$\log_p|\Omega_{\{1\}}(G/U^{p^k})| = \log_p|U^{p^{k-1}}/U^{p^k}| + \log_p|\Omega_{\{1\}}(T)|.$$

We observe that $U^{p^k} = \Phi(U^{p^{k-1}})$, hence $\log_p|U^{p^{k-1}}/U^{p^k}| = \mathrm{d}(U) = \dim(G)$. Finally, using (2.10) and the result of Héthelyi and Lévai we can conclude that

$$\mathrm{d}(G) = \dim(G) + \mathrm{d}(T).$$

Proof of Theorem 2.5.1. The torsion subgroup T is finite and characteristic in G so that $C_G(T) \trianglelefteq_{\mathrm{o}} G$. We choose a uniform open normal subgroup $U \trianglelefteq_{\mathrm{o}} G$ such that $U \subseteq C_G(T)$ and $U \subseteq \Phi(G)$; we can always do that by considering a uniform open subgroup contained in a suitable power of the Frattini subgroup $\Phi(G)$ and intersecting it with $C_G(T)$. Since U is torsion-free, this implies that

$$N = U \times T \trianglelefteq_{\mathrm{o}} G \qquad \text{and} \qquad \mathrm{d}(G) = \mathrm{d}(G/U). \tag{2.12}$$

We show below that there exists $k \in \mathbb{N}$ such that $U^{p^k} = \Phi^k(U) \trianglelefteq_{\mathrm{o}} G$ satisfies

$$\Omega_{\{1\}}(G/U^{p^k}) = \Omega_{\{1\}}(N/U^{p^k}). \tag{2.13}$$

Since $N/U^{p^k} \cong U/U^{p^k} \times T$ and because U is uniform, $\Omega_{\{1\}}(N/U^{p^k})$ is in bijection with the cartesian product of sets

$$\Omega_{\{1\}}(U/U^{p^k}) \times \Omega_{\{1\}}(T) = U^{p^{k-1}}/U^{p^k} \times \Omega_{\{1\}}(G) \tag{2.14}$$

and furthermore $\log_p|U^{p^{k-1}}/U^{p^k}| = \mathrm{d}(U)$. Put $s(G) = \log_p|\Omega_{\{1\}}(G)|$. Then, from (2.13) and (2.14), we see that the finite powerful p-group $P = G/U^{p^k}$ satisfies

$$\log_p|\Omega_{\{1\}}(P)| = \mathrm{d}(U) + s(G) = \dim(G) + s(G).$$

The theorem of Héthelyi and Lévai 2.5.2 yields $\log_p|\Omega_{\{1\}}(P)| = \mathrm{d}(P)$ and $s(G) = \log_p|\Omega_{\{1\}}(T)| = \mathrm{d}(T)$ so that

$$\dim(G) = \log_p|\Omega_{\{1\}}(P)| - s(G) = \mathrm{d}(P) - s(G) \overset{(2.12)}{=} \mathrm{d}(G) - s(G) = \mathrm{d}(G) - \mathrm{d}(T).$$

It remains to establish (2.13). We show that there exists an open normal subgroup $W \trianglelefteq_{\mathrm{o}} G$ such that, for every $x \in G \smallsetminus N \subseteq_{\mathrm{c}} G$, we have $x^p \notin W$, or in other words $x^p \not\equiv_W 1$. Since U^{p^k}, $k \in \mathbb{N}$, is a base for the neighbourhoods of 1 in G, this implies that there exists $k_0 \in \mathbb{N}$ such that, for every $x \in G \smallsetminus N$, $x^p \notin U^{p^{k_0}} \subseteq W$, i.e., $\Omega_{\{1\}}(G/U^{p^k}) \subseteq \Omega_{\{1\}}(N/U^{p^k})$, as claimed (the reverse inclusion is obvious). From $T \subseteq N$ we see that $G \smallsetminus N$ does not contain any elements of finite order. Hence, for every $x \in G \smallsetminus N$ there exists $W_x \trianglelefteq_{\mathrm{o}} G$ such that $x^p \not\equiv_{W_x} 1$, and consequently $y^p \not\equiv_{W_x} 1$ for all $y \in xW_x \subseteq_{\mathrm{o}} G$. Since $G \smallsetminus N$ is compact, it is covered by a finite union of such cosets xW_x, i.e., $G \smallsetminus N \subseteq \bigcup_{x \in X} xW_x$ with $|X| < \infty$. This implies that $W = \cap_{x \in X} W_x \trianglelefteq_{\mathrm{o}} G$ has the required property. □

As in the previous sections, if $\pi = \{p_1, \ldots, p_k\}$ and $G = G_1 \times \cdots \times G_k$ is a $\mathcal{C}_\pi$ group, we assume that each factor G_i is a Sylow pro-p_i subgroup of G.

Theorem 2.5.3. *For every positive integer r and all tuples of natural numbers $\mathbf{d} := (d_i)_{i \in \{1,\ldots,k\}}$ and $\mathbf{r} := (r_i)_{i \in i \in \{1,\ldots,k\}}$ satisfying $d_i \leq r$ for each i and $r = \max r_i$, there is a sentence $\delta^{alt}_{\pi,r,\mathbf{r},\mathbf{d}}$ in the language of groups $\mathcal{L}_{gp}$ such that, for every $\mathcal{C}_\pi$ group G, the following are equivalent:*

1. *G has rank r and dimension $\mathbf{d}$ and each factor G_i has rank r_i,*
2. *G is a model of $\delta^{alt}_{\pi,r,\mathbf{r},\mathbf{d}}$.*

Proof. Recall that $m = m(r) := \lceil \log_2(r) \rceil + 1$. Then $\Phi^m(G)$ is a semi-powerful and definable subgroup of (π, r)-bounded index in G. The dimensions of the direct factors of G do not change if we pass from G to an open subgroup. It is therefore enough to detect the dimensions of the direct factors of $F := \Phi^m(G)$. Let F_i denote the Sylow pro-p_i subgroup of F and T_i its torsion subgroup, for $p_i \in \pi$. By Theorem 2.5.1 it suffices to produce a sentence which defines the invariants

$$\mathrm{d}(F_i) = \log_{p_i} |F_i : \Phi(F_i)| \qquad \text{and} \qquad \mathrm{d}(T_i) = \log_{p_i} |\Omega_{\{1\}}(F_i)|,$$

within the finite range $\{0, 1, \ldots, r\}$, where $\Omega_{\{1\}}(F_i) = \{g \in F_i \mid g^{p_i} = 1\}$ is the set of all elements of F_i of order 1 or p_i. We observe that $F_i/\Phi(F_i) \cong F/F^{p_i}[F,F] = F/\Phi_{p_i}(F)$ is isomorphic to the p_i-Frattini quotient of F and that $\Omega_{\{1\}}(F_i) = \{g \in F \mid g^{p_i} = 1\}$.

The Frattini quotient $F/\Phi(F)$ has (π, r)-bounded order and maps onto the p_i-Frattini quotient $F/\Phi_{p_i}(F)$. As we have already seen, the group $F/\Phi(F)$ is interpretable in F, hence in G. There is a sentence which detects any prescribed isomorphism type of $F/\Phi(F)$ among a (π, r)-bounded number of possibilities. Forming a suitable disjunction, we can also detect the isomorphism type of the p_i-Frattini quotient $F/\Phi_{p_i}(F)$ and hence the minimal numbers of generators $\mathrm{d}(F_i)$. Alternatively, as $F/\Phi_{p_i}(F)$ is powerful, we can directly use the sentence $\beta^*_{\mathrm{d}(F_i)}$ to impose that $\mathrm{d}(F_i)$ is the minimal number of generators of F_i, but this yields a worse quantifier complexity (see Section 2.8).

Clearly, the closed subset $\{g \in F \mid g^{p_i} = 1\} \subseteq_{\mathrm{c}} F$ is definable in F, hence in G, by the formula $\omega(g) := g^{p_i} = 1$. Moreover, its size equals $p_i^{\mathrm{d}(T_i)}$ and is thus at most p_i^r. We can easily identify by means of a sentence its precise size and hence the invariant $\mathrm{d}(T_i)$.

In conclusion, if $\phi^F_{p_i,1}$ is the formula defining $\Phi_{p_i}(F) = [F,F]F^{p_i}$ in F, the group G of rank r has dimension $\mathbf{d}$ if and only if the subgroup $F = \Phi^m(G)$ satisfies the sentence ς given by

$$\bigvee_{\substack{\mathrm{d}(F_i),\,\mathrm{d}(T_i):\\ \mathrm{d}(F_i),\,\mathrm{d}(T_i)\leq r\\ \mathrm{d}(F_i)-\mathrm{d}(T_i)=d_i}} \bigwedge_{i\in\{1,\dots,k\}} \Big(\mathrm{lift}(\phi^F_{p_i,1}, \beta^*_{\mathrm{d}(F_i)})$$
$$\wedge\ \exists g_1,\dots g_{p^{\mathrm{d}(T_i)}} : g_n \neq g_j\ \wedge\ \omega(g_n) \text{ for all } n,j \in \{1,\dots,p^{\mathrm{d}(T_i)}\}$$
$$\wedge\ \neg\exists g_1,\dots g_{p^{\mathrm{d}(T_i)}+1} : g_n \neq g_j\ \wedge\ \omega(g_n) \text{ for all } n,j \in \{1,\dots,p^{\mathrm{d}(T_i)}+1\}\Big)$$

if and only if G satisfies the sentence

$$\delta^{\mathrm{alt}}_{\pi,r,\mathbf{r},\mathbf{d}} := \sigma_{\pi,r,\mathbf{r}} \wedge \mathrm{res}(\phi^G_m, \varsigma),$$

where $\sigma_{\pi,r,\mathbf{r}}$ is the sentence established in Corollary 2.3.6 which expresses the fact that G has rank r and each factor G_i has rank r_i. □

2.6 Finite axiomatizability of the rank of pro-π groups

In this section we prove that, given $\pi := \{p_1,\dots,p_k\}$ a finite set of primes, the rank of a pro-π group is finitely axiomatizable. Recall that pro-π groups are inverse limits of finite π-groups, i.e., finite groups whose index is divisible only by primes in π. An example of an infinite pro-π group is given by $\mathrm{GL}_d(\mathbb{Z}_p)$. The finite axiomatizability of the rank of these groups relies on the classification of the finite simple groups and on the finite axiomatizability of the rank of pronilpotent pro-π groups. We will need the following result, that generalizes Theorem 2.3.1 to virtually pronilpotent groups. Recall that, if G is a profinite group, $\mathrm{rk}_p(G)$ is the rank of any Sylow pro-p subgroup of G.

Theorem 2.6.1. *Let R be a positive integer. Suppose that the profinite group G has an open normal subgroup $F \trianglelefteq_{\mathrm{o}} G$ which is pronilpotent and such that each Sylow subgroup of F is powerful.*

1. *If $\mathrm{rk}_p(G) \leq R$ for some prime p, then*
$$\mathrm{rk}_p(G) = \mathrm{rk}_p\big(G/\Phi^{2R+1}(F)\big).$$
2. *If $\mathrm{rk}(G) \leq R$, then*
$$\mathrm{rk}(G) = \mathrm{rk}\big(G/\Phi^{2R+1}(F)\big).$$

Proof. It is convenient to write $F_i = \Phi^i(F)$ for $i \in \mathbb{N}$.

1. This part reduces to the virtually pro-p case (see Theorem 2.3.5). Indeed, let p be a prime such that $r_p = \mathrm{rk}_p(G) \leq R$. We need to show that $r_p = \mathrm{rk}_p(G/F_{2R+1})$. Since F is pronilpotent, its Hall pro-p' subgroup P' is normal in G. Working modulo P', we may assume without loss of generality that F is a powerful pro-p group. In this situation G is virtually a pro-p group and we can apply Theorem 2.3.5.

2. Now suppose that $\mathrm{rk}(G) \leq R$. Clearly, the maximal local rank

$$\mathrm{mlr}(G) = \max\left(\{\mathrm{rk}_p(G) \mid p \text{ prime}\}\right)$$

is at most $\mathrm{rk}(G)$. Conversely, Lucchini established in Theorem 3 and Corollary 4 in [L2] (see also [L] and [L1]) that

$$\mathrm{rk}(G) \leq \mathrm{mlr}(G) + 1,$$

with equality if and only if there are

- an odd prime p such that $r_p = \mathrm{rk}_p(G) = \mathrm{mlr}(G)$ and
- an open subgroup $H \leq_{\mathrm{o}} G$ and $N \trianglelefteq_{\mathrm{o}} H$ such that

$$H/\Phi_p(N) \cong H/N \ltimes N/\Phi_p(N) \cong C_q \ltimes C_p^{\mathrm{mlr}(G)},$$

  where $H/N \cong C_q$ is cyclic of prime order $q \mid (p-1)$, the p-Frattini quotient $N/\Phi_p(N) \cong C_p^{\mathrm{mlr}(G)}$ is elementary abelian of rank $\mathrm{mlr}(G)$, and H/N acts via conjugation faithfully on $N/\Phi_p(N)$ by power automorphisms (i.e., by non-zero homotheties if we regard $N/\Phi_p(N)$ as an $\mathbb{F}_p$-vector space).

Note that this result currently relies on the classification of finite simple groups. For short let us refer within this proof to such a pair (H, N) as a 'runaway couple' for G with respect to p.

By the first part of the theorem, we have $\mathrm{mlr}(G) = \mathrm{mlr}(G/F_{2R+1})$, and hence it suffices to show: if G admits a runaway couple, then so does G/F_{2R+1}, in fact, with respect to the same prime. This ensures that, if $\mathrm{rk}(G) = \mathrm{mlr}(G) + 1$, then also $\mathrm{rk}(G/F_{2R+1}) = \mathrm{mlr}(G/F_{2R+1}) + 1 = \mathrm{mlr}(G) + 1 = \mathrm{rk}(G)$. Conversely, it is clear that, if G/F_{2R+1} admits a runaway couple, i.e., if $\mathrm{rk}(G/F_{2R+1}) = \mathrm{mlr}(G/F_{2R+1})+1 = \mathrm{mlr}(G)+1 \geq \mathrm{rk}(G)$, then $\mathrm{rk}(G) \leq \mathrm{rk}(G/F_{2R+1}) = \mathrm{mlr}(G)+1$ and therefore $\mathrm{rk}(G) = \mathrm{mlr}(G) + 1 = \mathrm{rk}(G/F_{2R+1})$. Suppose that (H, N) is a runaway couple for G with respect to an odd prime p so that $H/\Phi_p(N) \cong C_q \ltimes C_p^{r_p}$ as detailed above, with the additional property that $|G : H|$ is as small as possible. Assume for a contradiction that G/F_{2R+1} does not admit a runaway couple.

As in the proof of the first part of the theorem, there is no harm in factoring out the Hall pro-p' subgroup P' of F, because $H \cap F \subseteq N$ and $H \cap P' \subseteq \Phi_p(N)$. Consequently we may as well assume that $F \trianglelefteq_{\mathrm{o}} G$ is a powerful pro-p group, which makes G virtually a pro-p group.

As in the proof of Theorem 2.3.5, the sequence

$$\mathrm{d}(H/((H \cap F_j)\Phi_p(N))) = \mathrm{d}(HF_j/\Phi_p(N)F_j), \quad j \in \mathbb{N},$$

is non-decreasing and eventually constant, with final constant value

$$\mathrm{d}(H/\Phi_p(N)) = \mathrm{d}(H) = r_p + 1 < 2R + 1.$$

We use the same arguments as the ones in the proof of Theorem 2.3.5 to conclude that there exists $j = j(H)$ such that the analogue of (2.3) for $H/\Phi_p(N)$ holds and we reduce to the situation where $[F_j, F_j] = F_{2j} = 1$. This reduction renders G finite, with abelian normal p-subgroups

$$A = F_j \qquad \text{and} \qquad B = F_{j+1} = \Phi(F_j) = A^p;$$

furthermore, we have

$$l = \mathrm{d}\big(N/((H\cap A)\Phi_p(N))\big) = \mathrm{d}\big(N/((H\cap B)\Phi_p(N))\big) < \mathrm{d}(N/\Phi_p(N)) = r_p. \quad (2.15)$$

It suffices to produce a runaway couple $(\widetilde{H}, \widetilde{N})$ for the group HA with respect to p such that $|HA : \widetilde{H}| < |HA : H|$; thus we may assume that

$$G = HA.$$

This reduction allows us to conclude that $\Phi_p(N) \cap A \trianglelefteq G$ and there is no harm in assuming $\Phi_p(N) \cap A = 1$. Likewise $M = H \cap A \trianglelefteq G$, and reduction modulo $\Phi_p(N)$ induces an embedding of $M \leq N$ into the elementary abelian group $N/\Phi_p(N) \cong C_p^{r_p}$. Using (2.15), we conclude that

$$M = H \cap A = H \cap B = \langle b_1, \ldots, b_m\rangle \cong C_p^m \qquad \text{for } m = r_p - l \geq 1.$$

The normal subgroup $M\Phi_p(N) \trianglelefteq H$ decomposes as a direct product $M \times \Phi_p(N)$. Recall that $H/\Phi_p(N) \cong C_q \ltimes C_p^{r_p}$, with the action given by power automorphisms. We build a minimal generating set $x, y_1, \ldots, y_l, b_1, \ldots, b_m$ for H modulo $\Phi_p(N)$ by choosing

$$x \in H \smallsetminus N \quad \text{and} \quad y_1, \ldots, y_l \in N$$

which supplement $b_1, \ldots, b_m$ suitably. We set

$$L_1 = \langle x, y_1, \ldots, y_l\rangle \leq H \qquad \text{and} \qquad L = L_1\Phi_p(N) \leq H.$$

In this situation $H = LM$ and we claim that $L \cap M = 1$ so that

$$H = L \ltimes M.$$

Indeed, our construction yields that the intersection in $H/\Phi_p(N) \cong C_q \ltimes C_p^{l+m}$ of the subgroups

$$L/\Phi_p(N) = \langle \overline{x}\rangle \ltimes \langle \overline{y_1}, \ldots, \overline{y_l}\rangle \cong C_q \ltimes C_p^l \quad \text{and} \quad M\Phi_p(N)/\Phi_p(N) \cong M \cong C_p^m$$

is trivial. This gives $L \cap M \subseteq \Phi_p(N)$ and consequently $L \cap M \subseteq \Phi_p(N) \cap M = 1$.

Put $\widetilde{M} = \{a \in A \mid a^p \in M\} \trianglelefteq G$. Recall that $M = H \cap B$ and $B = A^p$. The p-power map constitutes a surjective G-equivariant homomorphism $\widetilde{M} \to M$ whose kernel $K \trianglelefteq G$, say, includes M. From $L \cap M = 1$ we conclude that $LK \cap \widetilde{M} = (L \cap \widetilde{M})K \subseteq K$. Moreover, we have $L \cap K \subseteq H \cap A = M$ and thus $L \cap K \subseteq L \cap M = 1$.

These considerations show that the group $\widetilde{H} = L\widetilde{M}$ maps onto

$$\widetilde{H}/K \cong LK/K \ltimes \widetilde{M}/K \cong L \ltimes M = H,$$

and hence onto $C_q \ltimes C_p^{r_p}$. Thus $\widetilde{H}$ gives rise to a runaway couple for G, with respect to the prime p, just as H does. To conclude the proof we observe that $|K| \geq |M| \geq p$ implies $|\widetilde{H}| > |\widetilde{H}|/|K| = |H|$ and hence $|G : \widetilde{H}| < |G : H|$. □

Corollary 2.6.2. *Let R be a positive integer. Suppose that the profinite group G has an open normal subgroup $F \trianglelefteq_{\mathrm{o}} G$ which is pronilpotent.*

1. *If* $\mathrm{rk}_p(G) \leq R$ *for some prime* p*, then*

$$\mathrm{rk}_p(G) = \mathrm{rk}_p\big(G/\Phi^{2R+\lceil \log_2(R)\rceil+2}(F)\big).$$

2. *If* $\mathrm{rk}(G) \leq R$*, then*

$$\mathrm{rk}(G) = \mathrm{rk}\big(G/\Phi^{2R+\lceil \log_2(R)\rceil+2}(F)\big).$$

Proof. As in the proof of Theorem 2.6.1, one reduces to the case in which F is a pro-p group for a single prime p. From $\mathrm{rk}(F) \leq R$ it follows that $\Phi^{\lceil \log_2(R)\rceil+1}(F) \trianglelefteq_{\mathrm{o}} G$ is powerful. Therefore we can apply Theorem 2.6.1 to $\Phi^{\lceil \log_2(R)\rceil+1}(F)$ in place of F. □

Remark 2.6.3. As stated in the proof of Theorem 2.6.1, the result of Lucchini that we used to prove the second part of the theorem (hence of the corollary) currently relies on the classification of finite simple groups. However, in the prosoluble case the same result holds without use of the classification (see [L], Section 5). In particular, if $2 \notin \pi$, every pro-π group is prosoluble because of the Odd Order Theorem by Feit and Thompson.

Theorem 2.6.4. *Let* $\pi := \{p_1, \ldots, p_k\}$ *be a finite set of primes. For each positive integer* r *and for each tuple* $\mathbf{r} = (r_i)_{i\in\{1,\ldots,k\}}$ *in* $\{0, 1, \ldots, r\}$ *there exists a sentence* $\tilde{\sigma}_{\pi,r,\mathbf{r}}$ *in the language of groups* $\mathcal{L}_{gp}$ *such that, for every pro-*π *group* G*, the following are equivalent:*

1. $\mathrm{rk}(G) = r$ *and* $\mathrm{rk}_{p_i}(G) = r_i$ *for every* $i \in \{1, \ldots, k\}$*;*

2. G *is a model of* $\tilde{\sigma}_{\pi,r,\mathbf{r}}$*.*

The idea of the proof of this theorem is similar to the one of the proof of Corollary 2.3.6, i.e., given a pro-π group of finite rank r, we find a definable open $\mathcal{C}_\pi$ subgroup F that is semi-powerful and of bounded index in G, of which we can express the rank thanks to Corollary 2.3.6. From $\mathrm{rk}(G) \leq \mathrm{rk}(F) + \mathrm{rk}(G/F)$ we obtain a bound R on the rank of G. Finally, we impose in our sentence that $\mathrm{rk}(G/\Phi^{2R+1}(F)) = r$, which guarantees, thanks to Theorem 2.6.1, that $\mathrm{rk}(G) = r$.

Proof. Let G be a pro-π group with rank bounded by r and consider the set $\mathcal{S} := \{S \mid S \text{ finite simple } \pi\text{-group}\}$. Using the classification of finite simple groups one can deduce that $\mathcal{S}$ is finite ([Ma], Remark page 51).

Let Λ be the set

$$\{\phi \mid \phi : G \to \mathrm{Aut}(S^m) \text{ homomorphism}, S \in \mathcal{S}, m \in \mathbb{N} \text{ with } \mathrm{d}(S^m) \leq r\}.$$

Since $\mathcal{S}$ is finite, by definition Λ is also finite. It follows that the group

$$K := \bigcap_{\phi\in\Lambda} \mathrm{Ker}\phi$$

is an open normal subgroup of G and the finite quotient G/K has order bounded by a function $f(r, \pi)$ of r and π.

We claim that K is a pronilpotent pro-π group, i.e., a $\mathcal{C}_\pi$ group. Indeed, let L be an open normal subgroup of G. Starting from L we can construct a chief series

$$L =: G_n \lhd G_{n-1} \lhd \ldots \lhd G_1 \lhd G_0 := G,$$

where each G_i, for $i \in \{0, \ldots, n\}$, is normal in G and each quotient G_i/G_{i+1}, for $i \in \{0, \ldots, n-1\}$, is finite, hence of the form S^k for some $k \in \mathbb{N}$ and $S \in \mathcal{S}$. Moreover, since $\mathrm{rk}(G) \leq r$, the minimal number of generators of each such quotient is bounded by r. From such a series we get a normal series for K:

$$K \cap L = K \cap G_n \lhd K \cap G_{n-1} \lhd \ldots \lhd K \cap G_1 \lhd K \cap G_0 = K.$$

Since the quotients $K \cap G_i / K \cap G_{i+1}$ ($i \in \{0, \ldots, n-1\}$) are again of the form S^k for some $k \in \mathbb{N}$, $S \in \mathcal{S}$ and $\mathrm{d}(S^k) \leq r$, the action of K on them is trivial by the definition of K. It follows that $[K, K \cap G_i] \subseteq K \cap G_{i+1}$, i.e., the series

$$1 \lhd \frac{K \cap G_{n-1}}{K \cap G_n} \lhd \ldots \lhd \frac{K}{K \cap G_n} = \frac{K}{K \cap L}$$

is central and $K/K \cap L$ is nilpotent. Since every finite quotient of K arises as a quotient of some $K/K \cap L$ we can conclude that K is pronilpotent.

