ON GROUPS THAT CAN BE COVERED BY CONJUGATES OF FINITELY MANY CYCLIC OR PROCYCLIC SUBGROUPS

YIFTACH BARNEA, RACHEL CAMINA, MIKHAIL ERSHOV, AND MARK L. LEWIS

ABSTRACT. Given a discrete (resp. profinite) group G, we define $\mathrm{NCC}(G)$ to be the smallest number of cyclic (resp. procyclic) subgroups of G whose conjugates cover G. In this paper we determine all residually finite discrete groups with finite NCC and give an almost complete characterization of profinite groups with finite NCC. As a consequence we can show, for example, that for any $k \in \mathbb{N}$ and any prime $p > 3$ the number of finite p-groups P with more than 3 generators and $\mathrm{NCC}(P) = k$ is finite.

1. INTRODUCTION

1.1. **Motivation.** Questions of covering groups by conjugacy classes of subgroups, frequently called *normal coverings*, have a very long history. For instance, it is a classical theorem from the 19th century that a finite group cannot be written as a union of conjugates of a (single) proper subgroup.[1] In modern terminology, this theorem asserts that finite groups are invariably generated, a property which attracted plenty of attention over the past decade (see, e.g., [Min] and references therein). A lot of recent work was also devoted to studying the *normal covering number* $\gamma(G)$ for a finite non-cyclic group G – the smallest number of proper subgroups whose conjugates cover G (see, e.g., [BPS] and references therein as well as [BSW] for the investigation of a related quantity $\gamma_w(G)$).

In this paper we will study normal cyclic coverings, that is, coverings of groups by conjugacy classes of *cyclic* subgroups. The main invariant we will be interested in is defined as follows.

Definition. Let G be a group. We define $\mathrm{NCC}(G)$ to be the smallest k such that G can be written as a union of conjugacy classes of k cyclic subgroups. If no such k exists, we set $\mathrm{NCC}(G) = \infty$. Here *NCC* is an abbreviation for *normal cyclic covering*.

Our motivation for studying NCC was two-fold. On one hand, understanding which infinite groups have finite NCC and the closely related property (BVC) is related to certain problems about classifying spaces for families of subgroups, most notably a conjecture of Juan-Pineda and Leary [JPL, Conjecture 1] and a question of Lück, Reich, Rognes and Varisco [LRRV, Question 4.9] (see § 11.1 for details). On the other hand, it is natural to compare $\mathrm{NCC}(G)$ with the classical and much better understood invariant $k(G)$, the number of conjugacy classes of G. One of the basic properties of $k(G)$ is that for finite G, it grows with the size of the group: $k(G) \to \infty$ if $|G| \to \infty$. Thus one may ask the following question:

Question 1. *Let $\mathcal{C}$ be a class of finite groups. Is it true that* $\mathrm{NCC}(G) \to \infty$ *as* $|G| \to \infty$ *for* $G \in \mathcal{C}$*?*

[1] This theorem is often attributed to Burnside and appears in his 1897 book [Bu]. However, an equivalent result stated in terms of permutation groups was already established by Jordan [Jo] in 1872.

The answer to Question 1 is clearly negative if $\mathcal{C}$ contains all finite groups since $\mathrm{NCC}(G) = 1$ for any cyclic group. Excluding cyclic groups is not sufficient for a positive answer as it is easy to see that all non-abelian groups of order pq, with p and q distinct primes, have NCC equal to 2. Von Puttkamer asked in his Ph.D. thesis whether the answer is positive if $\mathcal{C}$ is the class of all non-cyclic finite p-groups for a fixed $p > 2$ [vP, Question 5.0.9], and this question served as the original motivation for this project.

It is natural to approach von Puttkamer's question via pro-p groups. If G is a profinite group, $\mathrm{NCC}(G)$ is defined in the same way as for discrete [2] groups except that one replaces cyclic subgroups by procyclic subgroups (that is, closed subgroups topologically generated by a single element). A standard argument (see Claim 8.3) shows that if for some $k \in \mathbb{N}$ there exist infinitely many (non-isomorphic) non-cyclic finite p-groups G with $\mathrm{NCC}(G) \leq k$, then there exists an infinite non-procyclic pro-p group G with $\mathrm{NCC}(G) \leq k$. Conversely, it is clear that if G is any infinite pro-p group which is not procyclic and $\mathrm{NCC}(G) = k < \infty$, then sufficiently large finite quotients of G form an infinite family of non-cyclic finite p-groups with NCC equal to k.

This led us to investigate which infinite pro-p groups have finite NCC. As we will explain below, infinite non-procyclic pro-p groups with finite NCC do exist, and thus von Puttkamer's question has negative answer as stated in [vP]. However, it turns out that infinite pro-p groups and more generally infinite profinite groups with finite NCC have very restricted structure (see Theorems 1.3 and 1.5 and Corollary 1.4), so our results can be viewed as saying that von Puttkamer's question has positive answer apart from a small family of exceptions. Using these results we will solve the aforementioned conjecture from [JPL] and give a positive answer to [LRRV, Question 4.9] for discrete *residually finite* groups (see Corollary 11.5).

Remark. We would like to mention a simple alternative characterization of NCC valid for all profinite groups (so in particular for finite groups) although it will not be used in the paper. If G is profinite, then $\mathrm{NCC}(G)$ is the number of conjugacy classes of maximal procyclic subgroups of G. This is because in a profinite group every procyclic subgroup is contained in a maximal procyclic subgroup. The corresponding assertion in the discrete case (with procyclic subgroups replaced by cyclic subgroups) does not always hold, even for residually finite groups. For example, $G = \oplus_p \mathbb{Z}/p\mathbb{Z}$, where the sum is over all primes, is a residually finite group which has infinite NCC but has no maximal cyclic subgroups.

1.2. **Discrete groups with finite NCC.** Our first main theorem asserts that in the discrete residually finite case there are no non-trivial examples with finite NCC, confirming a conjecture of von Puttkamer [vP, Conjecture 5.0.1]:

Theorem 1.1. *Let G be an infinite discrete residually finite group with finite NCC. Then G is infinite cyclic or infinite dihedral (both of these do have finite NCC, 1 and 3 respectively).*

There are several classes of infinite discrete (not necessarily residually finite) groups which were previously known to satisfy the conclusion of Theorem 1.1:

(a) virtually solvable groups,
(b) one-relator groups,
(c) acylindrically hyperbolic groups,
(d) 3-manifold groups,

[2] In this paper by a discrete group we will simply mean a group not endowed with any topology.

(e) CAT(0) cube groups,
(f) finitely generated linear groups,
(g) arbitrary linear groups in characteristic zero.

For (a) this was proved by Groves and Wilson [GW]. Von Puttkamer and Wu proved the result for classes (b)-(e) in [vPW1] and for (f) in [vPW2, Theorem 2.11].[3] Finally, (g) is a combination of (a) and a theorem of Bernik [Be] (see Theorem 5.2 for the statement) which, in turn, is based on the existence of generic elements in Zariski-dense subgroups of semisimple algebraic groups in characteristic zero, established by Prasad and Rapinchuk in [PR] (see also Proposition 3.5 and Remark 3.6 in [CRRZ]).

Since finitely generated linear groups are residually finite, the result for (f) is a special case of Theorem 1.1. However, our original proof of Theorem 1.1 which only applied to finitely generated groups actually reduced Theorem 1.1 to the corresponding result for (f). To prove Theorem 1.1 in the general case we will use a similar reduction strategy, but instead of [vPW2, Theorem 2.11] we will apply the above theorem from [Be].

Note that if a group G has finite NCC, then obviously so do all its quotients. Thus, we get an immediate consequence of Theorem 1.1 applicable to arbitrary discrete groups.

Corollary 1.2. *Let G be a discrete group with finite NCC. Then the image of G in its profinite completion (which is the largest residually finite quotient of G) is finite, cyclic or infinite dihedral.*

Remark. There are plenty of known examples of infinite discrete groups which have finitely many conjugacy classes and thus in particular have finite NCC. Such groups with only 2 conjugacy classes (albeit infinitely generated) were constructed already in the classical paper of Higman, B.H. Neumann and H. Neumann [HNN]. To the best of our knowledge, the first finitely generated examples are due to S. Ivanov [Ol, Theorem 41.2]. Finally, the main theorem of a remarkable paper of Osin [Os] implies that for any $n \geq 2$ there exist infinite 2-generated groups with exactly n conjugacy classes; moreover there exist such groups of exponent p for all sufficiently large prime p. For additional examples of infinite groups with finite NCC see [vPW2].

1.3. **Profinite groups with finite NCC.** We now turn to the classification of profinite groups with finite NCC. We start by describing pro-p groups with finite NCC.

Theorem 1.3. *Let p be a prime and G a pro-p group. Then G has finite NCC if and only if one of the following 3 mutually exclusive conditions holds:*

(i) *G is finite.*
(ii) *G is infinite procyclic or $p = 2$ and G is infinite prodihedral, that is, the pro-2 completion of the infinite dihedral group.*
(iii) *G is isomorphic to an open torsion-free subgroup of $\mathrm{PGL}_1(D)$ where D is the quaternion division algebra over $\mathbb{Q}_p$.*

Remark. Let us briefly comment on the structure of the groups in item (iii). Let D be the quaternion division algebra over $\mathbb{Q}_p$ and O_D its ring of integers. The group $\mathrm{PGL}_1(D) = D^\times/\mathbb{Q}_p^\times$ is virtually pro-p and virtually torsion-free. Moreover its first congruence subgroup $\mathrm{PGL}_1^1(O_D)$ is pro-p and for $p > 2$ contains every pro-p subgroup of

[3] Technically, the results for all classes (a)-(f) were not established until [vPW2] since [GW] and [vPW1] dealt not with groups with finite NCC, but with groups satisfying the related property (BVC) – see § 11.1. However, the proofs of the corresponding results for (BVC) are completely analogous.

$\mathrm{PGL}_1(D)$ (see § 7.2 for the definition of $\mathrm{PGL}_1^1(O_D)$). It is easy to show that if $p > 3$, already the group $\mathrm{PGL}_1^1(O_D)$ is torsion-free. Further, if $p > 2$, then $\mathrm{PGL}_1^1(O_D)$ is isomorphic to $\mathrm{SL}_1^1(O_D)$, the first congruence subgroup of $\mathrm{SL}_1(D)$ where $\mathrm{SL}_1(D)$ is the group of elements of reduced norm 1 in D. See Lemmas 7.9 and 7.10 and Corollary 7.11 for the proofs of these statements.

The classification of pronilpotent groups with finite NCC easily reduces to the pro-p case. Indeed, if G is pronilpotent, it is a direct product of its Sylow pro-p subgroups G_p. Moreover, by Lemma 2.3 below we have $\mathrm{NCC}(G) = \prod \mathrm{NCC}(G_p)$. Thus a pronilpotent group G has finite NCC if and only if each G_p has finite NCC and moreover $\mathrm{NCC}(G_p) = 1$ for almost all p. Since pro-p groups with NCC 1 are exactly procyclic pro-p groups and a product of procyclic groups of coprime orders is procyclic, we obtain the following corollary:

Corollary 1.4. *A pronilpotent group G has finite NCC if and only if $G = C \times \prod_{i=1}^{k} H_i$ where C is a procyclic group and there exist distinct primes $p_1, \dots, p_k$ not dividing $|C|$ such that each H_i is a non-cyclic pro-p_i group with finite NCC.*

The following theorem completes the classification of arbitrary profinite groups with finite NCC up to commensurability by reducing the problem to the pronilpotent case.

Theorem 1.5. *Let G be a profinite group with finite NCC. Then G contains an open pronilpotent subgroup (which must also have finite NCC by Lemma 2.2).*

Note that Theorem 1.5 does not provide a complete description of profinite groups with finite NCC up to isomorphism since finiteness of NCC is not necessarily preserved by finite index overgroups. Nevertheless, we will prove a variation of Theorem 1.5 which provides a precise characterization of groups which have an open pronilpotent subgroup with finite NCC – by Theorem 11.3 these are precisely the groups with property (BVC). By definition a profinite group G has (BVC) if it has finitely many virtually procyclic subgroups $\{V_i\}_{i=1}^{n}$ such that every virtually procyclic subgroup of G is conjugate to a subgroup of V_i for some i (see § 11 for details).

Back to von Puttkamer's question. Finiteness of NCC for the groups in item (iii) of Theorem 1.3 (which yields a negative answer to von Puttkamer's question, as discussed above) was essentially known prior to this paper. It may have been indirectly observed by many mathematicians, but the earliest reference in the literature we are aware of is a paper of Jaikin-Zapirain [Ja]. Let F be a p-adic field and D a finite-dimensional central division algebra over F. The proof of Theorem 1.3 in [Ja] shows that $\mathrm{PGL}_1(D)$ is covered by the conjugacy classes of finitely many abelian subgroups – in the terminology of § 7 this says that $\mathrm{PGL}_1(D)$ has finite NAC. This result easily implies that if $F = \mathbb{Q}_p$ and $\deg(D) = 2$, then any open torsion-free pro-p subgroup G of $\mathrm{PGL}_1(D)$ has finite NCC. Indeed, finiteness of NAC is preserved by open subgroups, so any such G has finite NAC. Since G is torsion-free and pro-p, all of its closed abelian subgroups must be procyclic (this is because $\mathfrak{sl}_1(D)$, the Lie algebra of $\mathrm{PGL}_1(D)$, is 3-dimensional and non-abelian and has no 2-dimensional subalgebras), and thus G has finite NCC.

The central problem investigated in [Ja] is the following: given a pro-p group G, how fast/slow can the number of conjugacy classes of finite quotients G/N grow relative to the size of G/N? Finiteness of NAC for the groups of the form $\mathrm{PGL}_1(D)$ was used in [Ja] to show that for every $\varepsilon > 0$ there is a finitely generated pro-p group G such that the number of conjugacy classes of G/N is at most $|G/N|^{\varepsilon}$ whenever $|G/N|$ is sufficiently large.

Finiteness of NAC for the groups of the form $\mathrm{PGL}_1(D)$, with D as in the previous paragraph, was also established by Böge, Jarden and Lubotzky in [BJL] using the same argument as in [Ja], but in a very different context. In the terminology of [BJL], a profinite group G is called *sliceable* if there exist finitely many closed subgroups of infinite index $H_1, \dots, H_k$ whose conjugacy classes cover G. [BJL, Theorem D] asserts that the groups of the form $\mathrm{PGL}_1(D)$ are sliceable (but the proof shows they actually have finite NAC). The notion of a sliceable group was introduced in [BJL] in connection with the number-theoretic problem on the existence of Kronecker field towers. It would be interesting to find any number-theoretic questions more directly related to Theorem 1.3.

Profinite groups with countable NCC. Recently Jaikin-Zapirain and Nikolov [JN] proved that any infinite compact Hausdorff group (in particular, any infinite profinite group) has uncountably many conjugacy classes (see also [Wil1] and [Wil2] for some more refined results of this type). Several recent papers investigated profinite groups in which a countable union of procyclic subgroups (without taking conjugates) contains a large portion of the group (in a suitable sense) – see, e.g. [AS].

As a natural continuation of this line of research with our results, we propose the following problem.

Problem 1. *Classify profinite groups with* **countable** *NCC.*

A simple example of a profinite group with countable, but infinite NCC is given by $\mathbb{Z}_p \times \mathbb{Z}/p\mathbb{Z}$. More generally, it is easy to show that every virtually procyclic group has countably many maximal procyclic subgroups, and therefore every profinite group with (BVC) has countable NCC. There do exist groups with countable NCC and without (BVC), e.g. $\mathbb{Z}_p^\times \ltimes \mathbb{Z}_p$ (the group of affine transformations of $\mathbb{Z}_p$) and $\mathrm{PGL}_2(\mathbb{Z}_p)$. One can check that $\mathbb{Z}_p^\times \ltimes \mathbb{Z}_p$ has countable NCC directly from definition. The latter combined with the proof of [BJL, Theorem G] implies that $\mathrm{PGL}_2(\mathbb{Z}_p)$ has countable NCC. Despite these additional examples, it is feasible that the class of infinite profinite groups with countable NCC is still quite small.