Now consider the group $H := G^{f(r,\pi)}$. By [NS1], Theorem 1, the word $g^{f(r,\pi)}$ has finite width and therefore H is a definable subgroup of G contained in K with index that is (π, r)-bounded by the positive solution to the Restricted Burnside Problem. In this specific case, however, we do not need to use these general theorems to infer these properties of H. Indeed, assume for the moment that the pro-π group G of rank r is finite of exponent $f(\pi, r)$. We need to show that $|G|$ is (π, r)-bounded. We established that G has a nilpotent normal subgroup K of (π, r)-bounded index. Thus there is no harm in assuming that $G = K$. Furthermore, K is a direct product of its Sylow p-subgroups, where p ranges over the finite set π. Hence we may even assume that G is a p-group of rank at most r, for some $p \in \pi$, and that $f(\pi, r)$ is a p-power, p^e say. In this situation, G contains a powerful normal subgroup of (p, r)-bounded index (see [DDMS], Theorem 2.13), and we may assume that G itself is powerful. The p-power series of a powerful p-group coincides with its lower p-series, and we obtain the bound $|G| \leq p^{re}$. As for the fact that every element of H can be written as a product of a (π, r)-bounded number of $f(\pi, r)$-th powers, descending without loss of generality to a subgroup of (π, r)-bounded index, as above, it suffices to recall that in a powerful pro-p group every product of p^e-th powers is itself a p^e-th power; see [DDMS], Corollary 3.5.

As K is pronilpotent, so is H and we can express this fact with a first-order sentence.

Claim. One can express with a first-order sentence that H is pronilpotent.

Proof of Claim. The idea of the proof is that H is pronilpotent if and only if $H/Z(H)$ is pronilpotent and we can express that the latter quotient is pronilpotent; note that this quotient is definable in G as H is definable.

Let $H_1, \ldots, H_k$ be the Sylow subgroups of H and, for $i \in \{1, \ldots, k\}$, let $x_1^i, \ldots, x_r^i$ be generators of H_i.

We first note that, for every $i \in \{1, \ldots k\}$,

$$C_H(H_i) = H_1 \times \cdots \times H_{i-1} \times Z(H_i) \times H_{i+1} \times \cdots \times H_k,$$

from which it follows that

$$\widetilde{\frac{C_H(H_i)}{Z(H)}} := \frac{C_H(H_1) \cap \ldots \cap C_H(H_{i-1}) \cap C_H(H_{i+1}) \cap \ldots \cap C_H(H_k)}{Z(H)} \cong \frac{H_i}{Z(H_i)}.$$

Therefore,

$$H/Z(H) = \frac{H_1 \times \cdots \times H_k}{Z(H_1) \times \cdots \times Z(H_k)} \cong \prod_{i=1}^{k} \widetilde{\frac{C_H(H_i)}{Z(H)}}. \tag{2.16}$$

Now each $C_H(H_i)$ is a definable subgroup (with parameters $x_1^i, \ldots, x_r^i$) defined as $\{x \in H \mid [x, x_j^i] = 1 \text{ for all } j : 1 \leq j \leq r\} = \{x \in H \mid \zeta(x, x_j^i) \text{ for all } j : 1 \leq j \leq r\}$. It follows that also the quotients $\widetilde{C_H(H_i)/Z(H)}$ ($i \in \{1, \ldots, k\}$) are definable.

We can then express the isomorphism (2.16) by a sentence ι holding true in H that states that

$$\widetilde{\frac{C_H(H_1)}{Z(H)}} \cdots \widetilde{\frac{C_H(H_k)}{Z(H)}} = \frac{H}{Z(H)}$$

as sets, that

$$\widetilde{\frac{C_H(H_i)}{Z(H)}} \cap \left(\widetilde{\frac{C_H(H_1)}{Z(H)}} \cdots \widetilde{\frac{C_H(H_{i-1})}{Z(H)}} \cdot \widetilde{\frac{C_H(H_{i+1})}{Z(H)}} \cdots \widetilde{\frac{C_H(H_k)}{Z(H)}} \right) = \{1\}$$

for each $i \in \{1, \ldots, k\}$ and that each factor $\widetilde{C_H(H_i)/Z(H)}$ is normal in $H/Z(H)$.

Moreover, we can express that each $Q_i := \widetilde{C_H(H_i)/Z(H)}$ is a pro-p_i group with a first-order sentence pr_i holding in H: given any $h \in Q_i$, the group $Z(C_{Q_i}(h))$ is a definable abelian pro-p_i subgroup of Q_i with rank bounded by r. This can be expressed by checking that the prime p_i is the only prime in π that occurs in the factorization of $Z(C_{Q_i}(h))$, as we did for expressing the dimension of an abelian $\mathcal{C}_\pi$ group. More precisely, $Z(C_{Q_i}(h))$ must satisfy the sentence $\bigvee_{r_i=1}^{r} \bigvee_{j=0}^{r_i} \tilde{\delta}^{\mathrm{ab}}_{p_i,r_i,j}$:

$$\forall h \in \widetilde{\frac{C_H(H_i)}{Z(H)}} : Z(C_{Q_i}(h)) \models \bigvee_{r_i=1}^{r} \bigvee_{j=0}^{r_i} \tilde{\delta}^{\mathrm{ab}}_{p_i,r_i,j}.$$

(Recall that $Z(C_{Q_i}(h)) \models \tilde{\delta}^{\mathrm{ab}}_{p_i,r_i,j}$ means that $Z(C_{Q_i}(h))$ is abelian and that

$$Z(C_{Q_i}(h)) \cong \mathbb{Z}_{p_i}^{j} \times C_{p_i}^{s_1} \times \cdots \times C_{p_i}^{s_l}$$

for some j and r_i, with $j + l = r_i$.)
Alternatively, as Q_i is a pro-π group, it is enough to impose that each element of Q_i is a q_i-th power, for $q_i = p_1 \cdots p_{i-1} p_{i+1} \cdots p_k$.

Putting everything together, one obtains a sentence that states that $H/Z(H)$ is a pronilpotent pro-π group, and hence that H is a pronilpotent pro-π group. □

Therefore, if $\mathfrak{n}$ is the formula defining H and ϖ is the sentence defining finite groups with order bounded by $f(r, \pi)$ and rank bounded by r, we can conclude that G satisfies the sentence $\eta_{\pi,r}$ given by

$$\mathrm{res}(\mathfrak{n}, \iota) \wedge \mathrm{res}(\mathfrak{n}, \bigwedge_{i=1}^{k} \mathrm{pr}_i) \wedge \mathrm{res}(\mathfrak{n}, \bigvee_{\tilde{r}=1}^{r} \bigvee_{\tilde{\mathbf{r}}:\max(\tilde{\mathbf{r}})_i=\tilde{r}} \sigma_{\pi,\tilde{r},\tilde{\mathbf{r}}}) \wedge \mathrm{lift}(\mathfrak{n}, \varpi).$$

In the previous sentence, the first term describes the isomorphism (2.16), the second term implies that H is a $\mathcal{C}_\pi$ group, the third term assures that $\mathrm{rk}(H) \leq r$ and the last term implies that the finite group G/H has rank bounded by r.

At this point we have a sentence $\eta_{\pi,r}$ that is satisfied by any pro-π group of rank r; conversely, if a pro-π group G satisfies $\eta_{\pi,r}$, then the rank of G is bounded by $2r$.

Now, let $R := 2r$ and consider the semi-powerful subgroup of H given by

$$P_{2R+1}(\Phi^{m(R)}(H)) = P_{2R+1}(\Phi^{m(R)}(H_1)) \times \cdots \times P_{2R+1}(\Phi^{m(R)}(H_k)),$$

where $m(R)$ is the function (2.2) defined in Section 2.3.
By Theorem 2.6.1, $\mathrm{rk}\, G = \mathrm{rk}(G/P_{2R+1}(\Phi^{m(R)}(H)))$ and, for each $p_i \in \pi$, $\mathrm{rk}_{p_i} G = \mathrm{rk}_{p_i}(G/P_{2R+1}(\Phi^{m(R)}(H)))$. We can impose that such ranks are equal to r and r_i respectively with a first-order sentence $\varrho_{\pi,r,\mathbf{r}}$ that holds in G. Indeed, the quotient $G/P_{2R+1}(\Phi^{m(R)}(H))$ is definable and it is enough to impose that it satisfies one of the finitely many formulas defining finite groups that have order bounded by $f(r,\pi) \cdot (p_1 \cdots p_k)^{m(R)+2R}$, rank r and p_i-rank r_i for each $p_i \in \pi$.

Therefore, the sentence

$$\tilde{\sigma}_{\pi,r,\mathbf{r}} := \eta_{\pi,r} \wedge \varrho_{\pi,r,\mathbf{r}}$$

holds true in the pro-π group G if and only if G has rank r and p_i-rank r_i for each $p_i \in \pi$.

□

2.7 Finite axiomatizability of the dimension of pro-π groups

Similarly to the case of $\mathcal{C}_\pi$ groups, we define the dimension of a pro-π group G of finite rank as the k-tuple $\mathbf{d} := (d_1, \ldots, d_k)$, where each d_i is the dimension of a pro-p_i Sylow of G.

Theorem 2.7.1. *For every positive integer r and every k-tuple of natural numbers $\mathbf{d} := (d_i)_{i\in\{1,\ldots,k\}}$ with $d_i \leq r$ for each $i \in \{1,\ldots,k\}$, there is a sentence $\tilde{\delta}_{\pi,r,\mathbf{d}}$ in the language of groups $\mathcal{L}_{gp}$ such that, for every pro-π group G of rank r, the following are equivalent:*

1. *G has dimension $\mathbf{d}$,*
2. *G is a model of $\tilde{\delta}_{\pi,r,\mathbf{d}}$.*

Proof. The proof of the theorem easily follows from the discussion in Section 2.6. Indeed, we saw in the proof of Theorem 2.6.4 that G contains an open normal definable $\mathcal{C}_\pi$ subgroup H with rank $\tilde{r} \leq r$ and index $f(r,\pi)$. We can use this group to express the dimension of G.
Indeed, let $S_1, \ldots, S_k$ be Sylow pro-p_i subgroups of G with $p_i \in \pi$ and $H_i \subseteq S_i$ for each $i \in \{1,\ldots,k\}$. Then $H_i = H \cap S_i$ is open in S_i. It follows that the dimension of H_i coincides with the dimension of S_i for every i and therefore we can use the formula $\delta^{\mathrm{alt}}_{\pi,\tilde{r},\tilde{\mathbf{r}},\mathbf{d}}$ established in Theorem 2.5.3 to express the dimension of the definable $\mathcal{C}_\pi$ group H, that is the same as the dimension of G.

Precisely, if $\mathfrak{n}$ is the formula defining H and $\eta_{\pi,r}$ is the sentence expressing that H is a pronilpotent pro-π group of index bounded by $f(r,\pi)$ and rank bounded by r (see the proof of Theorem 2.6.4), the required sentence is given by

$$\tilde{\delta}_{\pi,r,\mathbf{d}} := \eta_{\pi,r} \wedge \mathrm{res}\left(\mathfrak{n}, \bigvee_{\tilde{r}\leq r}\Big(\bigvee_{\tilde{\mathbf{r}}:\max(\tilde{\mathbf{r}})_i=\tilde{r}} \delta^{\mathrm{alt}}_{\pi,\tilde{r},\tilde{\mathbf{r}},\mathbf{d}}\Big)\right).$$

□

Corollary 2.7.2. *For every positive integer r and all k-tuples of natural numbers $\mathbf{d} := (d_i)_{i\in\{1,\dots,k\}}$ and $\mathbf{r} := (r_i)_{i\in\{1,\dots,k\}}$ with $d_i \leq r$ for each $i \in \{1,\dots,k\}$ and $\max r_i = r$, there is a sentence $\widetilde{\widetilde{\delta}}_{\pi,r,\mathbf{r},\mathbf{d}}$ in the language of groups $\mathcal{L}_{gp}$ such that, for every pro-π group G, the following are equivalent:*

1. *G has dimension $\mathbf{d}$, rank r and each Sylow pro-p_i subgroup of G has rank r_i,*
2. *G is a model of $\widetilde{\widetilde{\delta}}_{\pi,r,\mathbf{r},\mathbf{d}}$.*

Proof. Take

$$\widetilde{\widetilde{\delta}}_{\pi,r,\mathbf{r},\mathbf{d}} := \tilde{\sigma}_{\pi,r,\mathbf{r}} \wedge \widetilde{\delta}_{\pi,r,\mathbf{d}},$$

where $\tilde{\sigma}_{\pi,r,\mathbf{r}}$ is like in Theorem 2.6.4. □

Remark 2.7.3. In the soluble case one does not need to rely on the classification of finite simple groups. Indeed, if G is a soluble pro-π group, one can find a definable maximal abelian normal subgroup of G, A_1, of which one can compute the dimension by using the formula for the dimension of $\mathcal{C}_\pi$ groups (since A_1 is abelian, it is in particular pronilpotent). Proceeding inductively for at most r steps, one gets a formula for the dimension of G. This is very similar to the case of soluble $\mathcal{C}_\pi$ groups treated in 2.4.3.

2.8 Quantifier complexity of the sentences expressing rank and dimension

In this section we examine the quantifier complexity of the main sentences that we produced to express the rank and the dimension of pro-π groups. Here, by quantifier complexity we mean the type of quantifiers occurring in the sentence when put in prenex form, without considering the number of variables. Recall that a formula is said to be in prenex form if it is of the form $Q : P$ where Q is a string made of concatenated quantifiers and P is a quantifier-free formula; every first-order formula can be put in prenex form ([TZ], Exercise 1.2.3). For example, the sentence $\exists a_1,\dots,a_d \forall z \exists x_1,\dots,x_d : z = [a_1,x_1]\cdots[a_d,x_d]$ is in prenex form and has quantifier complexity $\exists\forall\exists$.

We prove here that all our main sentences have quantifier complexity $\exists\forall\exists$. Hence, in particular, the quantifier complexity is independent of the set of primes π and of the rank and the dimension that are being axiomatized. For the dimension we will consider the second sentence that we produced in Section 2.5. We will note that the sentence presented in Section 2.4 has the slightly worse complexity $\exists\forall\exists\forall$. In order to establish these results, we need the following preliminary observations.

Remark 2.8.1. Let G be any group and let $H = \{g \in G \mid \varphi(g)\}$ be a definable subgroup of G, where $\varphi(x)$ is of the form $\exists \underline{z}\colon \varphi_0(x, \underline{z})$ with φ_0 quantifier-free in free variables x and $z_1, \ldots, z_m$, say. In this case we will say that H is '$\exists$-definable'. Then H is 'quantifier-neutral' in the following sense. First-order assertions about H can be translated into assertions of the same quantifier complexity about G via res, simply by expressing universal quantification over elements of H as $\forall x, \underline{z}$: $(\varphi_0(x, \underline{z}) \to \ldots)$ and existential quantification over elements of H by $\exists x, \underline{z}$: $(\varphi_0(x, \underline{z}) \wedge \ldots)$. It is easy to see that, as H is $\exists$-definable, this does not change the quantifier complexity of the formula.

Remark 2.8.2. Let G be a profinite group and let $N \subseteq_{\mathrm{c}} G$. Suppose that N is definable in G; this means that there is an $\mathcal{L}_{\mathrm{gp}}$-formula $\varphi(x)$, with a single free variable x, such that $N = \{g \in G \mid \varphi(g)\}$.

Let $B = \{b_1, \ldots, b_n\}$ be a finite group of order n, with multiplication 'table'

$$b_i b_j = b_{m(i,j)}$$

encoded by a suitable function $m\colon \{1, \ldots, n\} \times \{1, \ldots, n\} \to \{1, \ldots, n\}$.

Then the sentence

$$\exists a_1, \ldots a_n \, \forall x, y, z : \ \varphi(1) \wedge \Big((\varphi(x) \wedge \varphi(y)) \to \varphi(x^{-1}y)\Big) \wedge \Big(\varphi(x) \to \varphi(y^{-1}xy)\Big)$$
$$\wedge \left(\bigwedge_{1 \le i < j \le n} \neg\varphi(a_i^{-1}a_j)\right) \wedge \left(\bigvee_{1 \le i \le n} \varphi(a_i^{-1}y)\right) \wedge \left(\bigwedge_{1 \le i,j \le n} \varphi(a_{m(i,j)}^{-1} a_i a_j)\right)$$

can be used to express that $N \trianglelefteq G$ and $G/N \cong B$. Note that the quantifier complexity of this sentence is the same as the quantifier complexity of φ increased by $\exists\forall$. In particular, if $N \subseteq_{\mathrm{c}} G$ is an $\exists$-definable subset of G, we obtain an $\exists\forall\exists$-sentence to express that $N \trianglelefteq_{\mathrm{c}} G$ and $G/N \cong B$.

Corollary 2.8.3. *Let m be a natural number and G a $\mathcal{C}_\pi$ group. Then, first-order sentences holding true in the iterated Frattini group $\Phi^m(G)$ give rise, via* res*, to sentences in G with the same quantifier complexity. Also, first-order sentences holding true in the finite quotient $G/\Phi^m(G)$ expressing the isomorphism type of this group give rise, via* lift*, to first-order sentences holding in G of complexity $\exists\forall\exists$.*

Proof. From the discussion in Section 2.2.3, we see that each iterated Frattini subgroup $\Phi^m(G)$ is defined in the previous iterated Frattini subgroup $\Phi^{m-1}(G)$ by an existential formula ϕ_m. Then, it follows from Remark 2.8.1 that a sentence expressing a property of $\Phi^m(G)$ can be iteratively translated into sentences with the same quantifier complexity holding in the lower Frattini subgroups, up to reaching G. Regarding the quotient $G/\Phi^m(G)$, it is easy to see that $\Phi^m(G)$ is $\exists$-definable in G; this can be inferred by looking directly at the formulas in Section 2.2.3 or, equivalently, by observing that, since the formula defining $\Phi^k(G)$ in $\Phi^{k-1}(G)$ for each natural number $k \geq 1$ is existential, restricting iteratively the formula defining $\Phi^m(G)$ in $\Phi^{m-1}(G)$ up to G, one finds again an existential formula. Then the claim follows from Remark 2.8.2. □

Theorem 2.8.4. *Let r be a positive integer and $\mathbf{r} := (r_i)_{i \in \{1,\ldots,k\}}$ a tuple of natural numbers with $\max r_i = r$, for $p_i \in \pi$. Let $\tilde{\sigma}_{\pi,r,\mathbf{r}}$ be the sentence established*

in Theorem 2.6.4 that axiomatizes the property of a pro-π group of having rank r and Sylow pro-p_i rank r_i for every $p_i \in \pi$. Then $\tilde{\sigma}_{\pi,r,\mathbf{r}}$ has quantifier complexity $\exists\forall\exists$.

Proof (Sketch). Recall that in the proof of Theorem 2.6.4 we found a definable open normal $\mathcal{C}_\pi$ subgroup H of finite index bounded by a function $f(r,\pi)$ in G. In the first part of the sentence $\tilde{\sigma}_{\pi,r,\mathbf{r}}$ we imposed that H satisfies the formula $\bigvee_{\tilde{r}=1}^{r} \bigvee_{\tilde{\mathbf{r}}:\max(\tilde{\mathbf{r}})_i=\tilde{r}} \sigma_{\pi,\tilde{r},\tilde{\mathbf{r}}}$, that expresses the fact that H has rank bounded by r. Recall that $H = G^{f(r,\pi)}$ and, therefore, H is $\exists$-definable and hence quantifier-neutral by the previous Remark 2.8.1. Therefore, we just need to look at the quantifier complexity of $\bigvee_{\tilde{r}=1}^{r} \bigvee_{\tilde{\mathbf{r}}:\max(\tilde{\mathbf{r}})_i=\tilde{r}} \sigma_{\pi,\tilde{r},\tilde{\mathbf{r}}}$. The sentence $\sigma_{\pi,\tilde{r},\tilde{\mathbf{r}}}$ was established in Corollary 2.3.6. In this sentence, we first express the fact that the iterated Frattini subgroup $\Phi^m(H)$, with $m := m(r)$ (see (2.2)), is semi-powerful and has minimal number of generators bounded by r. The latter fact is ensured by the sentence $\tilde{\beta}_r$ written down in Section 2.2.3, that has complexity $\exists\forall\exists$, while the sentence pow expressing that a group is semi-powerful (that can also be found in Section 2.2.3) has complexity $\forall\exists$. Hence, the conjunction of these two sentences has complexity $\exists\forall\exists$. From Corollary 2.8.3 it follows that the resulting sentence in G has again complexity $\exists\forall\exists$. Note that, in order to talk about the iterated Frattini subgroups up to $\Phi^m(G)$, we also need the generators of all $\Phi^k(G)$ for $k \in \{0,\dots,m-1\}$ (see the discussion in Section 2.2.3), and this can be done with the sentence β_r and its restriction to quantifier-neutral subgroups, that gives a contribution of $\forall\exists$ to the complexity. Finally, again by Corollary 2.8.3, the fact that the finite group $H/\Phi^m(H)$ has rank bounded by $\tilde{r}$ has complexity $\exists\forall\exists$. To conclude the discussion for $\sigma_{\pi,\tilde{r},\tilde{\mathbf{r}}}$, we just need to examine the complexity of the sentence expressing that $H/(F \cdot H^{p_i^{2\tilde{r}(4\tilde{r}+1+m)}})$, where $F := P_{4\tilde{r}+1}(\Phi^m(H))$, has rank $\tilde{r}$. The group $F \cdot H^{p_i^{2\tilde{r}(4\tilde{r}+1+m)}}$ is $\exists$-definable in H and therefore, by Remark 2.8.2, this sentence has complexity $\exists\forall\exists$ in H, hence in G, as H is quantifier-neutral. We now examine the rest of the sentence regarding H, that states that H is a $\mathcal{C}_\pi$ group and that the finite quotient G/H has rank bounded by r and index bounded by $f(r,\pi)$. By Remark 2.8.2, the latter term of the sentence, i.e., $\mathrm{lift}(\mathfrak{n},\varpi)$, has complexity $\exists\forall\exists$. The term $\mathrm{res}(\mathfrak{n},\iota)$, expressing the isomorphism

$$H/Z(H) = \frac{H_1 \times \cdots \times H_k}{Z(H_1) \times \cdots \times Z(H_k)} \cong \prod_{i=1}^{k} \frac{\widetilde{C_H(H_i)}}{Z(H)},$$

has also quantifier complexity $\exists\forall\exists$. Indeed, taking the generators of H and of the factors H_i as parameters, the groups $Z(H)$ and $C_H(H_i)$ are quantifier-free definable in H. Therefore, also the groups

$$\widetilde{C_H(H_i)} := C_H(H_1) \cap \ldots \cap C_H(H_{i-1}) \cap C_H(H_{i+1}) \cap \ldots \cap C_H(H_k)$$

are quantifier-free definable in H and we can conclude that the quotients $H/Z(H)$ and $\frac{\widetilde{C_H(H_i)}}{Z(H)}$ are quantifier-free interpretable in H. Now ι states that

$$\frac{\widetilde{C_H(H_1)}}{Z(H)} \cdots \frac{\widetilde{C_H(H_k)}}{Z(H)} = \frac{H}{Z(H)}$$

as sets, that

$$\frac{\widetilde{C_H(H_i)}}{Z(H)} \cap \left(\frac{\widetilde{C_H(H_1)}}{Z(H)} \cdots \frac{\widetilde{C_H(H_{i-1})}}{Z(H)} \cdot \frac{\widetilde{C_H(H_{i+1})}}{Z(H)} \cdots \frac{\widetilde{C_H(H_k)}}{Z(H)} \right) = \{1\}$$

for each $i \in \{1, \dots, k\}$ and that each factor $\widetilde{C_H(H_i)}/Z(H)$ is normal in $H/Z(H)$. It is easy to see that these three properties are expressed by a $\forall\exists$-sentence. Adding the existence of the generators as parameters at the beginning of the sentence yields another existential quantifier, leading to an $\exists\forall\exists$-sentence. The last piece of the sentence expressing the properties of H states that each $Q_i := \widetilde{C_H(H_i)}/Z(H)$ is a pro-p_i group via the first-order sentence pr_i. We saw that one possible way to write pr_i is to impose that each element of Q_i is a q_i-th power, for $q_i = p_1 \cdots p_{i-1} p_{i+1} \cdots p_k$, which yields a $\forall\exists$-sentence. Again by introducing the generators as parameters, one obtains an $\exists\forall\exists$-sentence. Finally, by using the fact that $P_{2R+1}(\Phi^{m(R)}(H))$ is $\exists$-definable in H, hence in G, we can infer by Remark 2.8.2 that also the sentence $\rho_{\pi,r,\mathbf{r}}$ expressing the properties of the quotient $G/P_{2R+1}(\Phi^{m(R)}(H))$ has complexity $\exists\forall\exists$. Putting all terms together we can conclude that the sentence $\tilde{\sigma}_{\pi,r,\mathbf{r}}$ has quantifier complexity $\exists\forall\exists$, as claimed. □

Theorem 2.8.5. *Let r be a positive integer and $\mathbf{d} := (d_i)_{i\in\{1,\dots,k\}}$ a tuple of natural numbers with $d_i \leq r$, for every $i \in \{1, \dots, k\}$. Let $\tilde{\delta}_{\pi,r,\mathbf{d}}$ be the sentence established in Theorem 2.7.1 that axiomatizes the property of a pro-π group with rank r of having dimension $\mathbf{d}$. Then $\tilde{\delta}_{\pi,r,\mathbf{d}}$ has quantifier complexity $\exists\forall\exists$.*

Proof (Sketch). Recall that the sentence $\tilde{\delta}_{\pi,r,\mathbf{d}}$ has a first term $\eta_{\pi,r}$ that ensures that G has a $\mathcal{C}_\pi$ subgroup H with rank bounded by r and index bounded by a function $f(\pi, r)$ and a second term that uses the sentence $\delta^{\mathrm{alt}}_{\pi,r,\mathbf{r},\mathbf{d}}$ and that certifies that H has dimension $\mathbf{d}$. As H has finite index in G, this tuple $\mathbf{d}$ will also be the dimension of G. We already saw in the proof of Theorem 2.8.4 that H is $\exists$-definable and that the sentence $\eta_{\pi,r}$ has quantifier complexity $\exists\forall\exists$. Regarding $\delta^{\mathrm{alt}}_{\pi,r,\mathbf{r},\mathbf{d}}$, setting $F := \Phi^m(H)$ with $m = m(r)$ as in (2.2), we want to express, for each $p_i \in \pi$, properties of the quotient $F/F^{p_i}[F, F]$ and of the set $\{g \in F \mid g^{p_i} = 1\}$. First, recall from the proof of Corollary 2.8.3 that F is $\exists$-definable in H and that, in order to talk about its properties we also need the generators of all $\Phi^k(H)$ for $k \in \{0, \dots, m-1\}$. This can be done by using the sentence β_r and its restriction to quantifier-neutral subgroups, that brings a contribution of $\forall\exists$ to the complexity. Once all these generators are given as parameters, $F^{p_i}[F, F]$ is $\exists$-definable in F, hence in H. Therefore, by Remark 2.8.2, the sentence expressing that $F/F^{p_i}[F, F]$ has a certain isomorphism type (hence a certain minimal number of generators $\mathrm{d}(F_i)$) has complexity $\exists\forall\exists$. Finally, expressing that the set $\{g \in F \mid g^{p_i} = 1\}$ has a prescribed cardinality $\mathrm{d}(T_i)$ requires an $\exists\forall$-formula. It follows that the overall sentence satisfied by F has $\exists\forall\exists$ quantifier complexity. Since F is $\exists$-definable in H and H is $\exists$-definable in G, hence quantifier-neutral (Remark 2.8.1), also the overall sentence satisfied by G has $\exists\forall\exists$ quantifier complexity. □

Corollary 2.8.6. *Let r be a positive integer, $\mathbf{r} := (r_i)_{i\in\{1,\dots,k\}}$ a tuple of natural numbers with $\max r_i = r$ and $\mathbf{d} := (d_i)_{i\in\{1,\dots,k\}}$ a tuple of natural numbers with $d_i \leq r$ for every $i \in \{1, \dots, k\}$. Let $\widetilde{\tilde{\delta}}_{\pi,r,\mathbf{r},\mathbf{d}}$ be the sentence established in Corollary*

2.7.2 that axiomatizes the property of a pro-π group of having rank r, Sylow pro-p_i rank r_i for every $p_i \in \pi$ and dimension $\mathbf{d}$. Then $\widetilde{\widetilde{\delta}}_{\pi,r,\mathbf{r},\mathbf{d}}$ has quantifier complexity $\exists\forall\exists$.

Proof. The sentence $\widetilde{\widetilde{\delta}}_{\pi,r,\mathbf{r},\mathbf{d}}$ is given by the conjunction

$$\tilde{\sigma}_{\pi,r,\mathbf{r}} \wedge \widetilde{\delta}_{\pi,r,\mathbf{d}}.$$

Since, by the previous theorems, both $\tilde{\sigma}_{\pi,r,\mathbf{r}}$ and $\widetilde{\delta}_{\pi,r,\mathbf{d}}$ have quantifier complexity $\exists\forall\exists$, also $\widetilde{\widetilde{\delta}}_{\pi,r,\mathbf{r},\mathbf{d}}$ has the same quantifier complexity. □

We conclude this section by observing that the sentence expressing the dimension introduced in Section 2.4 has quantifier complexity $\forall\exists\forall\exists$.

Proposition 2.8.7. *Let r be a positive integer and $\mathbf{d} := (d_i)_{i\in\{1,\dots,k\}}$ a tuple of natural numbers with $d_i \leq r$ for all $i \in \{1,\dots,k\}$. The sentence $\delta_{\pi,r,\mathbf{d}}$ expressing that a $\mathcal{C}_\pi$ group G of rank r has dimension $\mathbf{d}$ has quantifier complexity $\forall\exists\forall\exists$.*

In particular, if we were to use this sentence in place of $\delta^{\mathrm{alt}}_{\pi,\tilde{r},\tilde{\mathbf{r}},\mathbf{d}}$ to build the sentence $\widetilde{\delta}_{\pi,r,\mathbf{d}}$ holding for pro-π groups, we would get the worse complexity $\forall\exists\forall\exists$.

We will not prove this proposition. We just point out that, carrying out an analysis similar to the ones above, one finds that the sentences $(\delta^{\mathrm{s}}_{\mathbf{d}_1} \wedge \delta^{\mathrm{q}}_{\mathbf{d}_2})$ from Section 2.4 have complexity $\exists\forall\exists$. Since

$$\begin{aligned}\delta_{\pi,r,\mathbf{d}} :=& \exists h_1,\dots,h_r : \bigvee_{\mathbf{d}_1+\mathbf{d}_2=\mathbf{d}} \left(\delta^{\mathrm{s}}_{\mathbf{d}_1}(h_1,\dots,h_r) \wedge \delta^{\mathrm{q}}_{\mathbf{d}_2}(h_1,\dots,h_r)\right) \\ &\wedge \neg\exists h_1,\dots,h_r : \bigvee_{\substack{\mathbf{m}\in\{0,\dots,r\}^k \\ \mathbf{m}\neq(0,\dots,0)}} \left(\bigvee_{\mathbf{d}_1+\mathbf{d}_2=\mathbf{d}+\mathbf{m}} (\delta^{\mathrm{s}}_{\mathbf{d}_1}(h_1,\dots,h_r) \wedge \delta^{\mathrm{q}}_{\mathbf{d}_2}(h_1,\dots,h_r))\right),\end{aligned}$$

the negation in the second half of the sentence produces a string of quantifiers $\forall\exists\forall$, leading to the overall quantifier complexity $\forall\exists\forall\exists$.

2.9 Some open questions

We list here a few open questions that arise naturally from the work presented in this thesis.

From a purely group-theoretic point of view, we saw in Theorem 2.3.1 that, given a pro-p group G of rank r and F an open normal powerful subgroup of G, the quotient $G/P_{2r+1}(F)$ (dependent on r) has the same rank as G. A natural question arising from this is:

Question 2.9.1. *Is it possible to find a quotient of G that does not depend on* $\mathrm{rk}(G)$ *and has rank* $\mathrm{rk}(G)$*?*

Ideally, the quotient $G/P_2(F)$ could be a candidate, but the arguments used in the proof of Theorem 2.3.1 do not hold in this case (see Example 2.3.3, 2.). More generally, one might try to prove that the result holds for $\mathrm{rk}(G) = \mathrm{rk}(G/P_c(F))$ with c independent of the rank of G.

In another direction, regarding definability, the next step would be to investigate the finite axiomatizability of the dimension of R-analytic groups, where R is a pro-p ring (see [DDMS], Chapter 13).
Also, we have already observed that it is not possible to express that a pro-p group has finite (unbounded) rank by Feferman and Vaught's result (Proposition 2.2.12). A possible question would then be the following.

Question 2.9.2. *Is it possible to find a class of pro-p groups where the property of having finite (unbounded) rank is finitely axiomatizable?*

We already noticed at the end of Section 2.2.4 that one might try to consider the class of d-generated pro-p groups, where d is a fixed positive integer, to begin with.

Finally, one could consider the Hirsch length of polycyclic groups, that behaves as some sort of dimension for these groups, and investigate whether this is a first-order definable invariant.

2.10 List of main formulas

α: group is abelian; Section 2.4.1

β_d^*: minimal number of generators of a $\mathcal{C}_\pi$ group is d; Section 2.2.3

$\tilde{\beta}_d$: minimal number of generators of a $\mathcal{C}_\pi$ group is $\leq d$; Section 2.2.3

$\text{bound}_{\mathbf{d}}$: $x^{p_1^{f(d_1)}\cdots p_k^{f(d_k)}} = 1$; Section 2.4.2

$\gamma_{p,s}$: direct product of s copies of the cyclic group C_p; Section 2.4.1

$\delta_{\pi,r,\mathbf{d}}$: $\mathcal{C}_\pi$ group of rank r has dimension $\mathbf{d}$; Section 2.4.2

$\overline{\delta}_{\pi,r,\mathbf{r},\mathbf{d}}$: $\mathcal{C}_\pi$ group that has rank r, dimension $\mathbf{d}$ and p_i-ranks r_i; Section 2.4.2

$\delta^{\text{alt}}_{\pi,r,\mathbf{r},\mathbf{d}}$: alternative sentence for $\mathcal{C}_\pi$ group that has rank r, dimension $\mathbf{d}$ and p_i-ranks r_i; Section 2.5

$\tilde{\delta}_{\pi,r,\mathbf{d}}$: pro-$\pi$ group of rank r has dimension $\mathbf{d}$; Section 2.7

$\widetilde{\overline{\delta}}_{\pi,r,\mathbf{r},\mathbf{d}}$: pro-$\pi$ group that has dimension $\mathbf{d}$, rank r and p_i-ranks r_i; Section 2.7

$\delta^{\text{ab}}_{\pi,r,\mathbf{d}}$: abelian $\mathcal{C}_\pi$ group has rank r and dimension $\mathbf{d}$; Section 2.4.1

$\tilde{\delta}^{\text{ab}}_{\pi,r,\mathbf{d}}$: $\mathcal{C}_\pi$ group that is abelian, has rank r and dimension $\mathbf{d}$; Section 2.4.1

$\delta^{\text{j.i.}}_{\pi,r,\mathbf{d}}$: $\mathcal{C}_\pi$ group of rank r with non-soluble just-infinite p_i-adic analytic pro-p_i factors has dimension $\mathbf{d}$; Section 2.4.3

$\overline{\delta}^{\text{j.i.}}_{\pi,r,\mathbf{r},\mathbf{d}}$: $\mathcal{C}_\pi$ group with non-soluble just-infinite p_i-adic analytic pro-p_i factors has rank r, dimension $\mathbf{d}$ and p_i-ranks r_i; Section 2.4.3

$\delta^{\text{sim}}_{\pi,r,\mathbf{d}}$: $\mathcal{C}_\pi$ group of rank r satisfying $(\star)_\upsilon$ and whose factors have non-abelian simple Lie algebra has dimension $\mathbf{d}$; Section 2.4.3

$\overline{\delta}^{\text{sim}}_{\pi,r,\mathbf{r},\mathbf{d}}$: $\mathcal{C}_\pi$ group satisfying $(\star)_\upsilon$ and whose factors have non-abelian simple Lie algebra that has rank r, dimension $\mathbf{d}$ and p_i-ranks r_i; Section 2.4.3

$\delta^{\text{sol}}_{\pi,r,\mathbf{d}}$: soluble $\mathcal{C}_\pi$ group of rank r has dimension $\mathbf{d}$; Section 2.4.3

$\overline{\delta}^{\text{sol}}_{\pi,r,\mathbf{r},\mathbf{d}}$: soluble $\mathcal{C}_\pi$ group that has rank r, dimension $\mathbf{d}$ and p_i-ranks r_i; Section 2.4.3

ϕ^G_m: (iterated) Frattini subgroup $\Phi^m(G)$ of a $\mathcal{C}_\pi$ group G; Section 2.2.3

μ: maximality of dimension of abelian subgroup; Section 2.4.2

π^F_i: i^{th} term of the lower $q(\pi)$-series of a definable semi-powerful group F; Section 2.2.3

pow: (semi)powerful group; Section 2.2.3

$s(\kappa)$: set defined by κ is a subgroup; Section 2.2.1

$s_\triangleleft(\kappa)$: set defined by κ is a normal subgroup; Section 2.2.1

$\sigma_{\pi,r,\mathbf{r}}$: $\mathcal{C}_\pi$ group has rank r and p_i-ranks r_i; Section 2.3

$\tilde{\sigma}_{\pi,r,\mathbf{r}}$: pro-$\pi$ group has rank r and p_i-ranks r_i; Section 2.6

$\zeta(a,x)$: a and x commute; Section 2.4.2

Chapter 3

The unique product property for pro-p groups

3.1 Introduction

The unique product property is a combinatorial property related to the Kaplansky conjecture on zero divisors in group rings. This conjecture states that, if G is a torsion-free group and K is a field, then the group ring $K[G]$ has no non-trivial zero divisors. According to [G] and page 112 in [S], the zero divisor conjecture was formulated by Higman in his thesis in 1940 and appeared in written form in the report of a talk given by Kaplansky in 1956, whence the common attribution to Kaplansky. The zero divisor conjecture is related to two further conjectures on group rings, namely the unit conjecture and the idempotent conjecture. Given a field K and a torsion-free group G, the unit conjecture states that every unit in $K[G]$ is of the form λg, where $\lambda \in K \setminus \{0\}$ and $g \in G$, while the idempotent conjecture states that the only idempotents in $K[G]$ are 0 and 1. The basic relation between these three conjectures is the following:

$$\text{Unit conjecture} \Rightarrow \text{Zero divisor conjecture} \Rightarrow \text{Idempotent conjecture.}$$

The unit conjecture was disproved by Gardam in 2021 ([G]), while the zero divisor conjecture and the idempotent conjecture are still open. The zero divisor conjecture is known to be true for important classes of groups, such as: torsion-free abelian groups, free groups, torsion-free abelian-by-finite groups and elementary amenable groups. However, for some of these classes, such as for elementary amenable groups, the proof of the conjecture relies on ring-theoretic and K-theoretic machinery and it would therefore also in these cases be desirable to find a more direct group-theoretic or combinatorial proof.

It is easily seen that a group possessing the unique product property satisfies the zero divisor conjecture but it is known that the converse does not hold true (for instance by an example given by Promislow; [P]). In the realm of pro-p groups little is known regarding the unique product property, but the following result, proved by ring-theoretic means, holds true.

Theorem 1 (Farkas, Linnell; [FL])**.** *If G is a uniform pro-p group and K is a field of characteristic 0 or p, then $K[G]$ has no non-trivial zero-divisors.*

In light of the evidence provided by this result, Craig and Linnell formulated the following

Conjecture 2 (Craig, Linnell; [CL])**.** *Every uniform pro-p group has the unique product property.*

In the direction of proving this conjecture they show:

Theorem 3 (Craig, Linnell; [CL])**.** *A virtually soluble subgroup of a uniform pro-p group has the unique product property.*

In order to prove this result, they use properties of uniform pro-p groups and of linear groups to show that virtually soluble subgroups of uniform pro-p groups are torsion-free nilpotent-by-torsion-free abelian. In this way they actually show that these groups are right-orderable (see Section 3.2.2), a stronger property than the unique product property.

In this chapter we consider a larger class of pro-p groups, namely *saturable* pro-p groups (see Section 3.3) and we prove the following result (compare with Corollary 3.3.7):

Theorem 4. *A virtually soluble subgroup of a saturable pro-p group is right-orderable and therefore has the unique product property.*

Our proof uses Lie-theoretic methods and therefore provides not only a generalisation but also a different proof of Craig and Linnell's result.

We then proceed to investigate the related property of orderability in the realm of pro-p groups, finding both, classes of orderable and not orderable pro-p groups. As for non bi-orderable pro-p groups, it is easily seen that compact p-adic Chevalley groups cannot be bi-ordered (see the beginning of Section 3.4). It is then natural to ask what happens in general. In this respect we show (see Corollary 3.4.5):

Theorem 5. *Let G be a non-soluble p-adic analytic pro-p group. Then G is not bi-orderable.*

In order to prove this theorem we need to establish first another result, that is interesting on its own, which states that every non-trivial normal subsemigroup of a just-infinite insoluble pro-p group G is an open normal subgroup of G (Proposition 3.4.1).

In contrast, adapting the proof that abstract RAAGs are bi-orderable to the pro-p case, we find a large class of pro-p groups that are bi-orderable (see Section 3.5):

Theorem 6. *Pro-p RAAGs are bi-orderable.*

On the way, by using Theorem 3.1, we give some examples of subsets of uniform subgroups of pro-p Chevalley groups that display the unique product property (Example 3.3.20) and we try to relate the fact that a pro-p group is locally indicable to other properties of the group (compare with Corollary 3.3.16). In particular, in the case of metabelian profinite groups we obtain (see Corollary 3.3.19):

Theorem 7. *Let G be a metabelian profinite group with the ascending chain condition on closed subgroups. Then the following are equivalent:*

1. *G is torsion-free and, for every $H \leq_c G$, the abelianisation H/H' is infinite;*
2. *G is locally indicable.*

Also the questions and the formula contained in Sections 7 and 8 are original. Smaller new insights are collected in the following results and examples. Example 3.2.4 of a torsion-free profinite group that does not possess the unique product property is easily found by using Promislow's example. Lemma 3.2.24 and Corollary 3.2.27 show that extensions of groups with a locally invariant order have a locally invariant order (the result is probably known but a suitable reference for it was not found), from which one can easily deduce Example 3.2.28 of a profinite group with a locally invariant order. Finally, Remarks 3.2.20 and 3.2.23 in Section 2 and Example 3.3.3 in Section 3 are also new.

The organisation of the chapter is as follows. In Section 3.2 preliminaries on the unique product property and orderability of groups are presented. The main result on the right-orderability of virtually soluble subgroups of saturable pro-p groups can be found in Section 3.3, together with a characterisation of groups with the property that every closed subgroup has infinite abelianisation within the class of torsion-free soluble pro-p groups of finite rank. In Section 3.4 it is proved that insoluble pro-p groups of finite rank are not bi-orderable, while in Section 3.5 the bi-orderability of pro-p RAAGs is proven. Finally, in Section 3.6 some further open questions and lines of investigation are described and in Appendix 3.7 a commutator formula is proved.

3.2 Preliminaries

3.2.1 The unique product property

Definition 3.2.1. We say that a group G has the unique product property (UP for short) if, given two non-empty, finite subsets A and B of G, there always exists at least one element g of G that can be written in a unique way as a product $g = ab$ with $a \in A$ and $b \in B$.
If G satisfies UP we say that G is a unique product group (UPG for short).

It follows immediately from the definition that a group with the unique product property is torsion-free; indeed, if $g \in G \setminus \{1\}$ is a torsion element of order n, then the set $\{1, g, \dots, g^{n-1}\}$ contradicts the unique product property: every element of this set can be written in $n \geq 2$ ways as the product of two elements from the set itself.

Example 3.2.2. The group $\mathbb{Z}$ has the unique product property; indeed, if $\emptyset \neq A, B \subseteq \mathbb{Z}$ are finite and if a is the maximal element of A and b is the maximal element of B, then $a+b$ is greater than any other element in $A+B$. More generally, every ordered group has the unique product property (see Section 3.2.2).

Unique product groups were introduced in [RS] in relation to the Kaplansky conjecture regarding zero divisors in group rings. The conjecture predicts that, if K is a field and G is a torsion-free group, then the group ring $K[G]$ has no

non-trivial zero divisors; this conjecture is still open. Note that, by considering the quotient field of an integral domain, it is equivalent to state this conjecture for K an integral domain instead of a field.
Some classes of torsion-free groups which are known to satisfy the zero divisor conjecture are: free groups and torsion-free abelian groups (more generally orderable groups, see Section 3.2.2), groups with a locally invariant order (see Section 3.2.2) and torsion-free abelian-by-finite groups (see [Li]).
Indeed, it is not difficult to see that if G has the unique product property, then $R[G]$ has no zero divisors: let $x := r_1g_1 + ... + r_ng_n$ and $y := r'_1g'_1 + ... + r'_mg'_m$ be two non-zero elements in $R[G]$, each written as an R-linear combination of distinct elements of G with non-zero coefficients r_i, r'_j, and consider the finite non empty subsets of G given by $A := \{g_1, \dots, g_n\}$ and $B := \{g'_1, \dots, g'_m\}$. By the UP there exists an element in G, without loss of generality $g := g_1g'_1$, that can be written uniquely as the product of an element in A and an element in B. Hence $g_ig'_j \neq g_1g'_1$ for every $(i,j) \neq (1,1)$ and $xy = r_1r'_1(g_1g'_1) + r_1r'_2(g_1g'_2) + \dots \neq 0$.

However, the class of groups G such that $R[G]$ has no zero divisors is strictly larger than the class of groups which have the unique product property, as shown by the following example, given by Promislow in 1988 (see [P]).

Example 3.2.3. Let G_2 be the crystallographic group given by the presentation

$$\langle x, y : x^{-1}y^2x = y^{-2}, y^{-1}x^2y = x^{-2}\rangle.$$

It can be shown that G_2 is torsion-free and abelian-by-finite and therefore $R[G]$ does not have any zero divisors, whenever R is an integral domain; see [Li]. Indeed, the group G_2 is a non-split extension of $\mathbb{Z}^3$ by the finite group $C_2 \times C_2$. More precisely, setting $z := xy$, we see that $N := \langle x^2, y^2, z^2\rangle$ is a normal subgroup of G_2 which is free abelian of rank 3; the quotient G_2/N is isomorphic to $C_2 \times C_2$ (see [F] for more details about crystallographic groups).

In his paper, Promislow explicitly constructs a non-empty finite set A with fourteen elements such that there is no unique product in $A \cdot A$.

It is interesting to note that this group was used to give a counterexample to the units conjecture in [G]. By using Example 3.2.3, we can easily produce an example of a profinite group satisfying the zero divisor conjecture, but without the unique product property.

Example 3.2.4. We consider $\widehat{G_2}$, the profinite completion of G_2. Let $\overline{N}$ be the closure of the group N introduced in the previous example in $\widehat{G_2}$. As N has finite index in G_2, $\overline{N} \cong \widehat{N} \cong \widehat{\mathbb{Z}^3}$ (see Proposition 3.1.24 in [Wil]) and $\widehat{G_2}/\overline{N} \cong G_2/N \cong C_2 \times C_2$. We note that, since G_2 is torsion-free and finitely generated abelian-by-nilpotent, by Theorem 2.4 in [KW] its profinite completion is torsion-free. Therefore, $\widehat{G_2}$ is torsion-free abelian-by-finite.
Moreover, since G_2 is residually finite, it injects into $\widehat{G_2}$; thus, $\widehat{G_2}$ gives an example of a torsion-free profinite group without the unique product property. However, being torsion-free abelian-by-finite, $\widehat{G_2}$ does satisfy the zero divisor conjecture.

The first example of a torsion-free group without the unique product property was given in 1985 by Rips and Segev in [RiSe]. In 2014, Carter ([Ca]) gave new

examples of torsion-free groups that satisfy the zero divisor conjecture but do not possess the unique product property. More precisely, for each positive integer k, these groups are given by

$$P_k := \langle a, b \mid ab^{2^k}a^{-1}b^{2^k}, ba^2b^{-1}a^2 \rangle.$$

The group P_1 is the same as Promislow's group. However, Carter proves that, for every $k > 1$, the group P_k does not contain P_1 ([Ca], Theorem 3.6). Moreover, he proves that each P_k contains arbitrarily large non-unique product sets ([Ca], Theorem 1.5). More recently, in [CL] Craig and Linnell generalised Promislow's example in another direction. Namely, for each natural number n, they define the combinatorial generalized Hantzsche-Wendt group G_n as

$$G_n := \langle x_1, \ldots, x_n \mid x_i^{-1}x_j^2x_ix_j^2 \text{ for all } i \neq j \rangle.$$

Note that G_2 is the same group used in Promislow's example. Craig and Linnell prove that each G_n for $n \geq 1$ satisfies the zero divisor conjecture. However, for $n \geq 2$, each group G_n does not have the unique product property as it contains a copy of G_2.