A standard argument using Baire Category Theorem shows that a profinite group G with countable NCC must have a procyclic subgroup C such that $\cup_{g\in G} C^g$ has non-empty interior. Thus, as a further generalization of Problem 1 one can ask what can be said about the groups with the latter property. We are grateful to Colin Reid for proposing this question. We refer the reader to [Wes] for a discussion of the corresponding problem about conjugacy classes of elements (classify profinite groups which have a conjugacy class with non-empty interior); see also [JN, Question 2].

1.4. **Some quantitative questions and applications to finite p-groups.** Fix a prime p, and let D be the quaternion division algebra over $\mathbb{Q}_p$. The group $\mathrm{PGL}_1(D)$ has infinitely many non-isomorphic open torsion-free subgroups (for instance, the congruence subgroups $\mathrm{PGL}_1^k(O_D)$ are always open, torsion-free for sufficiently large k, and pairwise non-isomorphic as their abelianizations have different orders). Thus, by Theorem 1.3 there are infinitely many infinite pro-p groups with finite NCC. However, we will prove that there are only finitely many such groups with a given value of NCC.

Theorem 1.6. *For any prime p and integer k there are only finitely many infinite pro-p groups G with* $\mathrm{NCC}(G) = k$.

Let us now consider the following two sets (for each prime p):

(i) Let $\mathrm{NCC}_I(p)$ be the set of all $k > 1$ for which there exists an infinite pro-p group G with $\mathrm{NCC}(G) = k$.
(ii) Let $\mathrm{NCC}_{II}(p)$ be the set of all $k > 1$ for which there exists an infinite family of finite p-groups $\{P_i\}$ with $\mathrm{NCC}(P_i) = k$ for all i.

Since there are infinitely many infinite pro-p groups with finite NCC, Theorem 1.6 implies that the set $\mathrm{NCC}_I(p)$ is infinite. It is easy to show that NCC of any profinite group G is equal to the supremum of NCC of finite quotients of G (see Lemma 2.12). Therefore $\mathrm{NCC}_I(p) \subseteq \mathrm{NCC}_{II}(p)$ (so in particular, $\mathrm{NCC}_{II}(p)$ is also infinite). We do not know whether the reverse inclusion holds (for more on this see the remark at the end of § 8), but we will show that the sets $\mathrm{NCC}_I(p)$ and $\mathrm{NCC}_{II}(p)$ have the same minimal element, which will be denoted by $\mathrm{NCC}_{min}(p)$.

The following theorem provides an explicit formula for $\mathrm{NCC}_{min}(p)$:

Theorem 1.7.

$$\mathrm{NCC}_{min}(p) = \begin{cases} 3 & \text{if } p = 2 \\ 9 & \text{if } p = 3 \\ p+2 & \text{if } p > 3. \end{cases}$$

Problem 2. *Describe explicitly the sets* $\mathrm{NCC}_I(p)$ *and* $\mathrm{NCC}_{II}(p)$. *In particular, determine whether* $\mathrm{NCC}_{II}(p)$ *strictly contains* $\mathrm{NCC}_I(p)$.

By contrast to the set of possible values of $\mathrm{NCC}(G)$, there is an absolute upper bound on $d(G)$ (the minimal number of generators of G) for an infinite pro-p group with finite NCC or for an infinite family of finite p-groups with constant NCC.

Fix a prime p, and let $d_{\mathrm{NCC}}(p)$ be the set of all d for which there exists an infinite pro-p group G with finite NCC and $d(G) = d$.

Theorem 1.8. *The following hold:*

(a) *An integer d lies in $d_{\mathrm{NCC}}(p)$ if and only if there exists an infinite family $\{P_n\}$ of finite p-groups such that $d(P_n) = d$ for all n and $\mathrm{NCC}(P_n)$ is the same for all n.*
(b) (1) $d_{\mathrm{NCC}}(p) = \{1, 2, 3\}$ *for* $p > 3$.
(2) $\{1, 2, 3\} \subseteq d_{\mathrm{NCC}}(3) \subseteq \{1, 2, 3, 4\}$.
(3) $\{1, 2, 3\} \subseteq d_{\mathrm{NCC}}(2) \subseteq \{1, 2, 3, 4, 5, 6\}$.

Remark. Part (b) is an easy consequence of Theorem 1.3 and basic results on the minimal number of generators of p-adic analytic groups.

A finite p-group P with d generators has an elementary abelian p-group quotient of order p^d. The NCC of such an elementary abelian p-group is $\frac{p^d-1}{p-1}$, so $\mathrm{NCC}(P) \geq \frac{p^d-1}{p-1}$. Using this observation and Theorem 1.8, we deduce the following:

Corollary 1.9. *Fix p and k. Then the number of finite p-groups P with* $\mathrm{NCC}(P) = k$ *and $d(P) \notin d_{\mathrm{NCC}}(p)$ is finite.*

Problem 3. *In light of Corollary 1.9, find an explicit bound for the number of finite p-groups P with* $\mathrm{NCC}(P) = k$ *and $d(P) \notin d_{\mathrm{NCC}}(p)$. Find other possible information about such groups, e.g., bounds on their nilpotency class or their derived length.*

If $d \in d_{\mathrm{NCC}}(p)$, then Theorem 1.8 implies that there are infinitely many d-generated finite p-groups with bounded NCC since we can simply take finite quotients of one of the pro-p groups G with $d(G) = d$ and finite NCC in Theorem 1.3. In this case, it would be interesting to know whether every such finite p-group is close to being such a quotient. For instance, we can ask the following:

Problem 4. *Assume that $d \in d_{\mathrm{NCC}}(p)$. Does there exist a function f such that every finite p-group P with $d(P) = d$ and $\mathrm{NCC}(P) = k$ has a normal subgroup N of order $\leq f(p, d, k)$ such that P/N is a quotient of an infinite pro-p group G with $d(G) = d$ and $\mathrm{NCC}(G) < \infty$? If yes, can one also require that $\mathrm{NCC}(G) \leq k$?*

Additional motivation for Problem 4 is provided by a theorem of Leedham-Green [LG, Theorems 6,7] which asserts that every finite p-group of a fixed coclass r can be obtained from an infinite pro-p group of finite coclass in a similar way. We will also discuss a natural graph-theoretic interpretation of Problem 4 in § 8.

From p-groups to p-adic analytic groups. Our combined proof of Theorem 1.3 and Corollary 1.9 uses a well-established method for studying finite p-groups: given a question about finite p-groups, one first reformulates it in terms of pro-p groups, then shows that the resulting pro-p groups must be p-adic analytic and finally uses the structure of p-adic analytic groups to answer the question. For example, this idea was used in the solution to the coclass conjectures. Recently, Jaikin-Zapirain and Tent [JT] applied this method and classification of simple p-adic Lie algebras to show that for any odd $k < 25$ there are only finitely many finite 2-groups with k real conjugacy classes, while there are infinitely many such groups for $k = 25$. It is interesting to note that the proof of the latter result also uses groups of the form $\mathrm{PGL}_1(D)$: finite 2-groups with exactly 25 real conjugacy classes are obtained as quotients of $\mathrm{PGL}_1^1(D)$ where D is a degree 3 central division algebra over $\mathbb{Q}_2$.

1.5. **Outline of the paper.**

- In § 2, we introduce a certain generalization of the NCC invariant, $\mathrm{CC}(G, \Phi)$, where Φ is a group acting on G by automorphisms, and prove some general results about it.
- The proof of Theorem 1.5 is divided into three parts, which will be established in § 3, 4 and 10, respectively.
  - In § 3 we prove that a profinite group with finite NCC has an open prosolvable subgroup (which also has finite NCC by Lemma 2.2).
  - In § 4 we prove that if G is a prosolvable group with finite NCC, then for some $k \in \mathbb{N}$ the k^{th} term of its derived series $G^{(k)}$ is pronilpotent.
  - Finally in § 10 we prove that if G is a prosolvable group with finite NCC such that $G^{(k)}$ is pronilpotent for some $k \in \mathbb{N}$, then G is virtually pronilpotent.
- § 6 deals with pro-p groups. In particular, in § 6 we will prove that pro-p groups with finite NCC are p-adic analytic.
- In § 7 we will first recall various basic results about finite-dimensional division algebras and their multiplicative groups and also describe the structure of finite-dimensional division algebras over local fields. We will then use these results to compute NCC for the groups $\mathrm{PGL}_1(D)$ and their first congruence subgroups $\mathrm{PGL}_1^1(O_D)$ where D is the quaternion division algebra over $\mathbb{Q}_p$ (see Theorem 7.15).
- In § 8 we will prove the results stated in § 1.4 including Theorems 1.6, 1.7 and 1.8.
- Theorem 1.3 will be established in § 9.
- Theorem 1.1 will be proved in § 5. We will first prove Theorem 1.1 for finitely generated groups. This result is an easy consequence of the first two parts of the proof of Theorem 1.5, p-adic analyticity of pro-p groups with finite NCC and [vPW1, Theorem 2.11] which asserts that the only infinite finitely generated discrete linear groups with finite NCC are $\mathbb{Z}$ and the infinite dihedral group. The proof of

Theorem 1.1 in the general case will use both Theorem 1.3 and 1.5 as well as the aforementioned result from [Be] (Theorem 5.2).