Next we list some other properties of unique product groups. The following theorem, due to Strojnowski, states that the unique product property for a group G can be verified by considering products in product sets of the form $A \cdot A$, where A is a non-empty finite set of G. Moreover, it states that the seemingly stronger property of having two elements that can be expressed as a unique product is actually equivalent to the unique product property.

Theorem 3.2.5 (Strojnowski; [S])**.** *Let G be a group. The following are equivalent:*

1. *G has the unique product property;*
2. *For every non-empty finite subset A of G there exists (at least) one element $g \in G$ that can be written uniquely as a product $g = xy$ with $x, y \in A$;*
3. *Given any two non-empty finite subsets A and B of G with $|A| + |B| \geq 3$, there exist at least two elements of G which can be written in a unique way as the product of an element in A and an element in B.*

The following results, recalled in [CL], state that the unique product property is closed under some standard group theoretic constructions.

Theorem 3.2.6 (Strojnowski; [S], Theorem 2)**.** *Every free product of groups with the unique product property has the unique product property.*

Proposition 3.2.7 (Rudin, Schneider; [RS], Theorem 6.1)**.** *The unique product property is closed under extensions, i.e., given a group G and $N \triangleleft G$, if N and G/N have the unique product property, then G has the unique product property.*

Remark 3.2.8. The unique product property is a local property, i.e., a group G is a unique product group if and only if all the finitely generated subgroups of G are unique product groups. This is clear since the definition of unique product property involves only finite sets.

Corollary 3.2.9 (Compare with [CL], Introduction)**.** *Let G be a group having a subnormal series*

$$1 = G_0 \triangleleft G_1 \triangleleft \ldots \triangleleft G_n = G$$

such that every quotient G_{i+1}/G_i is torsion-free abelian.
Then G is a unique product group.

Proof. First of all we show that every torsion-free abelian group is a unique product group. By the structure theorem of finitely generated abelian groups, every finitely generated torsion-free abelian group is the direct product of finitely many copies of $\mathbb{Z}$ and we already noted that $\mathbb{Z}$ has the unique product property. For every natural number r, $H = \mathbb{Z}^r$ has a subnormal series of the form

$$1 = H_0 \triangleleft H_1 \triangleleft \ldots \triangleleft H_r = H$$

with $H_i \cong \mathbb{Z}^i$ and $H_i/H_{i-1} \cong \mathbb{Z}$ for all $i \in \{1, \ldots, r\}$. Using Proposition 3.2.7 inductively one obtains that $\mathbb{Z}^r$ has the unique product property.
Since the unique product property is a local property (Remark 3.2.8), it follows that every torsion-free abelian group is a unique product group.
Finally, if G has a subnormal series

$$1 = G_0 \triangleleft G_1 \triangleleft \ldots \triangleleft G_n = G$$

with all the quotients torsion-free abelian, it suffices to apply inductively Proposition 3.2.7. □

Remark 3.2.10. From the previous corollary we obtain in particular that every torsion-free abelian group has the unique product property and, in particular, $\mathbb{Z}^r$ and the free abelian pro-p group $\mathbb{Z}_p^r$ are unique product groups for every integer $r \geq 1$.
Moreover, the proof above works for every subnormal series in which the quotients possess the unique product property.

In [CL], Craig and Linnell conjectured that every uniform pro-p group G is a unique product group. This conjecture can be motivated by the fact that, if G is a uniform pro-p group, then $K[G]$ has no zero divisors for all fields K of characteristic 0 or p (see [FL]). Moreover, they remark that the crystallographic group G_2, that is known to be a non-unique product group (see Example 3.2.3), cannot be embedded in a uniform pro-p group: this follows from the fact that a virtually abelian subgroup of a uniform pro-p group is abelian ([CL], Theorem 2.4) and G_2 is virtually abelian but not abelian.
As a step towards proving this conjecture, Craig and Linnell show that, if H is a virtually soluble subgroup of a uniform pro-p group G, then H is a unique product group. In Section 3.3 we give a different proof of a somewhat more general result, namely that if H is a virtually soluble subgroup of a saturable pro-p group, then H is a unique product group (see Corollary 3.3.7).

3.2.2 Orderability and the unique product property

The unique product property is implied by some other group-theoretical properties related to the notion of orderability (see for example [BMR], the first chapters

of [DNR] or of [CR] for more on this topic). Recall that a *strict order* on a set X is a binary relation $<$ that is transitive (i.e., for all $x, y, z \in X$, $x < y$ and $y < z$ imply $x < z$) and irreflexive (i.e., for all $x \in X$, $x \not< x$). These two properties imply asymmetry, i.e., for all $x, y \in X$, if $x < y$ then $y \not< x$. From a strict order $<$ one can obtain a non-strict order $\leq$ by setting $x \leq y$ if and only if $x < y$ or $x = y$; such an order is a binary relation that is transitive, reflexive (i.e., for every $x \in X$, $x \leq x$) and antisymmetric (i.e., if $x, y \in X$ with $x \leq y$ and $y \leq x$, then $x = y$). Conversely, from a non-strict order $\leq$ one obtains a strict order $<$ by setting $x < y$ if and only if $x \leq y$ and $x \neq y$. Therefore we can speak without distinction of strict and non-strict orders. Finally, a strict (respectively non-strict) total order is a strict (respectively non-strict) order relation in which any two distinct elements (respectively any two elements) are comparable.

Definition 3.2.11. A *right-order* on a group G is a total order $\leq$ on G such that, if x, y are elements in G with $x \leq y$, then, for every $z \in G$, $xz \leq yz$. Similarly, a *left-order* on G is a total order $\leq$ such that, if $x \leq y$, then $zx \leq zy$ for every $z \in G$. A *bi-order* on G is a total order which is both a left- and a right-order. We say that a group is *(bi-)orderable* (respectively *right-orderable*, *left-orderable*) if it admits a bi-order (respectively right-order, left-order).

Note that a group G is right-orderable if and only if it is left-orderable. Indeed, let $\leq$ be a right-order (respectively left-order) on G and consider the order $\leq'$ defined by $x \leq' y$ if and only if $x^{-1} \geq y^{-1}$. Then $\leq'$ is a left-order (respectively right-order) on G. In light of this remark from now on we will consider only right-orders.

To give a right-order on a group G is equivalent to giving a subset P of G that is closed under multiplication and such that, for every $g \in G$ with $g \neq 1$, either $g \in P$ or $g^{-1} \in P$. Indeed, given a right-order $<$ we can take for P the set of positive elements $\{x \in G \mid 1 < x\}$ and, conversely, given such a set P, we can define on G the right-order given by $g < h$ if and only if $hg^{-1} \in P$. Note that P is a semigroup, called the *positive cone* of the associated order $<$.
The positive cone of a bi-order has these same properties and, in addition, it must be closed under conjugation by elements of G, i.e., it must be a normal subsemigroup of G.
It follows that to ask whether a group G admits a (right-)order is equivalent to asking whether G has subsemigroups with the properties mentioned above.

Remark 3.2.12. A group G with a right-order is torsion-free.

Proof. Let $g \in G$, $g \neq 1$. If $g > 1$, then $g^n > \ldots > g^2 > g > 1$ for every positive integer n. Similarly, if $g < 1$, then $g^n < \ldots < g^2 < g < 1$ for every n. □

Example 3.2.13. Some examples of bi-orderable groups are: torsion-free abelian groups, torsion-free nilpotent groups and free groups (see [DNR], Section 1.2). In particular, since the principal congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$ of level greater than 2 are free, they are bi-orderable. However, a result of Morris-Witte establishes that finite-index subgroups of $\mathrm{SL}_d(\mathbb{Z})$ for $d \geq 3$ are not right-orderable (see [DNR], Theorem 3.5.1). It follows that principal congruence subgroups of the p-adic analytic group $\mathrm{SL}_d(\mathbb{Z}_p)$ for $d \geq 3$ are not right-orderable.

We remark that a bi-orderable group has the unique product property: given two finite non-empty subsets A and B of G, the maximal element of A multiplied by the maximal element of B will have a unique representation. However, the converse is not true in general (see [KRD]).

Remark 3.2.14. Since the crystallographic group G_2 does not have the unique product property (see Example 3.2.3), it cannot admit a bi-order. However, we can also show this directly: if $\leq$ is a bi-order on G_2, then $y^{-2} = x^{-1}y^2x > 1$ if and only if $y^2 > 1$ if and only if $y^{-2} < 1$.

Note that, with a slightly more complicated argument, one can also prove that right-orderable groups have the unique product property (see [DNR], Section 1.4.3).

We now consider what happens for extensions of right-orderable groups.

Lemma 3.2.15. *Let G be an extension of N by K with N and K right-orderable groups. Then G is right-orderable.*

Proof. We fix right-orders $\leq_N$ and $\leq_K$ on N and K respectively. Let $i : N \to G$ and $p : G \to K$ be the two homomorphisms that come with the extension. For defining an order $\leq$ on G we remark that G is the disjoint union of the right-cosets of N in G; hence we define a sort of lexicographic order on G taking as a primary parameter the image of an element under p and as a secondary parameter the "N-part" of an element.[1]

Namely, let x, y be two distinct elements of G. We distinguish two cases:

1. $p(x) \neq p(y)$: in this case we set $x > y$ if $p(x) >_K p(y)$ in K;
2. $p(x) = p(y)$: this means that $xy^{-1} \in \mathrm{Ker}(p) = \mathrm{Im}(i)$, so there exists an element $n \in N$ such that $i(n) = xy^{-1}$. Moreover, n is the unique element of N with this property since i is injective. In this case we set $x \geq y$ if $n \geq_N 1_N$ in N.

The relation $\leq$ just defined is a (total) order.
It is clearly reflexive.
It is antisymmetric: let x and y be elements of G with $x \geq y$ and $y \geq x$. There are two possibilities: if $p(x) \neq p(y)$ this means that $p(x) \geq_K p(y)$ and $p(y) \geq_K p(x)$ in K, which would imply $p(x) = p(y)$ since $\leq_K$ is an order in K and this would contradict the hypothesis. Hence, $p(x) = p(y)$; let $n \in N$ such that $i(n) = xy^{-1}$. Then we have $n \geq_N 1_N$ and $n \leq_N 1_N$, thus $n = 1_N$ because $\geq_N$ is antisymmetric; it follows that $xy^{-1} = i(n) = 1_G$, i.e., $x = y$.
Finally, $\leq$ is transitive. Let x, y, z be elements of G such that $x \leq y$ and $y \leq z$. We have to distinguish several cases:

1. $p(x) \neq p(y)$ and $p(x) \leq_K p(y)$.
   - $p(y) = p(z)$, in which case $p(x) \neq p(z)$ and $p(x) \leq_K p(y) = p(z)$, so $x \leq z$.

[1] In [C], 3.7, Conrad defines the same order on G by defining the positive cone of the order; namely, $g \in G$, $g \neq 1$ is defined to be positive either if $g \in N$ and $g >_N 1_N$ or $g \in G \setminus N$ and $p(g) >_K 1_K$. This automatically defines a right-order.

- $p(y) \neq p(z)$ and $p(y) \leq_K p(z)$, from which $p(x) \leq_K p(y) \leq_K p(z)$ that implies $p(x) \leq_K p(z)$ by transitivity of $\leq_K$. Since $p(x) \neq p(y)$ by hypothesis, $p(x) \neq p(z)$ (otherwise we would have that $p(x) = p(y)$); hence we can conclude that $x \leq z$.

2. $p(x) = p(y)$ and $n_1 \leq_N 1_N$, where $i(n_1) = xy^{-1}$.

   - $p(y) = p(z)$ and $n_2 \leq 1_N$, where $i(n_2) = yz^{-1}$.
     Let $n_3 \in N$ such that $i(n_3) = xz^{-1}$; we want to show that $n_3 \leq_N 1_N$.
     Since $i(n_1 n_2) = xy^{-1}yz^{-1} = xz^{-1}$ and i is injective, $n_3 = n_1 n_2$.
     Since $\leq_N$ is a right-order on N, we have: $n_3 = n_1 n_2 \leq_N n_2 \leq_N 1_N$, from which $n_3 \leq_N 1_N$ by transitivity of $\leq_N$.
   - $p(y) \neq p(z)$ and $p(y) \leq_K p(z)$. In this case $p(x) \neq p(z)$ and $p(x) = p(y) \leq_K p(z)$, so $x \leq z$.

We now show that $\leq$ is a right-order.
Let x, y be elements of G with $x \leq y$ and let z be another element of G.
There are two cases: if $p(x) \neq p(y)$ then $p(xz) \neq p(yz)$, $p(x) \leq_K p(y)$ and $p(xz) = p(x)p(z) \leq_K p(y)p(z) = p(yz)$ because $\leq_K$ is a right-order. If $p(x) = p(y)$, then $p(xz) = p(yz)$, and, if $i(n) = xy^{-1}$, then $n \leq_N 1_N$. Since $i(n) = xy^{-1} = xzz^{-1}y^{-1}$ this also shows that $xz \leq yz$. □

Remark 3.2.16. In Example 1 of Section 5 of [C], Conrad notes that the extension of two bi-ordered groups need not be a bi-ordered group; in this example he considers the group

$$G := \langle x, y \mid x^y = x^{-1} \rangle.$$

The group G can be written as the non-abelian semidirect product $\langle y \rangle \ltimes \langle x \rangle \cong \mathbb{Z} \ltimes \mathbb{Z}$. The right-order induced on $\mathbb{Z} \ltimes \mathbb{Z}$ by the canonical order on $\mathbb{Z}$ is the lexicographic order and G inherits a right-order via the above isomorphism. However, G is not bi-orderable because $x^y = x^{-1}$, from which it follows that, in a given bi-order on G, the element x can be neither positive nor negative.

In general, given an extension $1 \to H \to G \to K \to 1$ where H and K are bi-ordered, the procedure used in the proof of Lemma 3.2.15 gives a bi-order on G if and only if the conjugation action of G on H preserves the order on H.

More generally, the orderability of the quotients of a group is related to the notion of convex subgroups.

Definition 3.2.17. Let G be a group with a right-order $\leq$. A subset C of G is said to be *convex* with respect to $\leq$ if, given any x, y in C and z in G, the inequalities $x < z < y$ imply $z \in C$. A subset C of G is said to be *relatively convex* if there exists a right-order with respect to which C is convex.

Note that for proving that a subgroup C is convex in G with respect to a certain right-order $\leq$ it is enough to prove that, for every $h \in C$ and every $g \in G$, if $1 < g < h$, then $g \in C$.

Convex subgroups are in particular *isolated*, i.e., if C is convex in G and $g^n \neq 1$ belongs to C for some $g \in G \setminus \{1\}$ and some $n \in \mathbb{N}$, then $g \in C$. This follows from the fact that, if $g > 1$, then $1 < g < g^n$ for every positive integer n and, if $g < 1$, then $g^n < g < 1$ for every positive integer n. In both cases $g \in C$

by convexity. If C is a normal subgroup of G, the group C is isolated in G if and only if the quotient G/C is torsion-free.

The importance of convex subgroups comes from the following proposition (see [CR], Section 2.2.).

Proposition 3.2.18. *Let G and H be right-orderable groups and let $\phi : G \to H$ be a homomorphism. Then* $\ker\phi$ *is relatively convex in G. Conversely, if G is a right-orderable group and* $\ker\phi$ *is relatively convex in G then the image of ϕ is right-orderable.*

The proof of this proposition is closely related to the following observation. If G is an extension of two right-orderable groups N and K endowed with the right-order $\leq$ constructed in the proof of Lemma 3.2.15, then N is convex in G with respect to $\leq$. Indeed, if $n \in N$ and $g \in G$ with $1 \leq g \leq n$, by definition of $\leq$, taking the projection p to K we get $1 = p(1) \leq p(g)$ and $p(g) \leq p(n) = 1$, from which it follows that $p(g) = 1$, i.e., $g \in N$.

A weaker form of order on a group is given by locally invariant orders.

Definition 3.2.19. A partial order relation $\leq$ on a group G is said to be a *locally invariant order* (LIO) if, for all f, $g \in G$ such that $g \neq 1$ it follows that $gf > f$ or $g^{-1}f > f$.

Remark 3.2.20. It is known that every partial order on a set can be extended to a total order; for example, if X is a set with a partial order $\leq$, one can apply Zorn's lemma to the non-empty set $\mathcal{F} := \{(Y, \leq_Y) \mid Y \subseteq X \text{ and } \leq_Y \text{ is a total order on } Y \text{ which extends } \leq \text{ restricted to } Y\}$, partially ordered by inclusion: $(Y_1, \leq_{Y_1}) \leq' (Y_2, \leq_{Y_2})$ if and only if $Y_1 \subseteq Y_2$ and $\leq_{Y_2}$ restricted to Y_1 is $\leq_{Y_1}$. It is straightforward to check that, if $(Y, \leq_Y)$ is maximal in $\mathcal{F}$ with respect to $\leq'$, then $Y = X$ and therefore X is totally ordered.

If G is a group with a partial order $\leq$ that is locally invariant, we can extend this partial order to a total order in the set theoretic way; this does not affect the property defining a locally invariant order, hence it is equivalent to ask whether a group G admits a LIO or a LIO that is also a total order.

Remark 3.2.21. A right-order on a group G is a locally invariant order.

Remark 3.2.22. A group G with a LIO is torsion-free.

Proof. Let $g \in G$ with $g \neq 1$. The definition of LIO yields $g > 1$ or $g^{-1} > 1$. First suppose $g > 1$. Then either $g^2 = g \cdot g > g$ or $1 = g^{-1} \cdot g > g$ by the definition of a LIO. Since $g > 1$ by assumption, it follows that $g^2 > g$.
Inductively, assume that $g^k > g^{k-1}$, with $k \geq 1$; hence, either $g^{k+1} = g \cdot g^k > g^k$ or $g^{k-1} = g^{-1} \cdot g^k > g^k$, from which it follows that $g^{k+1} = g \cdot g^k > g^k$.
Thus, for every $n \geq 1$, $g^n > 1$ and g is not a torsion element.
If $g < 1$, it suffices to consider $\tilde{g} := g^{-1}$; indeed, by the definition of a LIO, if $g < 1$, then $g^{-1} > 1$. □

Remark 3.2.23. Let $\{G_i\}_{i \in I}$, with I an arbitrary set of indices, be a collection of groups, each admitting a bi-order (a right-order or a locally invariant order, respectively). Then, by well-ordering I, one can consider the bi-order (right-order, or locally invariant order, respectively) on the direct product $\prod_{i \in I} G_i$ given by

the lexicographic order. In particular, if $\{G_i\}_{i\in I}$ is an inverse system of groups, each admitting a bi-order (right-order, locally invariant order, respectively), also the inverse limit of the groups G_i admits such an order.

As an example, we can consider pronilpotent groups, i.e., inverse limits of finite nilpotent groups. We already saw that a pronilpotent group G is isomorphic to the direct product of its Sylow subgroups (Proposition 1.1.22); thus, if all the Sylow subgroups of G are (locally invariant, right-)orderable, so is G.

We now investigate what happens for the LIO property when considering group extensions.

Lemma 3.2.24. *Let G, N and H be groups such that G is a split extension of N by H, i.e., $G \simeq H \ltimes N$. Assume that H has a locally invariant order $\leq_1$ and N has a locally invariant order $\leq_2$. Then G has a locally invariant order.*

Proof. Without loss of generality, thanks to Remark 3.2.20 we can assume that $\leq_1$ and $\leq_2$ are total orders. We order G via the lexicographic order, i.e., given (h_1, n_1) and (h_2, n_2) in $G \simeq H \ltimes N$, $(h_1, n_1) < (h_2, n_2)$ if and only if $h_1 <_1 h_2$ or $h_1 = h_2$ and $n_1 <_2 n_2$. Now let $x := (h, n)$ and $y := (\tilde{h}, \tilde{n})$, $x \neq (1, 1)$, be two elements in G. Then $xy = (h\tilde{h}, \tilde{h}^{-1}n\tilde{h}\tilde{n})$ and $x^{-1}y = (h^{-1}, hn^{-1}h^{-1})(\tilde{h}, \tilde{n}) = (h^{-1}\tilde{h}, \tilde{h}^{-1}hn^{-1}h^{-1}\tilde{h}\tilde{n})$.

If $xy > y$ there is nothing to say, so assume $xy < y$. Then there are two cases:

1. $h\tilde{h} <_1 \tilde{h}$ from which it follows that $h^{-1}\tilde{h} >_1 \tilde{h}$ by the definition of a LIO on H.

2. $h\tilde{h} = \tilde{h}$ (i.e., $h = 1$) and $\tilde{h}^{-1}n\tilde{h}\tilde{n} <_2 \tilde{n}$ which implies $\tilde{h}^{-1}n^{-1}\tilde{h}\tilde{n} >_2 \tilde{n}$ by the definition of a LIO on N.

In each case we conclude that $x^{-1}y > y$, as required. □

Using the lemma above we can deduce that the property of having a locally invariant order is preserved under arbitrary group extensions. In order to do so we need to recall the notion of a standard or regular wreath product.

Definition 3.2.25. Let N and H be two groups. For each $x \in H$ consider a copy N_x of N indexed by x, with elements n_x for $n \in N$. Let $Q := \prod_{x\in H} N_x$ be the (complete) direct product of all such copies of N and consider the following action of H on Q: if $h \in H$ and $\mathbf{q} = (q_x)_{x\in H} \in Q$, then $\mathbf{q}^h$ is the tuple in Q whose x-coordinate is $q_{xh^{-1}}$, the xh^{-1}-coordinate of $\mathbf{q}$; in symbols, $(\mathbf{q}^h)_x = q_{xh^{-1}}$. The resulting semidirect product $H \ltimes Q$ is called the *(complete) regular wreath product* of N by H and denoted $N \wr H$.

The following theorem, due to Krasner and Kaloujnine, states that $N \wr H$ contains an isomorphic copy of every group extension of N by H (see [Ro], Section 11.1, Exercise 11).

Theorem 3.2.26 (Universal embedding theorem)**.** *Let G be an extension of a group N by a group H. Then there exists an injective homomorphism $G \to N \wr H$.*

Corollary 3.2.27. *Let G be an extension of N by H, where N and H admit a locally invariant order. Then G admits a locally invariant order.*

Proof. By the universal embedding theorem, G can be embedded in the wreath product $N \wr H$. Since the direct product of groups with a locally invariant order has a locally invariant order (Remark 3.2.23), by the previous lemma we can conclude that $N \wr H$ has a locally invariant order, and so does G. □

Example 3.2.28. For every natural number k consider the semidirect product $\mathbb{Z}_p \ltimes \mathbb{Z}_p^{p^k}$, where the action of $\mathbb{Z}_p$ on $\mathbb{Z}_p^{p^k}$ factors through the finite quotient $\mathbb{Z}_p/p^k\mathbb{Z}_p$ and permutes the p^k coordinates of $\mathbb{Z}_p^{p^k}$ cyclically. The collection of these groups naturally forms an inverse system so that we can consider their inverse limit $\mathbb{Z}_p \,\widehat{\wr}\, \mathbb{Z}_p := \varprojlim \mathbb{Z}_p \ltimes \mathbb{Z}_p^{p^k}$. Combining Remark 3.2.23 and Lemma 3.2.24 we get that the pro-p group $\mathbb{Z}_p \,\widehat{\wr}\, \mathbb{Z}_p$ admits a locally invariant order.

It is known that a group admitting a locally invariant order has the unique product property. To prove this implication we need to mention the concept of weakly diffuse group introduced by Bowditch in [B].

Definition 3.2.29. A group G is said to be *weakly diffuse* if, for every non-empty finite set S of G, there exists $g \in S$ such that, if $hg \in S$ and $h^{-1}g \in S$ for some $h \in G$, then $h = 1$. Such an element g is called an *extremal point* of S.

One can immediately see that, if G is right-ordered, then, given any non-empty finite set S of G, the elements $\max(S)$ and $\min(S)$ are extremal points of S in the sense of the previous definition.

It turns out that a group is weakly diffuse if and only if it admits a locally invariant order ([DNR], Proposition 1.3.9). Therefore one can prove that a group admitting a locally invariant order is a unique product group by using that weakly diffuse groups have the unique product property.

Proposition 3.2.30 (see [DNR], Section 1.4.3)**.** *All weakly diffuse groups have the unique product property.*

Proof. Let G be weakly diffuse and let A and B be two finite non-empty subsets of G. Consider the set AB and let g be an extremal point of AB, i.e., an element in AB such that, if $hg \in AB$ and $h^{-1}g \in AB$ for some $h \in G$, then $h = 1$. Suppose that there exist a_1, a_2 in A and b_1, b_2 in B with $a_1 \neq a_2$ and $b_1 \neq b_2$ such that $g = a_1b_1 = a_2b_2$. Then, letting $a := a_2a_1^{-1}$, we have: $ag = a_2a_1^{-1}a_1b_1 = a_2b_1 \in AB$ and $a^{-1}g = a_1a_2^{-1}a_2b_2 = a_1b_2 \in AB$. By the property of g it follows that $a = 1$, i.e., $a_1 = a_2$ and therefore $b_1 = b_2$. Hence g is a unique product element. □

Summarizing what we collected so far, we have the chain of implications

$$\text{bi-orderable} \Rightarrow \text{right-orderable} \Rightarrow \mathsf{LIO} \Leftrightarrow \text{weakly diffuse} \Rightarrow \mathsf{UP}.$$

Moreover, the first two implications cannot be reversed: we already saw in Remark 3.2.16 an example of a non-orderable but right-orderable group and an example of a group with a LIO that is not right-orderable is given by Dunfield in the appendix of [KRD]; more precisely, he constructs a closed orientable hyperbolic 3-manifold whose fundamental group is weakly diffuse but not right-orderable.
At present it is not known whether the implication $\mathsf{UP} \Rightarrow \mathsf{LIO}$ holds true.
Also, it is not known to us whether for some 'non-artificial' class of groups at least (for example, metabelian groups), the unique product property is equivalent to right-orderability.

3.3 The unique product property for virtually soluble subgroups of saturable groups

In [CL] it is proven that every virtually soluble subgroup of a uniform pro-p group has the unique product property by showing that such a group is torsion-free nilpotent-by-torsion-free abelian (therefore in particular right-orderable). In this section we give a different proof of a somewhat more general result, i.e., that a virtually soluble subgroup of a saturable pro-p group is right-orderable (and thus it is a unique product group).

Saturable groups were introduced by Lazard in 1965 in his foundational work "Groupes analytiques p-adiques" ([La]). A modern account of Lazard's theory of p-adic analytic groups that is close to the original can be found in [Sc]. As already mentioned, the main source for the group-theoretic reformulation of this theory, along with the discussion of some of its ramifications and applications in group theory, is [DDMS]. In his seminal paper, Lazard established that any p-adic analytic group contains an open compact saturated subgroup ([Sc], Theorem 27.1) and that, conversely, any p-valued pro-p group has a natural structure of a p-adic analytic group ([Sc], Corollary 29.6). We start by introducing saturable pro-p groups, following [K] and [GS]. The definition that we use is slightly different from the original definition introduced by Lazard. In particular, we consider finitely generated pro-p groups to start with. For this class of groups, the definition that we use agrees with Lazard's ([K], Section 2).

Definition 3.3.1. Let G be a finitely generated pro-p group. A *valuation* of G is a map $\omega : G \to \mathbb{R}_{>0} \cup \{\infty\}$ with the following properties, holding for all $x, y \in G$:

1. $\omega(x) > (p-1)^{-1}$;
2. $\omega(x) = \infty$ if and only if $x = 1$;
3. $\omega(xy^{-1}) \geq \min\{\omega(x), \omega(y)\}$;
4. $\omega([x, y]) \geq \omega(x) + \omega(y)$;
5. $\omega(x^p) = \omega(x) + 1$.

A group G with a valuation ω satisfying the previous properties is said to be a *p-valued* group.
A p-valued pro-p group is said to be *saturated* if

6. for every $x \in G$ with $\omega(x) > p(p-1)^{-1}$ there exists $y \in G$ such that $x = y^p$.

A finitely generated pro-p group G is called *saturable* if it admits a valuation ω such that (G, ω) is a saturated p-valued pro-p group.

The last property (6.) ensures that in saturable pro-p groups we can extract p-roots of elements whose valuation is 'big enough'.

All uniform pro-p groups are saturable pro-p groups but the converse is not true in general. Indeed, let G be a uniform pro-p group and set $\varepsilon = 0$ if p is odd and $\varepsilon = 1$ if $p = 2$. For all positive integers n consider $G_n := G^{p^{n-1}}$. Then the map $\omega : G \to \mathbb{N} \cup \{\infty\}$ that sends any $g \in G$ to $\omega(g) := \varepsilon + \sup\{n \mid g \in G_n\}$ defines a valuation in the sense of the previous definition and turns G into a saturable

group (see [K], Remark 2.1). Conversely, saturable groups are not always uniform. For example, if $d < p-1$ and $d \geq 2$, then the Sylow pro-p subgroups of $\mathrm{GL}_d(\mathbb{Z}_p)$ and $\mathrm{SL}_d(\mathbb{Z}_p)$ are saturable but not uniform (see [K], Theorem 1.1 and Proposition 2.4). However, it is the case that saturable pro-p groups are virtually uniform and therefore have finite rank.

In [GS], González-Sánchez characterised saturable pro-p groups as groups having a potent filtration (or PF-groups). Using this characterisation he was able to recover the fact that in saturable pro-p groups, for any natural number k, the map $x \mapsto x^{p^k}$ is injective, or equivalently, that p^k-roots are unique. Note that from this fact it follows that saturable pro-p groups are torsion-free.

Proposition 3.3.2 ([GS], Proposition 2.2)**.** *Let G be a saturable pro-p group and k a natural number. If x, y belong to G and $x^{p^k} = y^{p^k}$ then $x = y$.*

Example 3.3.3. Let G be a saturable pro-p group with center $Z(G)$. Then $G/Z(G)$ is torsion-free and, if $G/Z(G)$ is bi-orderable, then G is bi-orderable.

Proof. We note that the center of a saturable group is isolated: if k is a natural number and z is an element of G such that z^{p^k} is in $Z(G)$ then $(x^{-1}zx)^{p^k} = x^{-1}z^{p^k}x = z^{p^k}$ for all x in G, and therefore $x^{-1}zx = z$ for all x in G by the previous proposition. It follows that the quotient $G/Z(G)$ is torsion-free. If it is bi-orderable, by Remark 3.2.16 the procedure of extension of the order given in the proof of Lemma 3.2.15 gives a bi-order on G because conjugation on $Z(G)$ is trivial. □

Conversely, it is always true that the quotient of a bi-orderable group by its center is bi-orderable ([KoK], Chapter II, Section 4, Theorem 3).

In general, there is a correspondence only between saturable pro-p groups of dimension less than p and residually-nilpotent $\mathbb{Z}_p$-Lie lattices of dimension less than p, under which closed subgroups correspond to $\mathbb{Z}_p$-Lie sublattices and closed normal subgroups to Lie ideals ([GSK], Theorem B). However, in the soluble case the following result about the correspondence between soluble saturable pro-p groups and soluble Lie lattices holds true.

Theorem 3.3.4 ([GS], Corollary 4.7)**.** *Let G be a saturable pro-p group and L the corresponding $\mathbb{Z}_p$-Lie lattice (on the same underlying set). Then the derived series of G and L coincide. In particular, G is soluble if and only if L is soluble and the derived lengths of G and L coincide.*

Recall also that, if G is a saturable pro-p group and L is the $\mathbb{Z}_p$-lattice associated to G, then $\mathfrak{L} := L \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is the $\mathbb{Q}_p$-Lie algebra associated to G. In particular, it follows from the previous theorem that, if G is soluble, then also L and therefore $\mathfrak{L}$ are soluble.

We can now prove that virtually soluble saturable pro-p groups are right-orderable.

Theorem 3.3.5. *Let G be a virtually soluble, saturable pro-p group. Then G is right-orderable (and in particular it has the unique product property).*

Proof. First of all we note that a virtually soluble, saturable pro-p group G is soluble. Indeed, let G_1 be a soluble normal subgroup of finite index in G; since G is a pro-p group, the quotient G/G_1 is a finite p-group, hence soluble. Thus, G is soluble, being an extension of soluble groups. Therefore we can assume that G is soluble.

We consider the derived series of G:

$$1 = G^{(n)} \trianglelefteq \ldots \trianglelefteq G'' := [G', G'] \trianglelefteq G' := [G, G] \trianglelefteq G^{(0)} := G;$$

by hypothesis it terminates in a finite number of steps, say n steps. Each quotient $G^{(i)}/G^{(i+1)}$ ($i \in \{0, \ldots, n-1\}$) is an abelian finitely generated pro-p group, hence of the form $\mathbb{Z}_p^{d_i} \times F_i$ with $d_i \geq 0$ a natural number and F_i a finite abelian p-group. We observe that, for each $i \in \{0, \ldots, n-1\}$, necessarily $d_i > 0$. Indeed, d_{n-1} is necessarily greater than 0 as G is torsion-free. Suppose that $d_{i_0} = 0$ for some $i_0 \in \{0, \ldots, n-2\}$, i.e., $G^{(i_0+1)}$ has finite index in $G^{(i_0)}$; then, if L_i denotes the $\mathbb{Z}_p$-Lie lattice corresponding to $G^{(i)}$ (on the same underlying set), we have that $\mathfrak{L}_{i_0+1} = L_{i_0+1} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = L_{i_0} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = \mathfrak{L}_{i_0}$, from which $\mathfrak{L}_{i_0+2} = [\mathfrak{L}_{i_0+1}, \mathfrak{L}_{i_0+1}] = [\mathfrak{L}_{i_0}, \mathfrak{L}_{i_0}] = \mathfrak{L}_{i_0+1}$ and, inductively, $\mathfrak{L}_{i_0+k} = \mathfrak{L}_{i_0} \neq 0$ for every $k \geq 0$, in contradiction with the fact that, by Theorem 3.3.4, $\mathfrak{L}_0$ is soluble.

Now we consider the *isolator* of G' in G, i.e., the group $H_1 = \mathrm{iso}_G(G') := \langle g \in G \mid \exists\, k \in \mathbb{N} : g^{p^k} \in G' \rangle$. It can be shown that $\mathrm{iso}_G(G')$ is a normal closed subgroup of G and that the index of G' in $\mathrm{iso}_G(G')$ is finite. Moreover, as G' is a closed subgroup of G and G is saturable, $\mathrm{iso}_G(G')$ is saturable (see [GSK], Section 3). It is clear from the definition that $\mathrm{iso}_G(G')$ is the maximal subgroup of G containing G' such that its quotient by G' is finite; hence $H_1/G' \cong F_0$ and $G/H_1 \cong \mathbb{Z}_p^{d_0}$. We now consider H_1'. For the same reason as before, since H_1 is a saturable soluble group, we have that the quotient H_1/H_1' is infinite. Therefore we can consider the proper subgroup of H_1 given by $H_2 := \mathrm{iso}_{H_1}(H_1')$, that is a normal closed saturable subgroup of H_1 such that H_1/H_2 is abelian torsion-free. We now iterate the same process for every $i \geq 2$ by setting $H_i := \mathrm{iso}_{H_{i-1}}(H_{i-1}')$. Every quotient H_i/H_{i+1} is an abelian torsion-free group. Furthermore, as G has finite dimension, this process must terminate in a finite number of steps. If H_{m-1} is the last non-trivial group in this series, then H_{m-1} must be torsion-free as G is torsion-free.

Thus we obtained a finite chain

$$1 = H_m \trianglelefteq \ldots \trianglelefteq H_2 \trianglelefteq H_1 \trianglelefteq H_0 := G, \tag{3.1}$$

where all the quotients H_i/H_{i+1} are abelian torsion-free, hence right-orderable. By using repeatedly Lemma 3.2.15, which states that extensions of right-orderable groups are right-orderable, we finally get that G is right-orderable. □

Remark 3.3.6. In general, the groups H_i in the previous proof differ from the derived subgroups $G^{(i)}$. For example, consider the $\mathbb{Z}_p$-Lie lattice given by $L = \mathbb{Z}_p x + \mathbb{Z}_p y + \mathbb{Z}_p z$ with Lie bracket $[x, y]_{\mathrm{Lie}} = p^k z$ for some integer $k \geq 1$. It is clear that L is a powerful $\mathbb{Z}_p$-Lie lattice and therefore it is associated to a uniform pro-p group G. Here $[L, L] = p^k\langle z \rangle$, hence, by Theorem 3.3.4, $G/G' \cong \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}/p^k\mathbb{Z}$. Therefore $H_1 = \langle \bar{z} \rangle \neq \langle \bar{z}^{p^k} \rangle = G'$, where $\bar{z}$ is the element corresponding to z under the Lie correspondence.
However, if we set $K_1 := \mathrm{iso}_G G'$ and $K_i := \mathrm{iso}_{K_{i-1}} G^{(i)} = \mathrm{iso}_G G^{(i)}$ for each

$2 \leq i \leq n$, then $K_i = H_i$ for each i, hence in particular $m = n$, i.e., the number of steps in the series (3.1) is the same as the derived length of G. This can be proven by induction. For $i = 1$ the groups H_1 and K_1 coincide by definition. Assume now that $H_\ell = K_\ell$ for some integer $\ell \geq 1$. By using Theorem 3.3.4 one can show that $K_\ell/K_{\ell+1} = H_\ell/K_{\ell+1}$ is torsion-free abelian, from which it follows that $H_{\ell+1} \subseteq K_{\ell+1}$ as, by definition, $H_\ell/H_{\ell+1}$ is the biggest torsion-free abelian quotient of H_ℓ. Conversely, from $H_\ell = K_\ell = \mathrm{iso}_{K_{\ell-1}} G^{(\ell)} \supseteq G^{(\ell)}$ one has $G^{(\ell+1)} = (G^{(\ell)})' \subseteq H'_\ell$ and therefore $K_{\ell+1} = \mathrm{iso}_{K_\ell}(G^{(\ell+1)}) \subseteq \mathrm{iso}_{H_\ell} H'_\ell = H_{\ell+1}$.

Corollary 3.3.7. *Let H be a virtually soluble subgroup of a saturable pro-p group G. Then H is right-orderable.*

Proof. Since the closure of H in G is again a virtually soluble group, we can assume that H is closed. By [GSK], Proposition 3.2, the isolator $\mathrm{iso}_G(H)$ of H in G is saturable and $[\mathrm{iso}_G(H) : H] < \infty$. It follows that $\mathrm{iso}_G(H)$ is a saturable virtually soluble group, hence right-orderable by the previous proposition. □

Corollary 3.3.8. *Let G be an extension or an arbitrary direct product of virtually soluble subgroups of saturable groups. Then G is right-orderable, hence has the unique product property.*

For example, pronilpotent groups whose Sylow subgroups are virtually soluble subgroups of saturable groups are right-orderable.

Remark 3.3.9. By construction, the subgroups H_i in the series (3.1) in the proof of Theorem 3.3.5 are convex with respect to the right-order constructed (see remark after Proposition 3.2.18). Moreover, it is easy to see that the series obtained by the chain of subgroups H_i is normal.

Recall that a group G is said to be *locally indicable* if each non-trivial finitely generated subgroup of G admits a non-trivial homomorphism onto $(\mathbb{Z}, +)$. Being locally indicable is equivalent to admitting Conradian orders ([DNR], Theorem 3.2.3). A right-order $\leq$ is said to be a Conradian order (or C-order) if, for all positive elements g, h in G there exists a natural number n such that $h^n g \geq h$. We will say that a group that possesses Conradian orders is *Conradian-orderable*. The property of being Conradian-orderable is weaker than bi-orderability and stronger than right-orderability (for examples of right-orderable but not Conradian-orderable groups, see [DNR], page 94; an example of a Conradian-orderable but not bi-orderable group is given in [BMR], Example 7.5.4). However, for amenable groups the following result of Morris-Witte holds (see [DNR], Theorem 4.1.3, and [Mo]).

Theorem 3.3.10 (Morris-Witte; [Mo], Theorem B)**.** *Right-orderable amenable groups are locally indicable. In particular, amenable groups are locally indicable (or, equivalently, Conradian-orderable) if and only if they are right-orderable.*

Since virtually soluble groups are amenable, the following holds.

Corollary 3.3.11. *Virtually soluble subgroups of saturable pro-p groups are locally indicable or, equivalently, Conradian-orderable.*

Note that this result follows also directly from the fact that a virtually soluble subgroup G of a saturable pro-p group possesses a finite chain as in (3.1). Indeed,

intersecting any non-trivial finitely generated subgroup K of G with such a chain, one gets that K has a non-trivial torsion-free abelian quotient.

In light of Theorem 3.3.5, it is natural to ask whether there are soluble torsion-free pro-p groups of finite rank other than soluble saturable pro-p groups that are right-orderable. If we consider the pro-2 completion of the group G_2 in Example 3.2.3, we get a torsion-free ([CBKL], Corollary 2.3) pro-2 group of finite rank that is not right-orderable, as it does not possess the unique product property. Therefore we cannot expect that all soluble torsion-free pro-p groups of finite rank are right-orderable. However, Example 4.2 in [GSK] shows that the soluble torsion-free p-adic analytic pro-p group given by

$$G := \langle \alpha \rangle \ltimes \langle x_1, \dots, x_{p-1} \rangle \cong \mathbb{Z}_p \ltimes \mathbb{Z}_p^{p-1},$$

with action

$$x_i^{\alpha} = \begin{cases} x_i x_{i+1}, & \text{if } 1 \leq i \leq p-2 \\ x_{p-1} x_1^p, & \text{if } i = p-1 \end{cases}$$

is not saturable. Nonetheless, as G is the extension of two torsion-free abelian groups, G is right-orderable.

Looking at these examples and at the proof of Theorem 3.3.5, it seems that the fact that closed subgroups of a given finitely generated soluble pro-p group G have infinite abelianisation is related with the fact that G is right-orderable, or, equivalently (by Theorem 3.3.10), locally indicable. Moreover, in the abstract setting, by definition a group is locally indicable if and only if each of its finitely generated subgroups has infinite abelianisation. The analogous situation in the pro-p setting would be that each non-trivial closed subgroup of the given finitely generated pro-p group has infinite abelianisation. It is not clear whether the latter condition is stronger than local indicability. In particular, we prove that the fact that all closed subgroups have infinite abelianisation is equivalent to local indicability plus an extra condition, that seems to be the analogue to the Conradian property of convex jumps in the profinite setting (see Theorem 3.3.12). It is not immediately apparent whether this extra condition is already implied by local indicability. We will prove that, in fact, it is in the special case of metabelian pro-p groups of finite rank (see Corollary 3.3.19).

In order to understand this condition and our statement, recall that, if G is a right-ordered group with order $\leq$, then the convex subgroups of G relative to $\leq$ are linearly ordered by inclusion, i.e., if C and D are convex subgroups of G with respect to $\leq$, then either $C \subseteq D$ or $D \subseteq C$. Moreover, arbitrary intersections and unions of convex subgroups are again convex subgroups ([BMR], Section 7.2). Finally, let C and D be convex subgroups of G, and assume without loss of generality that $C \subseteq D$. Then the pair (C, D) is called a *convex jump* if $C \neq D$ and there is no convex subgroup strictly contained between C and D. An order is a Conradian order if and only if the following property regarding convex jumps holds true: if (C, D) is any convex jump relative to the given order, then $C \lhd D$ and D/C is isomorphic to a subgroup of the additive group of the reals, hence it is in particular torsion-free abelian ([BMR], Theorem 7.4.1, (4)).

Finally, note that, since we are dealing with finitely generated profinite groups, we always consider the *topological* abelianisation $G/\overline{G'}$ of a given finitely generated group G. Indeed, in this case the abstract commutator subgroup G' is au-

tomatically closed and therefore $G' = \overline{G'}$ ([Se], Corollary 4.7.3). This is generally not the case for non finitely generated profinite groups.

We can now state the following result.

Theorem 3.3.12. *Let G be a soluble profinite group with the ascending chain condition on closed subgroups. Then the following are equivalent:*

1. *G is torsion-free and, for every non-trivial $H \leq_c G$, the abelianisation H/H' is infinite;*

2. *G is locally indicable and, for every $H \leq_c G$, there exists a Conradian order on H such that the maximal proper closed convex subgroup C of H' is normal in H' and the quotient H'/C is torsion-free abelian.*

Note that whenever we talk about local indicability, even in the context of profinite groups, we always consider *abstractly* finitely generated subgroups. It remains open to investigate whether a characterisation of right-orderable, or, equivalently (by Theorem 3.3.10), locally indicable soluble pro-p groups of finite rank can be established (see Section 3.6 for more open questions).

The proof of the theorem relies on the following

Proposition 3.3.13. *Let G be a profinite group with the ascending chain condition on closed subgroups and let K be a finite index subgroup of G. Assume that there exists a Conradian right-order $\leq$ on G such that the maximal proper closed convex subgroup C of K with respect to $\leq$ is normal in K and the quotient K/C is non-trivial and torsion-free abelian. Then the abelianisation of G is infinite.*

The proof of this proposition is a slight modification of the proof of a result of Rhemtulla, that we write for completeness (see Theorem 3 in [R] and Theorem 7.5.10 in [BMR]). We will need the following property of Conradian orders.

Lemma 3.3.14 ([BMR], Theorem 7.4.1, (2))**.** *Let G be a Conradian-orderable group and let $\leq$ be a Conradian order on G. Then, for all x, y in G with $y > x > 1$, there exists a positive integer m such that $xy^m x^{-1} > y$.*

Proof of Proposition 3.3.13. The group G is torsion-free. If G is abelian there is nothing to prove, so assume that the derived subgroup of G is non-trivial. As, by hypothesis, K/C is non-trivial and torsion-free abelian, the subgroup K has infinite abelianisation. Let $I := \mathrm{iso}_K K'$. Then K/I is a non-trivial torsion-free abelian group.

Now assume by contradiction that G/G' is finite and let $1 = x_1 < x_2 < \cdots < x_n$ be representatives of the cosets of K in G. Let $\tau : G \to K/I$ be the transfer map (see [Ro], Section 10.1). As K/I is torsion-free abelian and the abelianisation of G is finite, the map τ must be trivial.

Assume that there exists $g \in K$ such that $g > x_n$. Then $g > x_i > 1$ for all $i \in \{2, \ldots, n\}$ and therefore $g x_i^{-1} > 1$ for all such i. From $x_i > 1$ we get $g^{x_i^{-1}} = x_i g x_i^{-1} > g x_i^{-1} > 1$, thus $g^{x_2^{-1}} g^{x_3^{-1}} > g^{x_3^{-1}} > 1$ and so on until $g^{x_2^{-1}} \ldots g^{x_n^{-1}} > 1$. Therefore,

$$g^{x_2^{-1}} \ldots g^{x_n^{-1}} g > g.$$

Moreover, as τ is trivial, $g^{x_2^{-1}} \ldots g^{x_n^{-1}} g \in I$.
We now show that such an element g exists. Because of Lemma 3.3.14, if z is any

positive element in K with $z < x_n$, then there exists a positive integer m such that $zx_n^m z^{-1} > x_n$. We now show that g can be taken to be a power of $zx_n^m z^{-1}$.
Claim. There is a positive integer N such that $zx_n^N z^{-1} \in K$ and $zx_n^N z^{-1} > x_n$.

Proof of Claim. We know that $zx_n^m z^{-1} > x_n > 1$. Let N be any multiple of $n = [G : K]$ such that $N > m$. Then, as N is a multiple of n, the element $zx_n^N z^{-1}$ is in K. Moreover, as $N > m$, one has $zx_n^{N-m} z^{-1} > 1$ and therefore

$$zx_n^N z^{-1} = (zx_n^{N-m} z^{-1})(zx_n^m z^{-1}) > zx_n^m z^{-1} > x_n.$$

□

We can therefore assume that in a suitably chosen set of generators of K, we can find an element g greater than x_n.

Let $g_1 < g_2 < \cdots < g_l = g$ be such generators, with $g > x_n$. Let D be a closed convex subgroup of K containing g. By convexity, D must contain every g_i, for $i \in \{1, \ldots, l\}$, and therefore $D = K$. Now let $\tilde{C}$ be the union of closed convex subgroups of K not containing g. As the convex subgroups form a chain and G has the ascending chain condition on closed subgroups, this union is over finitely many terms and therefore a closed convex subgroup. It follows that $\tilde{C}$ is the maximal closed convex subgroup of K and does not contain g. Therefore $\tilde{C} = C$.

By hypothesis, C is normal in K and K/C is abelian torsion-free. Therefore, $I \subseteq C$ because I is the smallest closed subgroup of K such that K/I is abelian torsion-free. It follows from $g^{x_2^{-1}} \ldots g^{x_n^{-1}} g > g > 1$ and $g^{x_2^{-1}} \ldots g^{x_n^{-1}} g \in I$ that g belongs to C, which yields the required contradiction.