- Finally, in § 11 we will introduce property (BVC), a certain variation of finiteness of NCC, and prove Theorem 11.3 which completely classifies profinite groups with (BVC).

Acknowledgments. We are very grateful to Xiaolei Wu for asking us a version of von Puttkamer's question [vP, Question 5.0.9]. We would like to thank Andrei Rapinchuk for illuminating discussions and suggesting the reference [Be] and Alex Lubotzky for bringing [BJL] to our attention. We would also like to thank Andrei Jaikin-Zapirain, Ian Leary, Alex Lubotzky, Colin Reid and John Wilson for helpful feedback on earlier versions of this paper.

2. Cyclic covering number relative to a group of automorphisms

In this section we will establish some basic properties of the NCC invariant and some of its generalization defined below.

2.1. **Covering numbers for subgroups, quotients and direct products.** While we are primarily interested in NCC, in the proofs it will be very convenient to work with a certain generalization of NCC defined below which has better hereditary properties.

Definition. Let G be a discrete (resp. profinite) group and Φ a group acting on G by group automorphisms[4]. A *cyclic (resp. procyclic) Φ-cover* of G is a collection of cyclic (resp. procyclic) subgroups $\{C_i\}_{i\in I}$ of G such that $G = \bigcup_{i\in I,\varphi\in\Phi} \varphi(C_i)$. We define $\mathrm{CC}(G,\Phi)$ to be the smallest number of subgroups in a cyclic (resp. procyclic) Φ-cover of G.

Note that $\mathrm{NCC}(G) = \mathrm{CC}(G,G)$ (where G acts on itself by conjugation).

Lemma 2.1. *Let G be a group and Φ a group acting on G by automorphisms. The following hold:*

(i) *If H is a Φ-invariant subgroup of G, then $\mathrm{CC}(H,\Phi) \le \mathrm{CC}(G,\Phi)$. In particular, if H is any normal subgroup of G, then $\mathrm{CC}(H,G) \le \mathrm{NCC}(G)$.*

(ii) *If K is a Φ-invariant normal subgroup of G (so that Φ naturally acts on G/K), then $\mathrm{CC}(G/K,\Phi) \le \mathrm{CC}(G,\Phi)$. In particular, if K is any normal subgroup of G, then $\mathrm{NCC}(G/K) \le \mathrm{NCC}(G)$.*

(iii) *If Ψ is a finite index subgroup of Φ, then $\mathrm{CC}(G,\Psi) \le [\Phi:\Psi]\mathrm{CC}(G,\Phi)$.*

Proof. (i) and (ii) are obvious, and (iii) follows from the fact that for any action of Φ on a set, any orbit of Φ is a union of at most $[\Phi:\Psi]$ orbits of Ψ. □

The next result which follows from Lemma 2.1 and has been well known before is particularly useful.

Lemma 2.2. *Let G be a group with finite NCC and H a subgroup of finite index. Then H also has finite NCC and in fact* $\mathrm{NCC}(H) \le [G:H]\cdot\mathrm{NCC}(G)$

Proof. We have $\mathrm{NCC}(H) = \mathrm{CC}(H,H) \le [G:H]\cdot\mathrm{CC}(H,G) \le [G:H]\cdot\mathrm{NCC}(G)$ where both CC numbers are with respect to the conjugation action, the first inequality holds by Lemma 2.1(iii) and the second inequality holds by Lemma 2.1(i). □

[4]By a homomorphism between profinite groups we will always mean a continuous homomorphism unless explicitly indicated otherwise

Definition. Let G be a profinite group. The *order of* G is the supernatural number defined as the least common multiple of the orders of finite quotients of G (a supernatural number is a formal product $\prod_p p^{\alpha_p}$ where p ranges over all primes and each $\alpha_p \in \mathbb{Z}_{\geq 0} \cup \{\infty\}$).

Lemma 2.3. *Let G and H be discrete or profinite groups and let Φ and Ψ be groups acting by automorphisms on G and H, respectively, such that $\mathrm{CC}(G, \Phi)$ and $\mathrm{CC}(H, \Psi)$ are both finite. The following hold:*

(a) $\mathrm{CC}(G \times H, \Phi \times \Psi) \geq \mathrm{CC}(G, \Phi) \cdot \mathrm{CC}(H, \Psi)$. *In particular, if G and H both have finite NCC,*

$$\mathrm{NCC}(G \times H) \geq \mathrm{NCC}(G) \cdot \mathrm{NCC}(H).$$

(b) *Assume now that G and H are profinite and have coprime orders. Then both inequalities in (a) must be equalities.*

Proof. (a) For simplicity we will present a proof in the discrete case. The argument in the profinite case is completely analogous. Let $n = \mathrm{CC}(G, \Phi)$, $m = \mathrm{CC}(H, \Psi)$ and $t = \mathrm{CC}(G \times H, \Phi \times \Psi)$, and assume that t is finite (if t is infinite, there is nothing to prove).

Let $\{C_k\}_{k=1}^t$ be a cyclic $\Phi \times \Psi$-cover of $G \times H$. Let G_k and H_k denote the projections of C_k to G and H, respectively. Obviously, G_k and H_k are cyclic and $(\varphi \times \psi)(C_k) \subseteq \varphi(G_k) \times \psi(H_k)$ for all $\varphi \in \Phi$ and $\psi \in \Psi$. (Notice that $\varphi(G_k) \times \psi(H_k)$ need not be cyclic). Thus, $\{G_k \times H_k\}_{k=1}^t$ is a $\Phi \times \Psi$-cover of $G \times H$, that is,

$$G \times H = \bigcup_{1 \leq k \leq t, \varphi \in \Phi, \psi \in \Psi} (\varphi \times \psi)(G_k \times H_k) = \bigcup_{1 \leq k \leq t, \varphi \in \Phi, \psi \in \Psi} \varphi(G_k) \times \psi(H_k). \qquad (***)$$

If $G_i \subseteq \varphi(G_j)$ for some $i \neq j$ and $\varphi \in \Phi$, we can replace G_i by G_j and still have a $\Phi \times \Psi$-cover of $G \times H$. After applying this operation finitely many times, we obtain a new cover which can be written as $\{G_k \times H_{k,j}\}_{1 \leq k \leq n', 1 \leq j \leq m_k}$ where for $i \neq j$ we have $G_i \not\subseteq \varphi(G_j)$ for any $\varphi \in \Phi$. By construction the number of sets in the new cover does not exceed the number of sets in the original cover, that is, $m_1 + m_2 + \cdots + m_{n'} \leq t$. Therefore, it suffices to show that $n' \geq n$ and $m_k \geq m$ for each k.

Projecting both sides of (***) to the first component, we see that $\{G_k\}_{k=1}^{n'}$ is a cyclic Φ-cover of G, so $n' \geq n$. We now need to show that for a fixed k the collection $\{H_{k,j}\}_{j=1}^{m_k}$ is a cyclic Ψ-cover of H. Let x_k be a generator of G_k. If $i \neq j$, then $x_i \notin \varphi(G_j)$ for any $\varphi \in \Phi$ (for otherwise, $G_i \subseteq \varphi(G_j)$ contrary to our assumption). Hence for any $h \in H$, the pair (x_k, h) must be in $\varphi(G_k) \times \psi(H_{k,j})$ for some $1 \leq j \leq m_k$, $\varphi \in \Phi$ and $\psi \in \Psi$, so $h \in \psi(H_{k,j})$. We conclude that $\{H_{k,j}\}_{j=1}^{m_k}$ is a cyclic Ψ-cover of H and thus $m_k \geq m$ as desired.