□

In order to prove Theorem 3.3.12 we will also need the following result, stating that the extension of a Conradian order by a Conradian order is Conradian.

Lemma 3.3.15. *Let G be a an extension of N by K, where both N and K have a Conradian order. Then the extension of the order on N by the order on K, given as in the proof of Lemma 3.2.15, defines a Conradian order on G.*

Proof. We will use the fact that a right-order on a group G is a Conradian order if and only if, for all positive elements x, y in G, $y^2 x > y$ ([DNR], Proposition 3.2.1.). Let $i : N \to G$ be the inclusion map, $p : G \to G/N \cong K$ be the projection map and $\leq_N$ and $\leq_K$ the given Conradian orders on N and K respectively. Recall from Lemma 3.2.15 that the extension of $\leq_N$ by $\leq_K$ is the right-order $\leq$ on G defined in the following way. Let x, y be two elements of G.

1. If $p(x) \neq p(y)$ then $x > y$ if $p(x) >_K p(y)$ in K;
2. If $p(x) = p(y)$ then there exists a unique element $n \in N$ such that $i(n) = xy^{-1}$. We set $x \geq y$ if $n \geq_N 1_N$ in N. By slight abuse of notation we will just write $xy^{-1} \geq_N 1_N$ in this case.

We verify that this right-order is Conradian. Let x and y be positive in G with respect to $\leq$. We distinguish two cases.

1. Assume that $p(y^2xy^{-1}) \neq 1_K$. If also $p(x)$ and $p(y)$ are different from 1_K then $p(x) >_K 1_K$ and $p(y) >_K 1_K$ by definition of $\leq$. Therefore $p(x)$ and $p(y)$ are positive elements in K and, since $\leq_K$ is Conradian, $p(y)^2p(x)p(y)^{-1} >_K 1_K$, from which $y^2xy^{-1} > 1$. If $p(x) >_K 1_K$ but $p(y) = 1_K$, then $p(y)^2p(x)p(y)^{-1} = p(x) >_K 1_K$. Similarly, if $p(x) = 1_K$ and $p(y) >_K 1_K$, then $p(y)^2p(x)p(y)^{-1} = p(y) >_K 1_K$. Finally, if both $p(x) = p(y) = 1_K$, then also $p(y^2xy^{-1}) = 1_K$, a contradiction.

2. Now consider the case $p(y^2xy^{-1}) = 1_K$. If both $p(x) = p(y) = 1_K$ then $x >_N 1_N$ and $y >_N 1_N$ and we can again use the fact that $\leq_N$ is Conradian. Also, if one of $p(x)$ and $p(y)$ is equal to 1_K, from $p(y^2xy^{-1}) = 1_K$ it follows that also the other is equal to 1_K. Finally, if both $p(x) \neq 1_K$ and $p(y) \neq 1_K$ then, from the fact that $\leq_K$ is Conradian, we would get $p(y)^2p(x)p(y)^{-1} >_K 1_K$, a contradiction.

□

Proof of Theorem 3.3.12.

1. $\Rightarrow$ 2. Let H be a closed subgroup of G. By using the same argument of the proof of Theorem 3.3.5 we get that H has a finite subnormal series

$$1 = H_m \triangleleft \cdots \triangleleft H_1 \triangleleft H_0 = H,$$

where $H_i := \mathrm{iso}_{H_{i-1}} H'_{i-1}$ for each $i \in \{1, \ldots, m\}$. As this is in particular true for G, it follows as before that G is locally indicable. As each quotient H_i/H_{i+1} is Conradian-orderable, we can construct a Conradian order $\leq$ on H using Lemma 3.3.15. Note that, with respect to this order, $H_2 = \mathrm{iso}_{H_1} H'_1$ is convex in H_1. Moreover, as H_2 is normal in H_1 and H' is contained in H_1, also $H_2 \cap H'$ is normal in H'. Now $H'/(H' \cap H_2) \cong H'H_2/H_2 < H_1/H_2$ is abelian torsion-free and ordered. Therefore $H' \cap H_2 \triangleleft H'$ is a closed convex subgroup of H' with respect to $\leq$. (Alternatively, one can observe that, as $H' \subseteq H_1$ and H_2 is convex in H_1, then $H' \cap H_2$ is convex in H' by definition of convex subgroup.) It follows that the maximal closed convex subgroup C of H' with respect to $\leq$ contains $H' \cap H_2$. Therefore C is normal in H' and H'/C is torsion-free abelian.

2. $\Rightarrow$ 1. Let H be a closed subgroup of G and assume that H' has finite index in H. Then, if we apply Proposition 3.3.13 with $K = H'$, we obtain that G has infinite abelianisation, a contradiction.

□

Corollary 3.3.16. *Let G be a torsion-free soluble pro-p group with finite rank. Then the following are equivalent:*

1. *for every closed subgroup $H \leq_c G$ the abelianisation H/H' is infinite;*

2. *G is locally indicable and, for every $H <_c G$, there exists a Conradian right-order on H such that the maximal proper closed convex subgroup C of H' is normal in H' and the quotient H'/C is abelian torsion-free;*

3. *every closed subgroup of G admits a finite subnormal series whose factor groups are isomorphic to $\mathbb{Z}_p$.*

Proof.

1. $\Leftrightarrow$ 2. Since a pro-p group with finite rank satisfies the ascending chain condition on closed subgroups (see [W1], Chapter 8, Exercise 8 (c) or [K1], Section 5.8), this equivalence was already proved in the previous theorem.

3. $\Rightarrow$ 1. If H is a closed subgroup of G and admits such a subnormal series then H has infinite abelianisation.

1. $\Rightarrow$ 3. Let H be a closed subgroup of G. Under this hypothesis we can perform the same procedure carried out in the proof of Theorem 3.3.5 i.e., take $H_1 := \mathrm{iso}_H H'$ and, for $i \geq 2$, $H_i := \mathrm{iso}_{H_{i-1}} H'_{i-1}$. As G has finite rank, this subnormal series must terminate in a finite number of steps. All of its quotients are torsion-free finitely generated abelian pro-p groups and therefore this series can be refined to a finite one where each quotient is isomorphic to $\mathbb{Z}_p$. □

Remark 3.3.17. Before going further we note that, at least in some cases, insoluble pro-p groups of finite rank cannot be locally indicable because they contain a subgroup with property (T) (see [Mar], Chapter 3 or [Z], Section 7.1). For example, $\Gamma := \mathrm{SL}_d(\mathbb{Z})$ is a lattice in $\mathrm{SL}_d(\mathbb{R})$ ([Be], Section 2, Example 1.1). If $d \geq 3$, then, by [Z], Theorem 7.1.4, Γ has property (T) and therefore also its finite index subgroups have the same property. Moreover, a discrete group that possesses property (T) has finite abelianisation ([Z], Corollary 7.1.11). In particular, any finitely generated subgroup of finite index in Γ has finite abelianisation. Since $\Gamma \leq \mathrm{SL}_d(\mathbb{Z}_p)$, it follows that, for $d \geq 3$, the insoluble pro-p group of finite rank $\mathrm{SL}^1_d(\mathbb{Z}_p)$ cannot be locally indicable.

Going back to local indicability, in the special case when G is metabelian we can say more.

Proposition 3.3.18. *Let G be a metabelian right-orderable profinite group with the ascending chain condition on closed subgroups. Then the abelianisation of G is infinite and there exists a Conradian right-order on G such that, if C is the maximal proper normal closed convex subgroup of G, then the quotient G/C is torsion-free abelian.*

Proof of Proposition 3.3.18. Let n be the derived length of G. If $n = 1$ then G is abelian and there is nothing to prove because all right-orders on an abelian group are bi-orders, hence in particular Conradian.

Let then $n = 2$; we first prove that the abelianisation of G is infinite. As G is soluble and right-orderable, it is Conradian-orderable by Theorem 3.3.10. Therefore we can fix a Conradian order $\leq$ on G. Assume by contradiction that G/G' is finite. As G' is abelian, the maximal proper closed convex subgroup D of G' with respect to the restriction of $\leq$ is normal and this implies that G'/D is torsion-free abelian. Therefore, applying Proposition 3.3.13 with $K = G'$, we conclude that G has infinite abelianisation.

Now we show that there exists a Conradian order on G with the properties claimed in the statement. We consider the proper closed subgroup of G given by $I := \mathrm{iso}_G G'$. As G/I is an abelian torsion-free group, we can fix a Conradian

order $\leq^*$ on G/I. Also, the restriction of the Conradian order $\leq$ of G to I is still Conradian. The extension $\leq'$ of $\leq_{|I}$ by $\leq^*$ is Conradian by Lemma 3.3.15 and I is convex in G with respect to $\leq'$. Thus, if C is the maximal proper normal closed convex subgroup of G, then $I \subseteq C$ and therefore G/C is torsion-free abelian. □

Corollary 3.3.19. *Let G be a metabelian profinite group with the ascending chain condition on closed subgroups. Then the following are equivalent:*

1. *G is torsion-free and, for every $H \leq_c G$, the abelianisation H/H' is infinite;*
2. *G is locally indicable.*

Proof.

1. $\Rightarrow$ 2. This follows from Theorem 3.3.12.

2. $\Rightarrow$ 1. Every closed subgroup H of G is again a locally indicable metabelian profinite group with the ascending chain condition on closed subgroups. Therefore, by Proposition 3.3.18, the abelianisation of H is infinite.

□

We conclude this section with two examples in which we use the result in Theorem 3.3.5 to construct some pairs of sets in the congruence subgroups $\mathrm{SL}_2^\ell(\mathbb{Z}_p)$ (with ℓ any positive integer) that have a unique product element. Similar examples can be more generally obtained in pro-p Chevalley groups (see the beginning of Section 3.4 and [BJZK], Proposition 4.1). Recall that every element in $\mathrm{SL}_2^\ell(\mathbb{Z}_p)$ can be written in a unique way as an element of the form xhy, where x, h and y are in $\mathrm{SL}_2^\ell(\mathbb{Z}_p)$, x is an upper unitriangular matrix, h is a diagonal matrix and y is a lower unitriangular matrix. Also, every element in $\mathrm{SL}_2^\ell(\mathbb{Z}_p)$ can be written in a unique way as an element of the form $\tilde{y}\tilde{h}\tilde{x}$, where $\tilde{x}, \tilde{h}$ and $\tilde{y}$ are in $\mathrm{SL}_2^\ell(\mathbb{Z}_p)$, $\tilde{y}$ is a lower unitriangular matrix, $\tilde{h}$ is a diagonal matrix and $\tilde{x}$ is an upper unitriangular matrix.

Example 3.3.20.

1. Let $A = \{x_1h_1y_1, \ldots, x_nh_ny_n\}$ and B be two finite non-empty sets in $\mathrm{SL}_2^\ell(\mathbb{Z}_p)$ and assume that $y_1 = y_i$ for all $i \in \{1, \ldots n\}$; call y this common value. In this example we show that $A \cdot B$ has a unique product element, i.e., that there exists at least one element in $\mathrm{SL}_2^\ell(\mathbb{Z}_p)$ that can be written in a unique way as a product of an element of A and an element of B.
   Here by $A \cdot B$ we mean the list of all products of the form ab, with $a \in A$ and $b \in B$, possibly with repetitions, i.e., there might be $a \neq a'$ in A and $b \neq b'$ in B such that $ab = a'b'$, but both products would be listed in $A \cdot B$, as ab and $a'b'$ respectively.
   Set $A' := Ay^{-1}$ and $B' := yB$; then A' contains only upper triangular matrices, while B' can be partitioned as $B' = X_1\tilde{y}_1 \sqcup \cdots \sqcup X_k\tilde{y}_k$ where k is some index, $X_1, \ldots, X_k$ are sets containing upper triangular matrices and $\tilde{y}_1, \ldots, \tilde{y}_k$ are lower unitriangular matrices with $\tilde{y}_i \neq \tilde{y}_j$ for all $i \neq j$. This partition of B' comes from the fact, recalled above, that every element in $\mathrm{SL}_2^\ell(\mathbb{Z}_p)$ can be written as a product of three matrices in $\mathrm{SL}_2^\ell(\mathbb{Z}_p)$, namely an upper unitriangular matrix, a diagonal matrix and a lower unitriangular

matrix.

Note that $A \cdot B = A' \cdot B'$ and that, if $a \in A$ and $b \in B$, then $ay^{-1} \cdot yb = a \cdot b$ is a unique product element for A' and B' if and only if it is a unique product element for A and B. Therefore it is enough to consider $A' \cdot B'$.

As we proved that soluble uniform groups are unique product groups, for each pair of sets (A', X_i) $(i \in \{1, \dots, k\})$ we can find a unique product element $u_i = a'x$ in $A' \cdot X_i$. Now $u_i\tilde{y}_i \neq r_i\tilde{y}_i$ for each $r_i \in A' \cdot X_i \setminus \{a'x\}$ because $u_i = a'x$ is a unique product element. Also, $u_i\tilde{y}_i \neq x\tilde{y}_j$ for each $j \in \{1, \dots, k\} \setminus \{i\}$ and every $x \in X_j$ because these two elements have a different lower unitriangular part. Therefore, each $u_i\tilde{y}_i$ is a unique product element for A' and B', hence for A and B. Analogously, one could consider two sets A and B such that all the upper unitriangular parts of the elements in B coincide.

2. Let $A = \{x_1h_1y_1, \dots, x_nh_ny_n\}$ and $B = \{y'_1h'_1x'_1, \dots, y'_rh'_rx'_r\}$ be two finite non-empty sets in $\mathrm{SL}_2^\ell(\mathbb{Z}_p)$ and take the two sets A' and B' obtained from A and B by considering just the lower unitriangular parts of the elements of A and B: $A' = \{y_1, \dots, y_n\}$ and $B' = \{y'_1, \dots, y'_r\}$.

   Claim 1. If the two sets A' and B' have 1 as a unique product element obtained by $y_1 = 1$ and $y'_1 = 1$, then also A and B have a unique product element.

   From this we will deduce that any normal open subgroup of $\mathrm{SL}_2^\ell(\mathbb{Z}_p)$ contains at least two sets with a unique product element that are not contained in a soluble subgroup of $\mathrm{SL}_2^\ell(\mathbb{Z}_p)$.

   Proof of Claim 1. Note that some of the terms in A' and B' may be repeated in the original sets A and B but we consider them just once in A', B'. Also, if A' and B' are trivial there is nothing to say (we are in the soluble case since all elements in A and B are upper triangular).
   By using UP in the soluble case, we get an element $y_iy'_j$ among the products of the elements of A' and the elements of B' that can be written in a unique way as the product of an element of A' by an element of B'. Without loss of generality, we can assume, by reordering if necessary, that this element is $y_1y'_1$.

   Let $I := \{i_1, \dots, i_d\}$ be the set of indices i such that $y_i = y_1 = 1$. Note that I contains at least 1. Then we must have $x_{i_r}h_{i_r} \neq x_{i_s}h_{i_s}$ for every pair of distinct indices i_r and i_s in I.
   In a similar way define $J := \{j_1, \dots, j_e\}$, where $y'_j = y'_1 = 1$ for all $j \in J$.
   Consider the elements among the products of elements of A and elements of B of the form $x_ih_ih'_jx'_j$ with $i \in I$ and $j \in J$ (There is at least $x_1h_1 \cdot h'_1x'_1$).
   We claim that one of these elements is the required unique product.

   By using UP in the soluble case, we can find an element $x_{i_0}h_{i_0}h'_{j_0}x'_{j_0}$ with $i_0 \in I$ and $j_0 \in J$ that gives a unique product among the elements of this form. Moreover, this element must be different from all other products $(x_lh_ly_l)(y'_mh'_mx'_m)$ with $l \notin I$ or $m \notin J$. Indeed, since 1 is a unique product with respect to A' and B' and because of the definitions of I and J, all

these elements satisfy $y_l y'_m \neq 1$. Hence, if we rewrite $y_l y'_m h'_m x'_m$ as $\tilde{x}\tilde{h}\tilde{y}$ for some upper unitriangular matrix $\tilde{x}$, diagonal matrix $\tilde{h}$, lower unitriangular matrix $\tilde{y}$ in $\mathrm{SL}_2^\ell(\mathbb{Z}_p)$, the lower unitriangular matrix $\tilde{y}$ is non-trivial. Thus $(x_l h_l y_l)(y'_m h'_m x'_m) = (x_l h_l)\tilde{x}\tilde{h}\tilde{y}$ is an element with non-trivial lower unitriangular component, thus it cannot be an upper triangular matrix.
It follows that $x_{i_0} h_{i_0} h'_{i_0} x'_{j_0}$ is a unique product element for A and B. □

Now consider the initial situation where $A = \{x_1 h_1 y_1, \ldots, x_n h_n y_n\}$ and $B = \{y'_1 h'_1 x'_1, \ldots, y'_r h'_r x'_r\}$ are two finite non-empty sets in $\mathrm{SL}_2^\ell(\mathbb{Z}_p)$ and A' and B' are the set obtained from A and B by considering just the lower unitriangular parts of the elements of A and B: $A' = \{y_1, \ldots, y_n\}$ and $B' = \{y'_1, \ldots, y'_r\}$, but without making any assumption on the value of the unique product element of A' and B'.

Claim 2. There exist two lower unitriangular matrices y_0 and y'_0 in $\mathrm{SL}_2^\ell(\mathbb{Z}_p)$ such that $y_0 A y_0^{-1}$ and ${y'_0}^{-1} B y'_0$ have a unique product element.

Proof of Claim 2. By reordering the elements of A and B if necessary, we can assume that $y_1 y'_1$ is a unique product element for the sets A' and B'. From Claim 1 it follows that the sets $A(y_1)^{-1}$ and $(y'_1)^{-1}B$ have a unique product element. (Note that, in particular, if $y'_1 = (y_1)^{-1}$, then A and B have a unique product element. One could use the same argument by considering the upper triangular part and conclude that A and B have a unique product element if $\tilde{x}'_1 = \tilde{x}_1^{-1}$.)
Finally, note that, if u belongs to $A(y_1)^{-1}$ and v belongs to $(y'_1)^{-1}B$, then uv is a unique product element for $A(y_1)^{-1}$ and $(y'_1)^{-1}B$ if and only if $y_1 u v y'_1$ is a unique product element for $y_1 A(y_1)^{-1}$ and $(y'_1)^{-1} B y'_1$. Therefore, $y_0 = y_1$ and $y'_0 = y'_1$ prove the claim. □

Finally we can prove:

Claim 3. Any normal open subgroup of $\mathrm{SL}_2^\ell(\mathbb{Z}_p)$ contains at least two sets that are not contained in a soluble subgroup of $\mathrm{SL}_2^\ell(\mathbb{Z}_p)$ and have a unique product element.

Proof of Claim 3. Let N be a normal open subgroup of $\mathrm{SL}_2^\ell(\mathbb{Z}_p)$ and take A and B any two finite subsets of N that are not contained in a soluble subgroup of $\mathrm{SL}_2^\ell(\mathbb{Z}_p)$. By Claim 2 there exist elements y_0 and y'_0 such that $y_0 A {y_0}^{-1}$ and ${y'_0}^{-1} B' y'_0$ have a unique product property. Moreover, they are again not contained in a soluble subgroup of $\mathrm{SL}_2^\ell(\mathbb{Z}_p)$ and, since N is normal, they are contained in N. □

3.4 Non-orderability of insoluble p-adic analytic pro-p groups

We begin this section with a remark. Let $p > 2$ be a prime. By Theorem 3.3.5, the subgroups T_i of upper triangular matrices in the congruence subgroups

$G_i = \mathrm{SL}_2^i(\mathbb{Z}_p)$ $(i \geq 1)$ of $\mathrm{SL}_2(\mathbb{Z}_p)$ are right-orderable; however, we verify that they are not bi-orderable.

Indeed, any such matrix can be written in a unique way as

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} (1+t)^{-1} & 0 \\ 0 & 1+t \end{pmatrix} = \begin{pmatrix} (1+t)^{-1} & a(1+t) \\ 0 & 1+t \end{pmatrix},$$

where $a, t \in p^i\mathbb{Z}_p$ (see [BJZK], proof of Theorem 5.1).

Now consider a matrix $x(a') := \begin{pmatrix} 1 & a' \\ 0 & 1 \end{pmatrix}$ in T_i, where $a' \in p^i\mathbb{Z}_p \setminus \{0\}$; we compute a matrix $h(t) := \begin{pmatrix} (1+t)^{-1} & 0 \\ 0 & 1+t \end{pmatrix}$, where $t \in p^i\mathbb{Z}_p$, such that $h(t)^{-1}x(a')^{-1}h(t) = x(a')^{p^i-1}$.

This gives the required contradiction: if T_i is bi-orderable and $x(a') > 1$ then $x(a')^{p^i-1} > 1$ but $h(t)^{-1}x(a')^{-1}h(t) < 1$; the case $x(a') < 1$ is analogous.

We have

$$h(t)^{-1}x(a')^{-1}h(t) = \begin{pmatrix} 1 & -a'(1+t)^2 \\ 0 & 1 \end{pmatrix}$$

and

$$x(a')^{p^i-1} = \begin{pmatrix} 1 & (p^i-1)a' \\ 0 & 1 \end{pmatrix}.$$

Thus we have to solve the equation

$$t^2 + 2t + p^i = 0,$$

which has a unique solution in $p^i\mathbb{Z}_p$, obtained by applying Hensel's Lemma to the approximate solution $t = -p^i/2$ modulo p^{2i}.

This implies that subgroups of $\mathrm{SL}_2(\mathbb{Z}_p)$ of finite index cannot be bi-ordered as any such subgroup contains a principal congruence subgroup G_i.

More generally, we can deduce from this that also compact p-adic Chevalley groups are not bi-orderable. Here we recall briefly the idea of the construction of such groups; for more details see [C]. Given a crystallographic root system Φ and a complex semisimple Lie algebra $\mathfrak{L}$ of type Φ, one considers a Chevalley basis $\mathcal{B}$ of $\mathfrak{L}$ and takes the $\mathbb{Z}$-linear span $\mathfrak{L}_\mathbb{Z}$ of $\mathcal{B}$. Tensoring $\mathfrak{L}_\mathbb{Z}$ by the valuation ring R of a non-archimedean local field of characteristic 0 and residue field characteristic p, one obtains an R-Lie lattice $\mathfrak{L}_R := R \otimes_\mathbb{Z} \mathfrak{L}_\mathbb{Z}$. The Chevalley group of type Φ over R is then constructed as the subgroup of $\mathrm{Aut}(\mathfrak{L}_R)$ generated by the union of the root subgroups. It turns out that any compact p-adic Chevalley group has a subgroup commensurable to $\mathrm{SL}_2(\mathbb{Z}_p)$ (see [BJZK], Proposition 4.2), and therefore it cannot be bi-ordered.

The same reasoning can be applied also abstractly to all non-abelian uniform pro-p groups of rank 2. Indeed, let G be such a group. By Exercise 13 in [DDMS], Chapter 4, we get that G has a unique normal procyclic subgroup N with procyclic quotient G/N (compare also with [GSK], Section 7.1, where uniform pro-p groups of dimension 2 are classified). Let x be a generator of N and zN a generator of G/N; then, since N is normal and procyclic, we have that $z^{-1}xz = x^\lambda$ for some $\lambda \in \mathbb{Z}_p$ (see [RZ], Lemma 4.1.1, for the meaning of the power x^λ with $\lambda \in \mathbb{Z}_p$). Since G is uniform, $[N, G] \subseteq G^p \cap N = N^p$, and then

$x^{\lambda-1} = [z, x^{-1}] = z^{-1}xzx^{-1} \in [G, N] \subseteq N^p$, so $x^{\lambda-1} = x^{\mu p^e}$ for some integer $e \geq 1$ and some $\mu \in \mathbb{Z}_p^*$; hence $\lambda = 1 + \mu p^e$. Now there exists $\tau \in \mathbb{Z}_p^*$ such that $\lambda^\tau = 1 - p^e$, hence $z^{-\tau}xz^\tau = x^{\lambda^\tau} = x^{1-p^e}$. Since $1 - p^e < 1$ this proves that G is not bi-orderable, as no order would be preserved by conjugation.
Note that, if G is a non-abelian uniform pro-p group of rank 2, then G is non-nilpotent, since all nilpotent uniform pro-p groups of rank 2 are abelian; hence this is not in contradiction with the fact that torsion-free nilpotent groups are always bi-orderable (see [DNR], Section 2.1).
By using Corollary 1.7 in [KS], we also get that if $p \geq 3$ and G is a non-nilpotent saturable pro-p group with $\mathrm{d}(G) = \dim(G) = 2$, then G is uniform and so non bi-orderable by the previous remark.