(b) Let $\{G_i\}_{i=1}^n$ be a cyclic Φ-cover of G and $\{H_j\}_{j=1}^m$ be a cyclic Ψ-cover of H. Since G and H have coprime orders, this is true also for every G_i and H_j and therefore $G_i \times H_j$ is procyclic (by the Chinese Remainder Theorem). Hence $\{G_i \times H_j\}_{1 \leq i \leq n, 1 \leq j \leq m}$ is a cyclic $\Phi \times \Psi$-cover of $G \times H$. Thus $\mathrm{CC}(G \times H, \Phi \times \Psi) \leq nm = \mathrm{CC}(G, \Phi) \cdot \mathrm{CC}(H, \Psi)$, and by (a) the equality must hold.

□

2.2. **Quotients of groups with finite NCC.** In this subsection we collect several results which impose restrictions on infinite quotients of discrete and profinite groups with finite NCC. We start with the technically easier discrete case.

Lemma 2.4. *Let G be a residually finite discrete group with finite NCC, and assume that G is not cyclic. Then $\mathbb{Z}$ is not a homomorphic image of G. Thus, if in addition G is finitely generated, then G has finite abelianization.*

Proof. We argue by contradiction. Suppose that there exists an epimorphism $\pi : G \to \langle x \rangle$ where $\langle x \rangle$ is infinite cyclic. Let $H = \operatorname{Ker} \pi$. Since G is not cyclic, H is non-trivial. Since G is residually finite, there exists an epimorphism $\varphi : G \to F$ from G to some finite group F such that $\varphi(H) \neq \{1\}$.

Now let $g \in G$ be any element such that $\pi(g) = x$, let $h \in H$ be any element such that $\varphi(h) \neq 1$, and let $n = |F|$. Consider the sequence of elements $\{g_i = g^{n^i} h\}_{i=1}^{\infty}$. We claim that g_i and g_j cannot lie in conjugates of the same cyclic subgroup for $i \neq j$. Indeed, suppose that there exists $t \in G$ and $i < j$ such that $g^{n^i} h \sim t^a$ and $g^{n^j} h \sim t^b$ for some $a, b \in \mathbb{Z}$ where $\sim$ denotes conjugacy in G.

Let x^c be the projection of t to $\langle x \rangle$. Then projecting both sides of the above conjugacy relations onto $\langle x \rangle$, we get $x^{n^i} = x^{ac}$ and $x^{n^j} = x^{bc}$. Thus, $n^i = ac$ and $n^j = bc$, whence $b = n^k a$ where $k = j - i$. Therefore, $(g^{n^i} h)^{n^k} \sim t^{n^k a} = t^b \sim g^{n^j} h$. Now applying $\varphi : G \to F$ to both sides and recalling that $n = |F|$, we get $\varphi(h) = 1$, contrary to the choice of h. $\square$

In the profinite case we will prove a somewhat different result (see Lemma 2.6 below). Its proof will follow the same general approach as that of Lemma 2.4, but will involve extra technicalities. First we will introduce some additional terminology.

Definition. Let G be a profinite group and $x \in G$.

(i) Let p be a prime. We will say that x is a *pro-p element* if $\overline{\langle x \rangle}$ (the procyclic subgroup generated by x) is a pro-p group. Thus, x is a pro-p element $\iff$ $\overline{\langle x \rangle} \cong \mathbb{Z}_p$ or x has (finite) p-power order $\iff$ the image of x in any finite quotient of G has p-power order.

(ii) More generally, let S be a set of primes. We will say that x is a *pro-S element* if $|\overline{\langle x \rangle}|$ is a product of primes from S (equivalently, the order of the image of x in any finite quotient of G is a product of primes from S).

(iii) If p is a prime, we will say that x is a pro-p' element if x is pro-S where S is the set of all primes different from p.

Observation 2.5. *Let x be an element of a profinite group Q and S a set of primes.*

(a) *If x is pro-S, then so is any homomorphic image of x.*
(b) *If x and y are commuting pro-S elements, then xy is also pro-S.*
(c) *If x is both pro-S and pro-S', where S' is the complement of S, then $x = 1$.*
(d) *If $\pi : G \to Q$ is an epimorphism of profinite groups and $x \in Q$ is a pro-S element, there exists a pro-S element $g \in G$ with $\pi(g) = x$.*

Proof. (a), (b) and (c) are obvious, so we will only prove (d). Take any g_0 with $\pi(g_0) = x$. The procyclic group $\overline{\langle g_0 \rangle}$ decomposes as a direct product of its q-Sylow subgroups, so we can write $g_0 = gg'$ where g is pro-S, g' is pro-S' (where S' is the complement of S) and g and g' both lie in $\overline{\langle g_0 \rangle}$ (and therefore commute).

Applying π to both sides, we get $x = \pi(g)\pi(g')$ and hence $\pi(g)^{-1}x = \pi(g')$. By (a), $\pi(g)$ is pro-S and $\pi(g')$ is pro-S'. Since $\pi(g)$ commutes with $\pi(g')$ and hence with x, by (b) $\pi(g)^{-1}x$ is pro-S and hence by (c) $\pi(g)^{-1}x = \pi(g') = 1$. Thus, $x = \pi(g)$ as desired. $\square$

Lemma 2.6. *Let G be a profinite group, H a (closed) normal subgroup of G and $Q = G/H$. Suppose that Q has a pro-p element x of infinite order (that is, $\overline{\langle x\rangle} \cong \mathbb{Z}_p$) and $|H|$ is divisible by p. Then G has infinite NCC.*

Proof. Let $\pi : G \to Q = G/H$ be the natural projection. By Observation 2.5(d), G contains a pro-p element g with $\pi(g) = x$. Since $|H|$ is divisible by p and the topology of H is induced from G, there exists an open normal subgroup U of G such that the image of H in G/U has order divisible by p.

Let $\varphi : G \to G/U$ be the natural projection. Since $|\varphi(H)|$ is divisible by p, there exists $h \in H$ such that $\varphi(h)$ has order p. Since g is a pro-p element, $\varphi(g)$ has order p^n for some $n \in \mathbb{Z}_{\geq 0}$. Replacing g (resp. x) by g^{p^n} (resp. x^{p^n}) (which will not affect the hypotheses of Lemma 2.6), we can assume that $\varphi(g) = 1$, that is, $g \in U$.

Consider the infinite sequence of elements $\{g_k = g^{p^k}h\}_{k=1}^{\infty}$. We claim that distinct elements in this sequence cannot lie in conjugate procyclic subgroups (and therefore $\mathrm{NCC}(G) = \infty$). Suppose that g_i and g_j, with $i < j$ do lie in conjugate procyclic subgroups, so there exist $t, u, v \in G$ such that $g_i \in \overline{\langle t^u\rangle}$ and $g_j \in \overline{\langle t^v\rangle}$. In profinite groups there is a well-defined operation of raising an element to a power α where $\alpha \in \widehat{\mathbb{Z}}$ (profinite completion of $\mathbb{Z}$). Thus, there exist $\alpha, \beta \in \widehat{\mathbb{Z}}$ such that $g_i \sim t^\alpha$ and $g_j \sim t^\beta$ where again $\sim$ denotes conjugacy in G. We will now derive mutually exclusive conditions on α and β by projecting both sides of these relations to G/U and G/H.

Given $\gamma \in \widehat{\mathbb{Z}}$, let $\nu_p(\gamma) \in \mathbb{Z}_{\geq 0} \cup \{\infty\}$ be the exponent of the highest power of p dividing γ. It is defined by $\nu_p(\gamma) = \lim \nu_p(c_i)$ where $\{c_i\}$ is any integer sequence converging to γ. The function ν_p inherits all the standard properties of its restriction to $\mathbb{Z}$ except that we may have $\nu_p(\gamma) = \infty$ for nonzero γ. In fact, $\nu_p(\gamma) = \infty$ if and only if γ is a pro-p' element of $(\widehat{\mathbb{Z}}, +)$.

Let us now project the relations $g_i \sim t^\alpha$ and $g_j \sim t^\beta$ to G/U. Recalling that the projection to G/U is denoted by φ and that $g \in U$, we get $\varphi(h) \sim \varphi(t)^\alpha$ and $\varphi(h) \sim \varphi(t)^\beta$. Recall also that $\varphi(h)$ has order p and G/U is finite. This means that $\nu_p(\alpha)$ and $\nu_p(\beta)$ are both finite (otherwise, the order of $\varphi(h)$ would be coprime to p) and moreover,

$$1 = \nu_p(\mathrm{ord}(\varphi(h)) = \nu_p(\mathrm{ord}(\varphi(t))) - \nu_p(\alpha) = \nu_p(\mathrm{ord}(\varphi(t))) - \nu_p(\beta),$$

whence $\nu_p(\alpha) = \nu_p(\beta)$.

Now consider the projection $\pi : G \to Q = G/H$ and let $y = \pi(t)$. We get $x^{p^i} = \pi(g_i) \sim y^\alpha$ and $x^{p^j} = \pi(g_j) \sim y^\beta$. Choose a finite quotient R of Q where the images of y^α and y^β are non-trivial (recall that x has infinite order, so such R exists), and let $\rho : Q \to R$ be the projection. Since x is a pro-p element, $\rho(x)$ has order p^m for some $m \in \mathbb{N}$, and we must have $m > j$ (recall that $j > i$) since $\rho(y^\beta) \neq 1$. It follows that

$$m - j = \nu_p(\mathrm{ord}(\rho(x)^{p^j})) = \nu_p(\mathrm{ord}(\rho(y^\beta))) = \nu_p(\mathrm{ord}(\rho(y))) - \nu_p(\beta)$$

and similarly $m - i = \nu_p(\mathrm{ord}(\rho(y))) - \nu_p(\alpha)$. Thus, $\nu_p(\beta) - \nu_p(\alpha) = j - i > 0$, contrary to our earlier conclusion. □

Lemma 2.6 provides a very strong restriction in the case of pro-p groups:

Corollary 2.7. *Let G be an infinite pro-p group with finite NCC. Then G must be just-infinite (that is, all of its proper continuous quotients are finite).*

Proof. First we prove that G is finitely generated. Below we denote the minimal number of generators of a group by $d(\cdot)$. Let $\Phi(G)$ be the Frattini subgroup of G, that is, the intersection of (proper) maximal open subgroups of G. By [DDMS, Proposition 1.9], $d(G) = d(G/N)$ whenever $N \subseteq \Phi(G)$. On the other hand, since G is pro-p, we have $\Phi(G) = \overline{[G,G]G^p}$ by [DDMS, Proposition 1.13]. Therefore, $d(G) = d(G/\overline{[G,G]})$. But $G/\overline{[G,G]}$ is an abelian group with finite NCC, so it is clearly finitely generated and hence G is also finitely generated.

Suppose now that G has a non-trivial closed normal subgroup H such that G/H is infinite. Note that G/H is also finitely generated. By the positive solution to the general Burnside problem for pro-p groups [Ze], a finitely generated torsion pro-p group is finite. Thus, G/H must contain an element x of infinite order. Then x and H trivially satisfy the hypotheses of Lemma 2.6 and hence G has infinite NCC, contrary to our assumption. □

2.3. **Other lower bounds on NCC.** In this subsection we collect some additional results which provide either a lower bound on NCC of a group or a restriction on the structure of a group with finite NCC.

We start by relating NCC to the set of orders of elements. The following definition will only be introduced for discrete groups. The corresponding notion in the profinite case requires extra care, but also will not be needed; in fact, here the case of finite groups will be sufficient for our purposes.

Definition. Let G be a non-trivial discrete group.

(a) An integer $k > 1$ will be called a *primitive element order* of G if G has a maximal cyclic subgroup of order k.
(b) An integer $k > 1$ will be called a *maximal element order* of G if G has an element of order k, but has no element whose order is a proper (finite) multiple of k.

We will denote the set of all primitive (resp. maximal) element orders of G by $PEO(G)$ (resp. $MEO(G)$).

Lemma 2.8. *Let G be a discrete group. Then $MEO(G)$ is a subset of $PEO(G)$. Moreover, $|PEO(G)| \leq \mathrm{CC}(G, \Phi)$ for any Φ.*

Proof. The first assertion is clear. If $\{C_i\}$ is any cyclic Φ-cover of G, then for any maximal cyclic subgroup C of G, the Φ-orbit of C must contain one of the subgroups C_i, so $MC(G, \Phi) \leq \mathrm{CC}(G, \Phi)$ where $MC(G, \Phi)$ is the number of Φ-orbits of maximal cyclic subgroups. On the other hand, if C and C' are maximal cyclic subgroups of different orders, they must be in different orbits. Thus, $|PEO(G)| \leq MC(G, \Phi)$, which proves the second assertion. □

The next result can be used, in particular, to show that if G is a group with finite NCC, then a normal subgroup of G cannot decompose as a direct product of too many non-abelian simple groups.

Lemma 2.9. *Let H be a discrete or profinite group and Φ a group acting on H by automorphisms. Suppose that there exists an integer $e > 1$ and elements $h_1, \ldots, h_k$ of H with the following properties:*

(i) *Each h_i has order e.*
(ii) *For any $\varphi \in \Phi$ and $i \neq j$ the subgroups $\varphi(\langle h_i \rangle)$ and $\langle h_j \rangle$ have trivial intersection.*

Then $\mathrm{CC}(H, \Phi) \geq k$.

Proof. Suppose that $\mathrm{CC}(H,\Phi) < k$. Then there exist distinct indices $i \neq j$, integers a, b and an element $h \in H$ such that $h_i \sim h^a$ and $h_j \sim h^b$ where this time $u \sim v$ means that u and v are in the same Φ-orbit. Without loss of generality we can assume that a and b are coprime (if not, replace h by $h^{gcd(a,b)}$). Then $h_i^b \sim h^{ab} \sim h_j^a$. Condition (ii) implies that $h_i^b = h_j^a = 1$, so by condition (i) a and b must both be divisible by e, a contradiction. □

Corollary 2.10. *Let $H = S_1 \times \cdots \times S_k$ where S_i are non-abelian finite simple groups (not necessarily distinct). Then $\mathrm{CC}(H,\Phi) \geq k$ for any group Φ acting on H by automorphisms.*

Proof. We will only use the fact that each S_i is a finite group of even order and has trivial center.

Choose elements $s_i \in S_i$ of order 2, and for each $1 \leq i \leq k$ let $h_i = (s_1, s_2, \ldots, s_i, 1, \ldots, 1)$. Since each s_i is non-central in S_i, the sequence of centralizers $C(h_1) \supset C(h_2) \supset \cdots \supset C(h_k)$ is strictly decreasing. Hence the elements $\{h_i\}$ lie in different Φ-orbits. Since $\{h_i\}$ have prime order (namely order 2), they satisfy the hypotheses of Lemma 2.9 and hence $\mathrm{CC}(H,\Phi) \geq k$. □

Before stating our last result of this section, we introduce one more definition.

Definition. Let G be a discrete or profinite group. We will say that G has *property (FMHFG)* [5] if for any finite group F there are only finitely many homomorphisms from G to F.

Clearly finitely generated groups have (FMHFG). A simple example of an infinitely generated group with (FMHFG) is the direct sum or product of an infinite collection of finite groups of pairwise coprime orders.

Lemma 2.11. *Let G be a discrete or profinite group with finite NCC. Then G has (FMHFG).*

Remark. We will eventually prove that profinite and discrete residually finite groups with finite NCC are finitely generated. However, Lemma 2.11 will be needed as an auxiliary tool in order to establish finite generation.

Proof. Fix a finite group F, and let K be the intersection of the kernels of all homomorphisms from G to F. Then any homomorphism from G to F factors through G/K, so it suffices to prove that G/K is finite.

Clearly G/K embeds into a direct power $H = \prod_{i \in I} F$ for some index set I. Since H and hence G/K is torsion, all cyclic subgroups of H are closed, so there is no need to distinguish between the discrete and profinite cases. For any element $h \in H$ and $i \in I$ we denote by h_i the i^{th} coordinate of h.