It is therefore natural to investigate what happens in the general case. In this section we show that insoluble p-adic analytic pro-p groups are not bi-orderable. We already noted that some of these groups are not locally indicable (see Remark 3.3.17). However, we present here a more direct proof that holds for all insoluble p-adic analytic pro-p groups, does not depend on property (T) and requires some tools that are interesting in their own right. To this aim, we first deal with just-infinite insoluble pro-p groups and we prove that in such groups it is not possible to find subsemigroups with the properties of the positive cone of a bi-order. Recall that just-infinite pro-p groups are infinite pro-p groups all of whose proper quotients are finite (see Definition 2.4.12). One can show that just-infinite pro-p groups are always finitely generated (see [K1], Exercise 9.4).

Proposition 3.4.1. *Let G be a just-infinite insoluble pro-p group. Then every non-trivial normal subsemigroup of G is an open normal subgroup of G.*

Remark 3.4.2. Compare with [JZ], Proposition 1.1: Let G be a just-infinite pro-p group. Then G is insoluble if and only if every non-trivial abstract normal subgroup of G is open. This result yields that insoluble just-infinite pro-p groups are also just-infinite as abstract groups.

Before proving this proposition we need a standard lemma; we present the proof for completeness (see for example [Wr], Theorem I).

Lemma 3.4.3. *Let S be a closed non-empty subsemigroup of a profinite group. Then S is a group.*

Proof. We start by proving the so-called Ellis-Numakura lemma, that states that a compact Hausdorff non-empty semigroup T such that the product is continuous has at least one idempotent element, i.e., an element x such that $x^2 = x$. By applying Zorn's lemma to the family of non-empty compact sub-semigroups of T we can find a minimal subsemigroup in this family, with which we can replace T. Take x in T and consider the set Tx. As the product is continuous, Tx is again compact and is clearly a semigroup contained in T. By minimality we can therefore conclude that $Tx = T$. In particular, the subset A of T containing elements y that satisfy $yx = x$ is not empty and forms a compact subsemigroup of T (it is the inverse image of the closed set $\{x\}$ under the continuous map $T \to T$ that maps any y in T to yx). Again by minimality we can conclude that $A = T$ and therefore A contains x, hence $x^2 = x$.

Now consider S: being closed in a compact Hausdorff group it is compact and Hausdorff and its operation is continuous since it is inherited by the one in the topological group. For the same reason the only idempotent contained in S is the identity. Therefore, applying the Ellis-Numakura lemma we find that S contains the identity, hence it is a group. Indeed, for every $x \in S$, xS and Sx are compact Hausdorff non-empty semigroups and therefore, by using the Ellis-Numakura lemma, they contain the identity. □

Proof of Proposition 3.4.1. Let S be a normal subsemigroup of G and let T be its closure in G (i.e., the smallest closed subsemigroup of G containing S).
Since, as we have seen in the previous lemma, a closed subsemigroup of a profinite group is a group, T is actually a closed normal subgroup of G.
Hence $T = \overline{(S)}_{\text{semigp}} = \overline{\langle S \rangle}$. Since G is just-infinite, T has finite index in G, thus it is open (as it is closed of finite index). Since G is finitely generated, there are elements $x_1, \dots, x_d \in S$ such that $T = \overline{\langle x_1, \dots, x_d \rangle}$.

Since G is insoluble, the commutator subgroup $[T,T]$ is open. Indeed, there are two possibilities:

1. $[T,T] = 1$ implies that T is abelian. Since moreover G/T is a finite p-group (hence nilpotent), G is soluble in this case, a contradiction.

2. $[T,T] \neq 1$. The commutator subgroup $[T,T]$ is a closed subgroup of G because T is a finitely generated pro-p group, $[T,T]$ is closed in T and T is closed in G. Hence $[T,T]$ is open in the just-infinite group G.

We claim that $x_d x_{d-1} \cdots x_1 [T,T] \subseteq x_1^T x_2^T \cdots x_d^T \subseteq S$; more precisely, we prove by induction on $d \geq 1$ that

$$x_d x_{d-1} \cdots x_1 [x_1, t_1] \cdots [x_d, t_d] = x_1^{t_1 x_2^{-1} \cdots x_d^{-1}} x_2^{t_2 x_3^{-1} \cdots x_d^{-1}} \cdots x_d^{t_d}.$$

Indeed, recall that every element of $[T,T]$ is of the form $[x_1, t_1] \cdots [x_d, t_d]$ for $t_1, \dots, t_d$ elements of T (Proposition 1.2.2). For $d = 1$ one has

$$x_1 [x_1, t_1] = x_1^{t_1}.$$

Suppose now that the formula holds for $d-1$, i.e.,

$$x_{d-1} x_{d-2} \cdots x_1 [x_1, t_1] \cdots [x_{d-1}, t_{d-1}] = x_1^{t_1 x_2^{-1} \cdots x_{d-1}^{-1}} x_2^{t_2 x_3^{-1} \cdots x_{d-1}^{-1}} \cdots x_{d-1}^{t_{d-1}}.$$

For every integer m with $d > m \geq 1$, set $y_m := x_d x_{d-1} \cdots x_m$. With this notation our claim becomes

$$y_1 [x_1, t_1] \cdots [x_d, t_d] = x_1^{t_1 y_2^{-1}} x_2^{t_2 y_3^{-1}} \cdots x_d^{t_d}.$$

We have

$$\begin{aligned} y_1 [x_1, t_1] \cdots [x_d, t_d] &= x_d x_1^{t_1 y_2^{-1} x_d} x_2^{t_2 y_3^{-1} x_d} \cdots x_{d-1}^{t_{d-1}} [x_d, t_d] \\ &= (x_d x_1^{t_1 y_2^{-1} x_d} x_d^{-1})(x_d x_2^{t_2 y_3^{-1} x_d} x_d^{-1}) \cdots (x_d x_{d-1}^{t_{d-1}} x_d^{-1}) x_d^{t_d} \\ &= x_1^{t_1 y_2^{-1}} x_2^{t_2 y_3^{-1}} \cdots x_d^{t_d}. \end{aligned}$$

Since $[T,T]$ has finite index in G, there exists $k \in \mathbb{N}$ such that the element $(x_d x_{d-1} \cdots x_1)^{p^k}$ belongs to $[T,T]$, from which it follows that

$$\begin{aligned}[T,T] &= (x_d x_{d-1} \cdots x_1)^{p^k}[T,T] \\ &= (x_d x_{d-1} \cdots x_1)^{p^{k-1}} x_d x_{d-1} \cdots x_1 [T,T] \\ &\subseteq (x_d x_{d-1} \cdots x_1)^{p^{k-1}} x_1^T \cdots x_d^T \subseteq S.\end{aligned}$$

Now, let $S/[T,T]$ denote the quotient semigroup with respect to the semigroup congruence relation $\sim$ defined by $s_1 \sim s_2$ if and only if there is an element $t \in [T,T]$ such that $s_1 = s_2 t$. Recall that a semigroup congruence on the semigroup S is an equivalence relation $\sim'$ such that, if s_1, s_2, s_3, s_4 are elements of S such that $s_1 \sim' s_2$ and $s_3 \sim' s_4$, then $s_1 s_3 \sim' s_2 s_4$. It is clear that $\sim$ is an equivalence relation and, if $s_1 \sim s_2$ and $s_3 \sim s_4$ then there exist t_1, t_2 in $[T,T]$ such that $s_1 = s_2 t_1$ and $s_3 = s_4 t_2$. Then $s_1 s_3 = s_2 t_1 s_4 t_2 = s_2 s_4 t_3 t_2$ for some $t_3 \in [T,T]$ and so $s_1 s_3 \sim s_2 s_4$. Hence $S/[T,T]$ is a subsemigroup of $G/[T,T]$, which is a finite group. Since a semigroup in a finite group is a group, S is a group and it contains the open subgroup $[T,T]$, from which we can deduce that S is an open normal subgroup of G.

□

Corollary 3.4.4. *Let G be a just-infinite insoluble pro-p group. Then G is not bi-orderable.*

Proof. Assume that G is bi-orderable and let S be the subsemigroup of positive elements of G. Since S is normal, by the previous proposition S is a subgroup of G. This yields a contradiction as, if $x \in S$, then $x > 1$ and $x^{-1} < 1$ cannot belong to S. □

Corollary 3.4.5. *Let G be a non-soluble p-adic analytic pro-p group. Then G is not bi-orderable.*

In order to prove this corollary, we need to use the Lie correspondence between uniform pro-p groups and powerful $\mathbb{Z}_p$-Lie lattices. Recall from Chapter 1, Section 1.3 that, if G is a pro-p of finite rank and U is any of its open uniform subgroups, then the $\mathbb{Q}_p$-Lie algebra associated to G is given by $\mathfrak{L} := L(U) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, where $L(U)$ is the powerful $\mathbb{Z}_p$-Lie lattice associated to U. For proving our result we will need the following

Proposition 3.4.6. *Let G be a non-soluble pro-p group of finite rank and let $\mathfrak{H}$ be a simple Lie subalgebra of the Lie algebra associated to G. Then G has a uniform subgroup H which is non-abelian just-infinite and whose associated Lie algebra is $\mathfrak{H}$.*

Proof. Let U be a uniform open subgroup of G and $L(U)$ the corresponding $\mathbb{Z}_p$-Lie lattice. The intersection $L(U) \cap \mathfrak{H} =: L$ is a non-empty $\mathbb{Z}_p$-Lie lattice such that $L \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = \mathfrak{H}$. As recalled in Chapter 1, Section 1.3, if p is odd (if $p = 2$ respectively), then p (respectively $4L$) is a powerful $\mathbb{Z}_p$-Lie sublattice of $L(U)$ and therefore corresponds to a uniform subgroup H of U. The Lie algebra of H is $\mathfrak{L}_H = pL \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = L \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = \mathfrak{H}$ (respectively, $4L \otimes_{\mathbb{Z}_2} \mathbb{Q}_2 = \mathfrak{H}$) and is therefore simple.

We now show that H is just-infinite. If this was not the case, we could find a closed normal subgroup N of H of infinite index. Consider the powerful pro-p group H/N. By Theorem 1.3.12, the torsion subgroup T/N of H/N is a finite characteristic subgroup and $\frac{H/N}{T/N} \cong H/T$ is uniform. As both H and H/T are uniform, by Theorem 1.3.14, T is a normal uniform subgroup of H of infinite index and $L(T)$ is a $\mathbb{Z}_p$-Lie ideal of L of infinite index. Then $\mathfrak{L}_T = L(T) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is a proper ideal of $\mathfrak{L}_H = \mathfrak{H}$, which contradicts the fact that $\mathfrak{H}$ is simple. □

Proof of Corollary 3.4.5. Let U be a uniform open normal subgroup of G and let $\mathfrak{L} := L(U) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ be the Lie algebra associated to G. By Levi's decomposition theorem ([Serre1], Part I, Chapter VI, Corollary 4.1), $\mathfrak{L} = \mathfrak{H} \ltimes \mathfrak{R}$, where $\mathfrak{H}$ is a non-trivial semisimple Lie subalgebra of $\mathfrak{L}$ and $\mathfrak{R}$ is the soluble radical of $\mathfrak{L}$. Then $\mathfrak{H}$ can be written as $\mathfrak{H} = \mathfrak{H}_1 \oplus \ldots \oplus \mathfrak{H}_m$, where each $\mathfrak{H}_i$ is a simple Lie algebra ([Serre1], Part I, Chapter VI, Corollary 2.1). For each i, set $L_i := \mathfrak{H}_i \cap L(U)$. By the previous proposition, each pL_i corresponds to a non-abelian just-infinite subgroup H_i of G. As, by Corollary 3.4.4, each H_i is not bi-orderable, we can conclude that G is not bi-orderable. □

Remark 3.4.7. By using some of the previous arguments, we can conclude that any bi-orderable finitely generated pronilpotent group has infinite abelianisation. Indeed, let G be a bi-orderable finitely generated pronilpotent group, with generators $x_1, \ldots, x_d$ chosen to be positive for a fixed bi-order on G. Let S be the normal subsemigroup of G generated by $x_1, \ldots, x_d$ and T its closure. By the same reasoning used in the proof of Proposition 3.4.1 we see that $T = G$. Assume that G is non-abelian and that $[G, G]$ has finite index in G. Again proceeding as in the proof of Proposition 3.4.1, we can conclude that

$$x_d x_{d-1} \cdots x_1 [G, G] \subseteq x_1^G x_2^G \cdots x_d^G \subseteq S \tag{3.2}$$

and that, for some positive integer m,

$$[G, G] = (x_d x_{d-1} \cdots x_1)^m [G, G] = (x_d x_{d-1} \cdots x_1)^{m-1} (x_d x_{d-1} \cdots x_1)[G, G] \subseteq$$
$$\subseteq (x_d x_{d-1} \cdots x_1)^{m-1} x_1^G x_2^G \cdots x_d^G \subseteq S.$$

As S contains only positive elements because G is bi-orderable, we can argue as in the proof of Corollary 3.4.4 to find a contradiction. It follows that any bi-orderable finitely generated pronilpotent group must have infinite abelianisation. In particular, this gives an alternative proof of Corollary 3.4.4.
(Alternatively, one can assume that G is bi-orderable and take $S = P$ the semigroup of positive elements of G, thus obtaining the same contradiction.)

Note that we actually proved something more, namely that, if $G = \prod_p G_p$ is a bi-orderable finitely generated pronilpotent group, then G maps onto $\mathbb{Z}_p$ for each p such that G_p is non-trivial. Indeed, each such G_p is a bi-orderable finitely generated pro-p group, hence in particular it has infinite abelianisation and therefore it maps onto $\mathbb{Z}_p$. Composing this map with the natural projection $G \to G_p$ one gets the required surjective homomorphism.

Note also that, if G is a bi-orderable finitely generated pronilpotent group with generators $x_1, \ldots, x_d$, by (3.2) every element of the form $x_d x_{d-1} \cdots x_1 z$ with $z \in [G, G]$ is positive. It is clear that the same is true for any permutation of $x_1, \ldots, x_d$ and that, given any positive integers $\alpha_1, \ldots, \alpha_d$ with $\alpha_i \geq 1$ for all $i \in \{1, \ldots, d\}$,

also $x_d^{\alpha_d} x_{d-1}^{\alpha_{d-1}} \cdots x_1^{\alpha_1}[G,G] = x_d^{\alpha_d - 1} x_{d-1}^{\alpha_{d-1}-1} \cdots x_1^{\alpha_1 - 1} x_d x_{d-1} \cdots x_1 [G,G] \subseteq P$.
It follows that the elements of the form $x_d^{\alpha_d} x_{d-1}^{\alpha_{d-1}} \cdots x_1^{\alpha_1}$ with the exponents α_i as before and any permutation of them are greater or equal than any element of $[G,G]$.

From the previous remark we can conclude that also soluble non-abelian just-infinite pro-p groups are not bi-orderable, as bi-orderable pronilpotent groups have infinite abelianisation. The same result can also be deduced less directly from Proposition 6.1 in [GSK], which states that every soluble just-infinite pro-p group other than $\mathbb{Z}_p$ has torsion.

3.5 Orderability of pro-p RAAGs

In this section we prove that the class of bi-orderable pro-p groups contains a large supply of interesting groups by proving that pro-p RAAGs are bi-orderable. In particular, pro-p groups belonging to this class satisfy the unique product property.

A *right-angled Artin group* (RAAG), or *free partially commutative group*, is an abstract group $F(A,\theta)$ with the following presentation: let A be a finite set and θ a symmetric and irreflexive subset of $A \times A$ (a *partial commutation relation*), then

$$F(A,\theta) := \langle A \mid \ ab = ba, (a,b) \in \theta \rangle. \tag{3.3}$$

We note that, if we consider the limit case where $\theta = (A \times A) \setminus \Delta(A)$ with $\Delta(A) := \{(a,a) \mid a \in A\}$, we get the free abelian group on the set A, while, if $\theta = \emptyset$, we get the free group on A.
It is known that RAAGs are bi-orderable groups (see for example [R2] or [DK]).

We now consider the presentation given by (3.3) as a pro-p presentation, and we call the pro-p group with this presentation a pro-p RAAG. This pro-p group, that we will denote $F(A,\theta)_{\text{pro-}p}$, is the pro-$p$ completion of the abstract right-angled Artin group $F(A,\theta)$.
By slightly modifying one of the proofs of the bi-orderability of RAAGs given in [DK], we prove that also pro-p RAAGs are bi-orderable.
For all the following definitions and constructions in the abstract case see [DK], where the same are carried out for a generic non-trivial ring of coefficients.

Let A be the set consisting of the variables $X_1, \ldots, X_n$ and let θ be a symmetric and irreflexive subset of $A \times A$. We consider the partially commutative formal power series ring $\mathbb{Z}_p[[X_1, \ldots, X_n; \theta]]$, consisting of the formal power series in the variables $X_1, \ldots, X_n$ with coefficients in $\mathbb{Z}_p$ where two variables X_i and X_j commute if and only if $(X_i, X_j) \in \theta$, for $i, j \in \{1, \ldots, n\}$.
A series in $\mathbb{Z}_p[[X_1, \ldots, X_n; \theta]]$ has the form $S = \sum_{\mathbf{X}} \lambda_{\mathbf{X}} \mathbf{X}$, where $\lambda_{\mathbf{X}} \in \mathbb{Z}_p$ and $\mathbf{X}$ runs over a set of representatives of the semigroup M generated by the variables $X_1, \ldots, X_n$ and subject to the relations $X_i X_j = X_j X_i$ whenever $(X_i, X_j) \in \theta$, for $i, j \in \{1, \ldots, n\}$.
The *support* of such a series S is given by the set of monomials $\mathbf{X}$ occurring in S with non-zero coefficient. Given a monomial $\mathbf{X} = X_{i_1} \cdots X_{i_m}$, the *length* of $\mathbf{X}$ is the number of variables m occurring in $\mathbf{X}$. The *valuation* $\nu(S)$ of a series S is

the minimal length of the elements in the support of S. Thanks to this valuation it is possible to define a filtration on $\mathbb{Z}_p[[X_1, \ldots, X_n; \theta]]$ as follows:

$$\forall k \in \mathbb{N},\ \ \mathbb{Z}_p[[X_1, \ldots, X_n; \theta]]_k := \{S \in \mathbb{Z}_p[[X_1, \ldots, X_n; \theta]] :\ \nu(S) \geq k\}.$$

The *augmentation ideal* of $\mathbb{Z}_p[[X_1, \ldots, X_n; \theta]]$ is given by

$$M(n; \theta) := M(X_1, \ldots X_n; \theta) := \mathbb{Z}_p[[X_1, \ldots, X_n; \theta]]_1,$$

i.e., by the set of series that do not have a non-zero constant term, and the *partially commutative Magnus group* is defined as

$$Mg(n; \theta) = Mg(X_1, \ldots X_n; \theta) := 1 + M(n, \theta),$$

i.e., the set of series with constant term 1, with group operation given by multiplication. $Mg(n; \theta)$ has a filtration inherited from the valuation filtration of the partially commutative formal power series ring; we write

$$Mg(n; \theta)_k := 1 + \mathbb{Z}_p[[X_1, \ldots, X_n; \theta]]_k$$

for every $k \geq 1$.

Consider the product $\mathbb{Z}_p^{\mathcal{T}(\{1,\ldots,n\})}$, where $\mathcal{T}(\{1, \ldots, n\})$ is a set of tuples of natural numbers in $\{1, \ldots, n\}$ that is in bijection with the set of monomials of $\mathbb{Z}_p[[X_1, \ldots, X_n; \theta]]$ via $X_{i_1} \cdots X_{i_m} \mapsto (i_1, \ldots, i_m)$. Note that some of these tuples are identified according to the partial commutation relation θ. For example, if X_1 and X_2 commute, then $(1, 2) = (2, 1)$. There is a map from $\mathbb{Z}_p[[X_1, \ldots, X_n; \theta]]$ to $\mathbb{Z}_p^{\mathcal{T}(\{1,\ldots,n\})}$ that sends a series to the sequence of its coefficients. We put on $\mathbb{Z}_p[[X_1, \ldots, X_n; \theta]]$ the topology of simple convergence of the coefficients (i.e., the product topology on copies of $\mathbb{Z}_p$ indexed by monomials in the variables $X_1, \ldots, X_n$); in other words, a sequence of series in $\mathbb{Z}_p[[X_1, \ldots, X_n; \theta]]$ converges with respect to this topology if and only if, for each monomial $\mathbf{X}$, the sequence of coefficients of $\mathbf{X}$ converges in the product topology. Let I be the maximal ideal of $\mathbb{Z}_p[[X_1, \ldots, X_n; \theta]]$. It is a known fact that the I-adic topology ([DDMS] Chapter 6, Section 6) on $\mathbb{Z}_p[[X_1, \ldots, X_n; \theta]]$ is equivalent to the topology of simple convergence of the coefficients described before. We sketch the idea of the proof of this fact for completeness.

Lemma 3.5.1. *The I-adic topology and the topology of simple convergence of the coefficients on $\mathbb{Z}_p[[X_1, \ldots, X_n; \theta]]$ are equivalent.*

Proof. As the topology of simple convergence of the coefficients is the same as the product topology on $\mathbb{Z}_p^{\mathcal{T}(\{1,\ldots,n\})}$, a basis for this topology is given by the open sets $\{U_k\}_{k \in \mathbb{N}}$, where each U_k is of the form

$$U_k = \prod_{i=1}^{k} \tilde{U}_i \times \prod_{i=k+1}^{|\mathcal{T}(\{1,\ldots,n\})|} \mathbb{Z}_p,$$

with $\tilde{U}_i$ open subsets of $\mathbb{Z}_p$. Recall that an open set in $\mathbb{Z}_p$ is given by $p^m\mathbb{Z}_p$ for some natural number m. When looking at series, this means that an open set of this basis contains series with k coefficients that belong to open sets of $\mathbb{Z}_p$. A

basis of open sets for the I-adic topology is given by translates of powers of I, i.e. by the sets

$$\{x + I^h \mid x \in \mathbb{Z}_p[[X_1, \ldots, X_n; \theta]], h \in \mathbb{N}\}.$$

It is now not difficult to check that a set is open in the I-adic topology if and only if it is open in the topology of simple convergence of the coefficients.

□

As a consequence, with the topology of simple convergence of the coefficients, $\mathbb{Z}_p[[X_1, \ldots, X_n; \theta]]$ is a complete $\mathbb{Z}_p$-module in the sense of Lazard, since, considered with the I-adic topology, it is a topological $\mathbb{Z}_p$-module that is complete and has a basis of neighbourhoods of zero given by its open submodules (see [La], Chapter II, Section 2, (2.2.4)). The Magnus group $Mg(n; \theta)$ inherits the subspace topology, that turns it into a pro-p group; this group is topologically generated by the monomials $1 + X_1, \ldots, 1 + X_n$.

Now consider the pro-p RAAG $F(n; \theta)_{\text{pro-}p} := F(x_1, \ldots, x_n; \theta)_{\text{pro-}p}$, where $F(x_1, \ldots, x_n; \theta)_{\text{pro-}p}$ is the pro-p group with pro-p presentation

$$\langle x_1, \ldots, x_n;\ x_i x_j = x_j x_i \text{ for } i, j \in \{1, \ldots, n\} \text{ and } (x_i, x_j) \in \theta \rangle_{\text{pro-}p}.$$

It is clear that $F(n; \theta)_{\text{pro-}p}$ is a free partially commutative pro-p group.

We are going to show that the continuous homomorphism $\mu : F(n; \theta)_{\text{pro-}p} \to Mg(n; \theta)$, defined by $x_i \mapsto 1 + X_i$ ($i \in \{1, \ldots, n\}$), is injective. This slightly generalises a result of Lazard, where the previous statements are proved in the case of a free pro-p group; the proofs in the partially commutative case are very similar to the ones in the free case. See [La], Chap. II, Section 3.1.

Lemma 3.5.2. *The Magnus homomorphism $\mu : F(n; \theta)_{pro\text{-}p} \to Mg(n; \theta)$ is an injective continuous homomorphism of pro-p groups.*

Proof. First of all we note that the homomorphism $\mu : F(n; \theta)_{\text{pro-}p} \to Mg(n; \theta)$ defined by $\mu(x_i) := 1 + X_i$ is well defined because of the universal property of relatively free groups.