Take any $h \in H$, let $e = \mathrm{ord}(h)$, and let $I(h)$ be any finite subset of I such that $LCM(\{\mathrm{ord}(h_i) : i \in I(h)\}) = e$. Then if some $x \in H$ lies in a conjugate of $\langle h \rangle$ and $x_i = 1$ for all $i \in I(h)$, we must have $x = 1$. Since G/K has finite NCC, it lies in the union of conjugacy classes of finitely many cyclic subgroups $\langle h_1 \rangle, \ldots, \langle h_k \rangle$. If $J = \bigcup_{i=1}^{k} I(h_k)$, then any $g \in G/K$ such that $g_j = 1$ for all $j \in J$ must be trivial. But this means that G/K embeds into the finite group $\prod_{j \in J} F$, as desired. □

[5] (FMHFG) stands for 'finitely many homomorphisms to a finite group'

2.4. **NCC of a profinite group and its finite quotients.** In this last short subsection we will prove the following result:

Lemma 2.12. *Let $G = \varprojlim_{i\in I} P_i$ where $\{P_i\}_{i\in I}$ is an inverse system of finite groups in which all the maps $P_i \to P_j$ are surjective. Then*

$$\mathrm{NCC}(G) = \sup \mathrm{NCC}(P_i).$$

In particular, for any profinite group G we have $\mathrm{NCC}(G) = \sup \mathrm{NCC}(P)$ where P ranges over all finite quotients of G.

Proof. By [DDMS, Proposition 1.4], the inverse limit of a system of compact (in particular, finite) sets P_i is always non-empty. Moreover, the proof shows that if all the maps $P_i \to P_j$ are surjective, then so is the induced map $\varprojlim_{i\in I} P_i \to P_j$. Thus, in our setting $\mathrm{NCC}(G) \geq \mathrm{NCC}(P_i)$ for each i, and so $\mathrm{NCC}(G) \geq \sup \mathrm{NCC}(P_i)$.

To prove the reverse inequality $\mathrm{NCC}(G) \leq \sup \mathrm{NCC}(P_i)$ we just need to show that if $k \in \mathbb{N}$ is such that $\mathrm{NCC}(P_i) \leq k$ for all i, then $\mathrm{NCC}(G) \leq k$. Take any such k, and for each $i \in I$ let S_i be the set of all sequences $(g_i(1), \ldots, g_i(k)) \in P_i^k$ such that the conjugacy classes of the cyclic subgroups $\langle g_i(1)\rangle, \ldots, \langle g_i(k)\rangle$ cover P_i. By the choice of k each S_i is non-empty. Moreover, the sets $\{S_i\}$ form an inverse system with the maps $S_i \to S_j$ defined componentwise. By [DDMS, Proposition 1.4], the inverse limit $S = \varprojlim_{i\in I} S_i$ is non-empty; on the other hand, we can naturally identify S with a subset of G^k. Let $(g(1), \ldots, g(k))$ be any element of S, and let $T = \bigcup_{i=1}^{k} \overline{\langle g(i)\rangle}^G$ (where $\overline{A}$ is the topological closure of A and A^G is the normal closure of A in G). Then T is a closed subset of $G = \varprojlim_{i\in I} P_i$ which projects onto each P_i, and from this it is easy to deduce that $T = G$. Thus $\mathrm{NCC}(G) \leq k$, as desired. □

3. Reduction to the residually solvable case

Throughout the paper by a *residually solvable* (resp. *residually nilpotent, prosolvable, pronilpotent*) group we will always mean a residually-(finite solvable) (resp. residually-(finite nilpotent), pro-(finite solvable), pro-(finite nilpotent)) group.

The goal of this section is to establish the first of the three parts in the proof of Theorem 1.5 (recall that the three parts were introduced in § 1.5).

Theorem 3.1. *Let G be a profinite (resp. a discrete residually finite) group, and assume that $\mathrm{NCC}(G) < \infty$. Then G is virtually prosolvable (resp. virtually residually solvable).*

Theorem 3.1 in the discrete case immediately follows from its profinite analogue. Indeed, let G be a discrete residually finite group with finite NCC. Then its profinite completion $\widehat{G}$ is a profinite group with finite NCC. By the profinite part of Theorem 3.1, $\widehat{G}$ has an open prosolvable subgroup U, and so $G \cap U$ is a finite index residually solvable subgroup of G.

Thus, it suffices to prove Theorem 3.1 for a profinite group G. This will be done by analyzing the action of G on the factors of its chief series defined as follows.

Definition. Let G be a profinite group. A descending chain of open normal subgroups $G = G_1 \supseteq G_2 \supseteq \cdots$ will be called a *chief series* of G if the following hold:

(i) $\{G_i\}$ is a base of neighborhoods for the topology on G. Since G is profinite, this is equivalent to requiring that $\cap G_i = \{1\}$.
(ii) G does not have any normal subgroups lying strictly between G_i and G_{i+1}.

Note that a profinite group G has a series satisfying (i) if and only if it is countably based. Moreover, if we start with any series $\{G_i\}$ satisfying (i), then (ii) can always be achieved by refining the series (since each G_i/G_{i+1} is finite and hence has a chief series in the usual sense). Recall that at the end of the previous section we introduced property (FMHFG) which generalizes finite generation and must hold for all groups with finite NCC. We will now show that property (FMHFG) guarantees that the group is countably based.

Lemma 3.2. *Let G be a profinite group with (FMHFG). Then G is countably based and hence has a chief series.*

Proof. For each $i \in \mathbb{N}$, let G_i be the intersection of the kernels of all (continuous) homomorphisms from G to a finite group of order $\leq i$. Since there are finitely many isomorphism classes of finite groups of a given finite order and G has (FMHFG), G_i is the intersection of finitely many open subgroups and thus itself is open. It is also clear that $G_1 \supseteq G_2 \supseteq \cdots$ and every open normal subgroup of index i contains G_i, so $\{G_i\}$ satisfies (i) as desired. □

Observation 3.3. *Let G be a countably based profinite group. The following hold:*

(a) *G is pronilpotent if and only if it admits a chief series $\{G_i\}$ such that G acts trivially on each quotient G_i/G_{i+1}.*
(b) *G is prosolvable if and only if it admits a chief series $\{G_i\}$ such that each quotient G_i/G_{i+1} is abelian.*

For the rest of this section we fix a profinite group G with (FMHFG) and also fix a chief series $\{G_i\}$ of G. For each i let $Q_i = G_i/G_{i+1}$. We know that $Q_i \cong S_i^{n_i}$ for some finite simple group S_i and $n_i \in \mathbb{N}$.

Lemma 3.4. *Whenever S_i is non-abelian we have $n_i \leq \mathrm{NCC}(G)$.*

Proof. By Corollary 2.10 we have $\mathrm{CC}(Q_i, G) \geq n_i$ (where CC is with respect to the conjugation action of G on Q_i), and by Lemma 2.1(i)(ii) $\mathrm{CC}(Q_i, G) \leq \mathrm{NCC}(G)$. □

Lemma 3.5. *For any non-abelian simple group S there are only finitely many i such that $S_i = S$.*

Proof. Fix S. Since G has (FMHFG), there are only finitely many homomorphisms from G to the finite group $\mathrm{Aut}(S^{\mathrm{NCC}(G)})$. Let H be the intersection of the kernels of these homomorphisms. Then H is an open subgroup of G. By Lemma 3.4, for any i with $S_i = S$, the group $\mathrm{Aut}(Q_i)$ embeds into $\mathrm{Aut}(S^{\mathrm{NCC}(G)})$, whence H acts trivially on Q_i and thus cannot contain G_i for any such i (since G_i acts non-trivially on Q_i as S_i is non-abelian). On the other hand, since H is open, it must contain G_j for some j, so we can only have $S_i = S$ for $i < j$. □

We are now ready to prove Theorem 3.1. In view of Observation 3.3(b), the result can be reformulated as follows.

Proposition 3.6. *Assume that $\mathrm{NCC}(G) < \infty$. Then S_i is abelian for all sufficiently large i and therefore G is virtually prosolvable.*

Proof. Let I be the set of all i such that S_i is non-abelian. Our goal is to show that I is finite. First we want to reduce the problem to the case where $n_i = 1$ for all $i \in I$.