Let $\mathbb{Z}_p[[F(n; \theta)_{\text{pro-}p}]]$ be the completed group algebra of $F(n; \theta)_{\text{pro-}p}$. This is also a $\mathbb{Z}_p$-complete module in the sense of Lazard ([La], Chapter II, Section 2, Example (2.2.4.1)). Since $\mathbb{Z}_p[[X_1, \ldots, X_n; \theta]]$ is a complete $\mathbb{Z}_p$-module, there exists a unique morphism $\alpha : \mathbb{Z}_p[[F(n; \theta)_{\text{pro-}p}]] \to \mathbb{Z}_p[[X_1, \ldots, X_n; \theta]]$ which extends μ (see [La], Chapter II, Section 2, Lemma 2.2.5).
We construct the inverse of α as $\beta : \mathbb{Z}_p[[X_1, \ldots, X_n; \theta]] \to \mathbb{Z}_p[[F(n; \theta)_{\text{pro-}p}]]$ that sends X_i to $x_i - 1$. This is well-defined since the powers of the ideal generated by the $x_i - 1$ tend to zero in the completed algebra $\mathbb{Z}_p[[F(n; \theta)_{\text{pro-}p}]]$ (see [La], Chapter II, Section 2, 2.2.3). This implies that μ, being the restriction of the bijective morphism α, is injective.

□

We will now use the following

Theorem 3.5.3 ([DK], Section 3, Theorem 3.1)**.** *Let G be a group with a filtration $(G_k)_{k \geq 1}$ of normal subgroups with the following properties:*

1. $\forall\, k \geq 1,\ \forall\, g \in G,\ \forall\, s \in G_k,\ \exists\, h \in G_k :\ [hg, s] \in G_{k+1}$

2. $G_1 = G$

3. $\bigcap_{k\geq 1} G_k = \{1\}$

Suppose that every quotient G_k/G_{k+1} is bi-orderable. Then G is bi-orderable.

In the case of pro-p groups we will need to add the requirement that the G_k are *closed* subgroups of G.

One can verify that the valuation filtration of the Magnus group satisfies all the hypotheses of the previous theorem. Since, for every $k \geq 1$, the quotients $Mg(n;\theta)_k/Mg(n;\theta)_{k+1}$ are isomorphic to the product of a finite number of copies of $(\mathbb{Z}_p, +)$ and $(\mathbb{Z}_p, +)$, being torsion-free abelian, is bi-orderable (see Example 3.2.13), it follows that $Mg(n;\theta)$ is bi-orderable. Alternatively, it is also possible to construct a bi-order on the Magnus group. Namely, one can fix a bi-order on the additive group $\mathbb{Z}_p$ and an order on monomials and declare a power series U greater than a power series V if the coefficient of the first monomial of U at which U and V differ is greater than the corresponding coefficient of V (see [CR], Chapter 3, Section 3.2). In any case, the pro-p group $F(n;\theta)_{\text{pro-}p}$ can be ordered via the injective homomorphism μ.

Note that it would also be possible to work directly with the lower central series of $F(n,\theta)_{\text{pro-}p}$ and show that each of its factors is torsion-free abelian. As the groups forming the lower central series of $F(n,\theta)_{\text{pro-}p}$ clearly satisfy the conditions in Theorem 3.5.3, this would give an alternative proof of the bi-orderability of $F(n,\theta)_{\text{pro-}p}$ (compare with [DK], Theorem 2.1).

In [Ch], Chong-Keang replaces $\mathbb{Z}_p$ with $\widehat{\mathbb{Z}}$ and considers the formal power series ring $\widehat{\mathbb{Z}}[[X_1,\ldots,X_n]]$. In this case, the closed multiplicative subgroup of $\widehat{\mathbb{Z}}[[X_1,\ldots,X_n]]$ generated by $1+X_1,\ldots,1+X_n$ turns out to be the free pronilpotent group on n generators. By modifying the previous argument we therefore find that free partially commutative pronilpotent groups are bi-orderable.

Hence, as bi-orderable groups are locally indicable, we can conclude that free (partially commutative) pronilpotent groups are locally indicable. It is an open problem to determine whether this holds true in the case of free profinite groups. Jaikin-Zapirain conjectures that all finitely generated free profinite groups are indeed locally indicable ([JZ2], Conjecture 4).

3.6 Some further questions

We collect here some questions that arise naturally by what was done so far.

The first obvious question is whether it is possible to fully prove the conjecture posed by Craig and Linnell, which states that every uniform pro-p group has the unique product property, or, alternatively, provide a counterexample. It seems to us that this is not immediately possible to accomplish with the methods used in this thesis.

Another less ambitious direction would be to try to extend the results in Section 3.3 to other classes of (soluble) profinite groups. Moreover, in Corollary 3.3.19 we saw a characterisation of (abstractly) locally indicable groups within the class of metabelian profinite groups with the ascending chain condition on closed subgroups. It remains open to find a similar characterisation of locally

indicable groups in the class of profinite groups of finite rank, at least in the soluble case.

Task 3.6.1. *Find a characterisation of locally indicable groups in the class of soluble profinite groups of finite rank.*

More generally, it would be interesting to study local indicability in the realm of profinite groups; an already cited open conjecture in this regard is that all finitely generated free profinite groups are locally indicable ([JZ2], Conjecture 4).

Regarding orderability, we saw at the beginning of Section 3.4 that soluble non-nilpotent uniform groups of rank 2 are not bi-orderable. It is natural to ask whether it is possible to extend this result to soluble non-nilpotent uniform groups of higher rank, i.e.,

Question 3.6.2. *Are soluble non-nilpotent uniform groups of rank higher than* 2 *not bi-orderable?*

Still related to orderability it is natural to ask the following:

Question 3.6.3. *Are insoluble saturable groups right-orderable?*

It might be the case that these groups possess the unique product property but are not right-orderable. Moreover, it would be interesting to study the space of right-orders on soluble saturable groups. Finally, it is known that there is no order on p-adic analytic pro-p groups that is compatible with both the profinite topology and the group operation. It would then be natural to examine the topology induced by an order and compare it with the profinite topology. We also want to mention that many known results on orderability of groups concern countable groups; it would be an interesting task to think about which of these results can be translated to the realm of profinite groups. For example, it seems to us that one of the results regarding the structure of bi-orderable soluble groups proved by Botto Mura and Rhemtulla ([BMR], Lemma 3.3.2) can be adapted to the pro-p case.

Finally, regarding the relations among the unique product property and the various kinds of orderability (see the end of Section 3.2.2), one might ask the following question, which was posed to me by Olga Varghese.

Question 3.6.4. *Are there some classes of groups (for example, metabelian groups) for which the unique product property is equivalent to right-orderability?*

Also, it is clear that taking the profinite (or pro-p) completion of the group G in Remark 3.2.16 we obtain a profinite (respectively, pro-p) group that is right-orderable but not bi-orderable. Therefore it would be good to carry out the following task.

Task 3.6.5. *Find an example of a profinite group that is locally indicable but not right-orderable.*

3.7 Appendix

In this section we prove a commutator formula for nilpotent groups similar to the one in the proof of Proposition 3.4.1. More precisely, let G be a (pronilpotent

or abstract) nilpotent group of nilpotency class c generated by $x_1, \ldots, x_d$, let $a_1, \ldots, a_d$ be integers and $t_1, \ldots t_d$ be elements of G. Then

$$x_1^{a_1} x_2^{a_2} \cdots x_d^{a_d} [x_1, t_1][x_2, t_2] \cdots [x_d, t_d] = x_1^{b_1} x_1^{g_1^{(1)}} \cdots x_1^{g_{k_1}^{(1)}} \cdots x_d^{b_d} x_d^{g_1^{(d)}} \cdots x_d^{g_{k_d}^{(d)}},$$

where, for each $i \in \{1, \ldots, d\}$, b_i is an integer such that $a_i - 1 \geq b_i \geq a_i - c + 1$, $k_i \leq c - 1$ and $g_1^{(i)}, \ldots, g_{k_i}^{(i)}$ are elements of G.

We prove this formula by induction on the nilpotency class c of G.
Let $c = 2$. When $d = 2$ we have:

$$x_1^{a_1} x_2^{a_2} [x_1, t_1][x_2, t_2] = x_1^{a_1} [x_1, t_1] x_2^{a_2} [x_2^{a_2}, [x_1, t_1]][x_2, t_2] = x_1^{a_1 - 1} x_1^{t_1} x_2^{a_2 - 1} x_2^{t_2},$$

as $c = 2$ implies $[x_2^{a_2}, [x_1, t_1]] = 1$. Similarly, for $d > 2$ we get

$$\begin{aligned} & x_1^{a_1} x_2^{a_2} \cdots x_d^{a_d} [x_1, t_1][x_2, t_2] \cdots [x_d, t_d] \\ & = x_1^{a_1} [x_1, t_1] x_2^{a_2} [x_2, t_2] \cdots x_d^{a_d} [x_d, t_d] \\ & = x_1^{a_1 - 1} x_1^{t_1} x_2^{a_2 - 1} x_2^{t_2} \cdots x_d^{a_d - 1} x_d^{t_d}, \end{aligned}$$

as all commutators $[x_i^{a_i}, [x_j, t_j]]$ vanish.

Assume now that the formula holds for the nilpotency class $c \geq 2$ and let G be of class $c + 1$. Quotienting by $\gamma_{c+1}(G)$ we get a nilpotent group of class c and therefore

$$x_1^{a_1} x_2^{a_2} \cdots x_d^{a_d} [x_1, t_1][x_2, t_2] \cdots [x_d, t_d] = x_1^{b_1} x_1^{g_1^{(1)}} \cdots x_1^{g_{k_1}^{(1)}} \cdots x_d^{b_d} x_d^{g_1^{(d)}} \cdots x_d^{g_{k_d}^{(d)}} z,$$

where $z \in \gamma_{c+1}(G)$ and the conditions on the b_i's, k_i's and $g_j^{(i)}$'s are as before. Now z can be written as

$$z = \prod_{\underline{i} \in \{1, \ldots, d\}^c} [x_{i_1}, x_{i_2}, \ldots, x_{i_c}, t_{\underline{i}}],$$

with $\underline{i} = (i_1, \ldots, i_c)$ and $t_{\underline{i}} \in G$ (see [Se] Corollary 1.2.8). As G has class $c + 1$, each commutator $[x_{i_1}, x_{i_2}, \ldots, x_{i_c}, t_{\underline{i}}]$ is central in G. Moreover, again because we are in class $c + 1$ we have

$$[x_{i_1}, x_{i'_2}, \ldots, x_{i'_c}, t_{\underline{i}'}][x_{i_1}, x_{i_2}, \ldots, x_{i_c}, t_{\underline{i}}] = [x_{i_1}, [x_{i_2}, \ldots, x_{i_c}, t_{\underline{i}}][x_{i'_2}, \ldots, x_{i'_c}, t_{\underline{i}'}]].$$

Therefore we get

$$x_1^{a_1} x_2^{a_2} \cdots x_d^{a_d} [x_1, t_1][x_2, t_2] \cdots [x_d, t_d] = x_1^{b'_1} x_1^{g_1^{\prime(1)}} \cdots x_1^{g_{k'_1}^{\prime(1)}} \cdots x_d^{b'_d} x_d^{g_1^{\prime(d)}} \cdots x_d^{g_{k'_d}^{\prime(d)}},$$

where, for each $i \in \{1, \ldots, d\}$, $b'_i \leq b_i \leq a_i - 1$, $b'_i \geq b_i - 1 \geq a_i - (c + 1) + 1$, $k'_i \leq k_i + 1 \leq c$ and $g_1^{\prime(i)}, \ldots, g_{k_i}^{\prime(i)}$ are elements of G. This proves the formula.

Bibliography

[BJZK] Barnea Y., Jaikin-Zapirain A., Klopsch B., *Abstract versus topological extensions of profinite groups*, unpublished manuscript

[Be] Benoist Y., *Five lectures on lattices in semisimple Lie groups* in *Géométries à courbure négative ou nulle, groupes discrets et rigidités*, 117–176, Sémin. Congr., 18, Société Mathématique de France, Paris, 2009

[BMR] Botto Mura R. T., Rhemtulla A. H., *Orderable groups*, Lecture Notes in Pure and Applied Mathematics, Vol. 27, Marcel Dekker Inc., New York-Basel, 1977

[Ba] Barwise J., *An introduction to first-order logic* in *Handbook of mathematical logic*, 5-46, Stud. Logic Found. Math., 90, North-Holland, Amsterdam, 1997

[B] Bowditch B. H., *A variation on the unique product property*, J. London Math. Soc. (2) 62 (2000), no. 3, 813-826

[C] Carter, R. W., *Simple groups of Lie type*, Pure and Applied Mathematics Vol. 28, John Wiley & Sons, London-New York-Sydney, 1972

[Ca] Carter, W., *New examples of torsion-free non-unique product groups*, J. Group Theory 17 (2014), no.3, 445–464

[Ch] Chong-Keang, L., *A corollary to Lazard's theorem on pro-p-groups*, J. London Math. Soc., (2) 6 (1973), 570

[CR] Clay A., Rolfsen D., *Ordered groups and topology*, Graduate Studies in Mathematics, 176. American mathematical Society, Providence, RI, 2016

[C] Conrad P., *Right-ordered groups*, Michigan Math. J. **6** (1959), 267-275

[CK] Conte M., Klopsch B., *Finite axiomatizability of the rank and the dimension of a pro-π group*, arXiv preprint, arXiv:2304.02504v2, 2023

[CW] Cornulier Y., Wilson J. S., *First-order recognizability in finite and pseudofinite groups*, J. Symb. Log. 85 (2020), no. 2, 852-867

[CL] Craig W., Linnell P. A., *Unique product groups and congruence subgroups*, J. Algebra Appl. 21 (2022), no. 2, Paper No. 2250025, 9 pp

[CBKL] Crawley-Boevey, W. W., Kropholler, P. H., Linnell, P. A., *Torsion-free soluble groups, completions, and the zero divisor conjecture*, J. Pure Appl. Algebra 54 (1988), no. 2-3, 181–196

[DDMS] Dixon J. D., du Sautoy M. P. F., Mann A., Segal D., *Analytic pro-p groups*, volume 61 of Cambridge Studies in Advanced Mathematics, CUP, second edition, 1999

[DNR] Deroin B., Navas A., Rivas C., *Groups, Orders, and Dynamics*, arXiv preprint, arXiv:1408.5805v2, 2016

[DK] Duchamp G., Krob D., *The lower central series of the free partially commutative group*, Semigroup Forum Vol. 45 (1992) 385-394

[E] Eklof P. C., *Ultraproducts for algebraists* in *Handbook of mathematical logic*, 105-137, Stud. Logic Found. Math., 90, North-Holland, Amsterdam, 1997

[F] Farkas, D. R., *Crystallographic groups and their mathematics*, Surfaces (Stanford, Calif., 1982), Rocky Mountain J. Math. 11 (1981), no.4, 511-551

[FL] Farkas, D. R., Linnell, P. A., *Congruence subgroups and the Atiyah conjecture* in *Groups, rings and algebras*, 89–102, Contemp. Math., 420, American Mathematical Society, Providence, RI, 2006

[FA] Fernández-Alcober G. A., *Omega subgroups of powerful p-groups*, Israel J. Math. **162** (2007), 75-79

[FV] Feferman S., Vaught R. L., *The first order properties of products of algebraic systems*, Fund. Math. 47 (1959), 57-103

[G] Gardam G., *A counterexample to the unit conjecture for group rings.* Ann. of Math. (2) 194 (2021), no.3, 967–979

[GS] González-Sánchez J., *On p-saturable groups*, Journal of Algebra, **315** (2007), 809-823

[GSK] González-Sánchez J., Klopsch B., *Analytic pro-p groups of small dimensions*, J. Group Theory **12** (2009), 711-734

[HL] Héthelyi L., Lévai L., *On elements of order p in powerful p-groups*, J. Algebra **270** (2003), 1-6

[H] Hirshon R., *Some cancellation theorems with applications to nilpotent groups*, J. Austral. Math. Soc. Ser. A23 (1977), no.2, 147–165

[Ki] Kiehlmann J. A., *Classifications of countably-based abelian profinite groups*, J. Group Theory 16 (2013), no.1, 141–157

[KRD] Kionke S., Raimbault J., with an Appendix by Dunfield N., *On Geometric Aspects of Diffuse Groups*, Documenta Mathematica **21** (2016), 873-915

[KLGP] Klaas G., Leedham-Green C. R., Plesken W., *Linear pro-p groups of finite width*, Lecture Notes in Mathematics, 1674, Springer-Verlag, Berlin, 1997

[K] Klopsch B., *On the Lie theory of p-adic analytic groups*, Math. Z. **249** (2005), 713-730

[K1] Klopsch B., *An introduction to compact p-adic Lie groups* in *Lectures on profinite topics in group theory*, 7-61, London Math. Soc. Stud. Texts, 77, Cambridge Univ. Press, Cambridge, 2011

[K2] Klopsch B., *Abstract quotients of profinite groups, after Nikolov and Segal* in *New directions in locally compact groups*, 73-91, London math. Soc. Lecture Note Ser., 447, Cambridge Univ. Press, Cambridge, 2018

[KS] Klopsch B., Snopce I., *A characterisation of uniform pro-p groups*, Q. J. Math. **65** (2014), 1277-1291

[KoK] Kokorin, A. I., Kopytov, V. M., *Fully ordered groups*, Translated from the Russian by D. Louvish. Halsted Press [John Wiley and Sons], New York-Toronto; Israel Program for Scientific Translations, Jerusalem-London, 1974

[KW] Kropholler P. H., Wilson, J. S., *Torsion in profinite completions*, Journal of Pure and Applied Algebra, **88** (1993), 143-154

[JZ] Jaikin-Zapirain A., *On linear just infinite pro-p groups*, Journal of Algebra, **255** (2002), 392-404

[JZ2] Jaikin-Zapirain A., *The finite and solvable genus of finitely generated free and surface groups*, Res. Math. Sci. 10 (2023), no. 4, Paper No. 44, 24 pp.

[JL] Jarden M., Lubotzky A., *Elementary equivalence of profinite groups*, Bull. London Math. Soc. 40 (2008) 887-896

[La] Lazard M., *Groupes analytiques p-adiques*, Publications mathématiques de l'I.H.É.S., tome 26 (1965), 5-219

[Li] Linnell, P. A., *Zero divisors and idempotents in group rings*, Math. Proc. Cambridge Philos. Soc. 81 (1977), no. 3, 365–368.

[L] Lucchini A., *A bound on the number of generators of a finite group*, Arch. Math. (Basel) 53 (1989), no. 4, 313-317

[L1] Lucchini A., *Some questions on the number of generators of a finite group*, Rend. Sem. Mat. Univ. Padova 83 (1990), 201-222

[L2] Lucchini A., *A bound on the presentation rank of a finite group*, Bull. London Math. Soc. 29 (1997), no. 4, 389–394

[Mar] Margulis G. A., *Discrete subgroups of semisimple Lie groups*, Ergeb. Math. Grenzgeb. (3), 17 [Results in Mathematics and Related Areas (3)] Springer-Verlag, Berlin, 1991

[M] Marker D., *Model Theory. An introduction*, Graduate Texts in Mathematics, 217. Springer-Verlag, New York, 2002

[Ma] Mazurov V. D., *On the set of orders of elements of a finite group* (Russian. Russian summary), Algebra i Logika 33 (1994) no. 1, 81-89, 105; translation in Algebra and Logic 33 (1994), no. 1, 49-55

[Mi] Miller G. A., *The ϕ-subgroup of a group*, Trans. Amer. Math. Soc. 16 (1915), no. 1, 20-26

[Mo] Morris, D. W., *Amenable groups that act on the line*, Algebr. Geom. Topol. 6 (2006), 2509–2518

[N1] Nies A., *Separating classes of groups by first-order sentences*, Internat. J. Algebra Comput. 13 (2003), no. 3, 287-302

[N2] Nies A., *Describing groups*, Bull. Symbolic Logic 13 (2007), no. 3, 305-339

[NST] Nies A., Segal D., Tent K., *Finite axiomatizability for profinite groups*, Proc. London Math. Soc. (3) 123 (2021), no. 6, 597–635

[NS] Nikolov N., Segal D., *On finitely generated profinite groups, I: strong completeness and uniform bounds*, Annals of Math., Vol. 165 (2006), 171-238

[NS1] Nikolov N., Segal D., *Powers in finite groups*, Groups Geom. Dyn. 5 (2011), no.2, 501–507

[N] Nikolov N., *Algebraic properties of profinite groups*, arXiv preprint, arXiv:1108.5130v6, 2012

[O] Oger F., *Cancellation and elementary equivalence of finitely generated finite-by-nilpotent groups*, J. London Math. Soc., (2) 44 (1991), no.1, 173–183

[P] Promislow S. D., *A simple example of a torsion-free, non unique product group*, Bull. London Math. Soc. **20** (1988), 302-304

[R] Rhemtulla, A. H., *Right-ordered groups*, Canadian J. Math. 24 (1972), 891–895

[R2] Rhemtulla A. H., *Residually F_p-groups, for many primes p, are orderable*, Proceedings of the American Mathematical Society, Volume 41, Number 1, November 1973

[RiSe] Rips, E., Segev, Y., *Torsion-free group without unique product property*, J. Algebra 108 (1987), no.1, 116–126

[Ro] Robinson D. J. S., *A course in the theory of groups*. Second edition. Grad. Texts in Math., 80, Springer-Verlag, New York, 1996

[RS] Rudin W., Schneider H., *Idempotents in group rings*, Duke Math. J. **31** (1964), 585-602

[RZ] Ribes L., Zalesskii P., *Profinite Groups*. Second edition. Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], 40, Springer-Verlag, Berlin, 2010

[S] Sandling R. G. *Higman's thesis "Units in group rings"* in *Integral representations and applications* (Oberwolfach, 1980), pp. 93–116, Lecture Notes in Math., 882, Springer, Berlin-New York, 1981

[Sc] Schneider P., *p-adic Lie groups*, Grundlehren Math. Wiss., 344 [Fundamental Principles of Mathematical Sciences], Springer, Heidelberg, 2011

[Se] Segal D., *Words: notes on verbal width in groups*, London Mathematical Society Lecture Note Series, 361, CUP, Cambridge, 2009

[Se2] Segal D., *Some aspects of profinite group theory* in *Essays in geometric group theory*, 27-60, Ramanujan Math. Soc. Lect. Notes Ser. 9, Ramanujan Math. Soc., Mysore, 2009

[Serre1] Serre J. P., *Lie algebras and Lie groups*, 1964 lectures given at Harvard University. Corrected fifth printing of the second (1992) edition, Lecture Notes in Math., 1500 Springer-Verlag, Berlin, 2006

[Serre2] Serre J. P., *Bounds for the orders of the finite subgroups of* $G(k)$ in *Group representation theory*, 405-450, EPFL Press, Lausanne, 2007

[S] Strojnowski A., *A note on U.P. groups*, Communications in algebra, 8(3), 231-234, 1980

[T] Tao T., *Hilbert's fifth problem and related topics*, Grad. Stud. Math., 153 American Mathematical Society, Providence, RI, 2014

[TZ] Tent K., Ziegler M., *A course in model theory*, Lecture Notes in Logic, 40. Association for Symbolic Logic, La Jolla, CA; Cambridge University Press, Cambridge, 2012

[Wil] Wilkes G., *Part III. Profinite Groups*, Lecture Notes, Lent Term 2020, available at `https://www.dpmms.cam.ac.uk/~grw46/LectureNotes.pdf`

[W] Wilson J. S., *First-order group theory* in *Infinite groups 1994 (Ravello)*, 301-314, de Gruyter, Berlin, 1996

[W1] Wilson J. S., *Profinite Groups*, London Mathematical Society Monographs. New Series, vol. 19, The Clarendon Press, Oxford University Press, New York, 1998

[W2] Wilson J. S., *Finite axiomatization of finite soluble groups*, J. London Math. Soc. (2) 74 (2006), no. 3, 566-582

[Wi] Wilson L., *On the power structure of powerful p-groups*, J. Group Theory **5** (2002), 129-144

[Wr] Wright F. B., *Semigroups in compact groups*, Proc. Amer. Math. Soc. 7 (1956), 309–311.

[Z] Zimmer R. J., *Ergodic theory and semisimple groups*, Monogr. Math., 81 Birkhäuser Verlag, Basel, 1984

Eidesstattliche Erklärung

Ich versichere an Eides statt, dass diese Dissertation von mir selbständig und ohne unzulässige fremde Hilfe unter Beachtung der "Grundsätze zur Sicherung guter wissenschaftlicher Praxis an der Heinrich-Heine-Univeristät Düsseldorf" erstellt worden ist.

Martina Conte
Düsseldorf, Oktober 2023