For each i the conjugation action of G on $Q_i = S_i^{n_i}$ induces a homomorphism $\pi_i : G \to Sym(n_i)$. Since $n_i \leq \mathrm{NCC}(G)$ by Lemma 3.4 and G has (FMHFG) by Lemma 2.11, there are only finitely many such homomorphisms. If H is the intersection of the kernels of these homomorphisms, then H is an open subgroup of G which preserves each direct factor of each Q_i. Thus, H has a chief series (obtained by a refinement of the series $\{H \cap G_i\}$) where all non-abelian chief factors are simple.

Thus, replacing G by H (which also has finite NCC) we can assume that $n_i = 1$ for $i \in I$, as desired. Now under this extra assumption, for each $i \in I$ we have a homomorphism $\pi_i : G \to \mathrm{Aut}(S_i)$. For any finite simple group S, the outer automorphism group $\mathrm{Out}(S)$ is solvable of derived length at most 3 (this follows from the classification of finite simple groups). Thus, if $K = G^{(3)}$ is the third (closed) derived subgroup of G, then $\pi_i(K) \subseteq \mathrm{Inn}(S_i)$ for all $i \in I$. In fact, we have $\pi_i(K) = \mathrm{Inn}(S_i)$ for all $i \in I$. Indeed, $\pi_i(G)$ contains $\pi_i(S_i) = \mathrm{Inn}(S_i)$ and hence $\pi_i(K)$ contains $\mathrm{Inn}(S_i^{(3)}) = \mathrm{Inn}(S_i)$ (since S_i is perfect).

Let $K_i = K \cap G_i$ and let $\widetilde{Q}_i = K_i/K_{i+1}$ which can be identified with a subgroup of Q_i. A straightforward computation shows that $\widetilde{Q}_i = Q_i = S_i$ for $i \in I$ (again only using the fact that S_i is perfect). Thus if $\widetilde{\pi}_i$ is the natural map from K to $\mathrm{Aut}(\widetilde{Q}_i)$, we have $\widetilde{\pi}_i(K) = \mathrm{Inn}(S_i)$. This implies that K/K_{i+1} must decompose as $R_i \times S_i$ where $R_i = \mathrm{Ker}\,\widetilde{\pi}_i/K_{i+1}$ and thus $R_i \cong K/K_i$.

Now let $L = K_{i_{min}}$ where i_{min} is the smallest element of I. We claim that for each $i \in I$ the quotient L/K_{i+1} maps (homomorphically) onto $P_i := \prod_{j \in I, j \leq i} S_j$. If we prove this, Corollary 2.10 would imply that $|\{j \in I : j \leq i\}| \leq \mathrm{CC}(L/K_{i+1}, G) \leq \mathrm{NCC}(G) < \infty$ and hence I is finite, which would finish the proof.

We prove the claim by induction on i. If $i = i_{min}$ is the smallest element of I, then by construction $L/K_{i+1} = S_i$, so there is nothing to prove.

Now suppose we already proved that L/K_{i+1} maps onto P_i for some $i \in I$ and let m be the smallest element of I larger then i (if such m exists). Then L/K_{m+1} decomposes as $R_m \times S_m$ where $R_m \cong L/K_m$. Since L/K_m maps onto L/K_{i+1} which in turn maps onto P_i, we conclude that L/K_{m+1} maps onto $P_i \times S_m = P_m$, as desired. □

4. Reduction to the residually nilpotent case

Notation: Given a discrete group G we will denote by $\{G^{(i)}\}_{i=0}^{\infty}$ its derived series, that is, define the subgroups $G^{(i)}$ inductively by $G^{(0)} = G$ and $G^{(i)} = [G^{(i-1)}, G^{(i-1)}]$ for $i \geq 1$. If G is profinite, $\{G^{(i)}\}$ will denote the closed derived series, that is, $G^{(i)} = \overline{[G^{(i-1)}, G^{(i-1)}]}$ for $i \geq 1$.

In this section we will complete the second part of the proof of Theorem 1.5 by establishing the following result.

Theorem 4.1. *Let G be a prosolvable (resp. a discrete residually solvable) group, and assume that $\mathrm{NCC}(G) < \infty$. Then there exists $k \in \mathbb{N}$ such that $G^{(k)}$ is pronilpotent (resp. residually nilpotent).*

Similarly to Theorem 3.1, it suffices to prove Theorem 4.1 for prosolvable groups.

The third and final part of the proof of Theorem 1.5 is fairly long and will be postponed till § 10. However, Theorems 3.1 and 4.1 and Lemma 2.4 are sufficient to deduce the counterpart of Theorem 1.5 for finitely generated discrete residually finite groups:

Corollary 4.2. *Let G be a finitely generated discrete residually finite group with finite NCC. Then G is virtually residually nilpotent.*

Proof. By Theorems 3.1 and 4.1, G has a finite index subgroup U such that $U^{(k)}$ is residually nilpotent for some k. If G is virtually cyclic, there is nothing to prove. If G is not virtually cyclic, applying Lemma 2.4 k times we deduce that $U^{(k)}$ has finite index in G, which finishes the proof. □

We now begin the proof of Theorem 4.1. For the rest of the section we fix a prosolvable group G with finite NCC. By Observation 3.3(b), G admits a chief series $\{G_i\}$ such that all the quotients $Q_i = G_i/G_{i+1}$ are abelian. We will also fix such a chief series. For each i we have $Q_i \cong \mathbb{F}_{p_i}^{n_i}$ for some prime p_i and $n_i \in \mathbb{N}$.

We start by reducing Theorem 4.1 to a certain result on solvable subgroups of linear groups over finite fields (see Proposition 4.3 below).

For each i we can think of Q_i as a finite-dimensional vector space over $\mathbb{F}_{p_i}$. To emphasize this point of view we will write $\mathrm{GL}(Q_i)$ instead of $\mathrm{Aut}(Q_i)$. Let T_i denote the image of G in $\mathrm{GL}(Q_i)$. Note that each T_i must be solvable. To prove Theorem 4.1 it suffices to show that the derived lengths of the groups T_i are bounded by some $k \in \mathbb{N}$ (in fact, we will explicitly bound k in terms of $\mathrm{NCC}(G)$). Indeed, if this is true, then $G^{(k)}$ acts trivially on all chief factors $Q_i = G_i/G_{i+1}$ and hence also on their subgroups $(G_i \cap G^{(k)})/(G_{i+1} \cap G^{(k)})$ as well as on the chief factors of any chief series of $G^{(k)}$ refining $\{G_i \cap G^{(k)}\}_{i=1}^{\infty}$. Hence $G^{(k)}$ must be pronilpotent by Observation 3.3(a).

For each i we have $\mathrm{NCC}(T_i) \leq \mathrm{NCC}(G)$. On the other hand, if C is the conjugacy class of a cyclic subgroup of G/G_{i+1}, then the intersection of C with Q_i is either trivial or is the orbit of a 1-dimensional subspace of Q_i under the action of T_i. Thus the action of T_i on the set of 1-dimensional subspaces of Q_i has at most $\mathrm{NCC}(G)$ orbits.

Let T_i' be the subgroup of $\mathrm{GL}(Q_i)$ generated by T_i and the scalar matrices. Then T_i' is also solvable of the same derived length as T_i, and the action of T_i' on the set of nonzero elements of Q_i has the same number of orbits as the action of T_i on 1-dimensional subspaces. Thus, if we bound the derived length of T_i' in terms of the number of orbits of its action on $Q_i \setminus \{0\}$, we will be done. More precisely, we are now reduced to proving the following result:

Proposition 4.3. *Let H be a solvable subgroup of $\mathrm{GL}_n(\mathbb{F}_p)$ for some prime p. Consider H as an abstract group acting on $\mathbb{F}_p^n$, and let r be the number of orbits of this action. Then the derived length of H is bounded above by $f(r)$ for some absolute function f (independent of p and n).*

We need some preparations before proving Proposition 4.3.

Definition. Let P be a permutation group acting on a set X.

(i) Define $r(P)$ to be the number of orbits of P on X.
(ii) The *rank of P*, denoted $\mathrm{rk}(P)$, is the number of orbits of the induced action of P on $X \times X$.
(iii) The *degree of P* is the cardinality of X.

The following result is well known, but for completeness we provide a sketch of proof.

Lemma 4.4. *Let H be a subgroup of $\mathrm{GL}(V)$ for some vector space V, and let AH be the group generated by H and all translations $x \mapsto x + v$ with $v \in V$ (so AH is a subgroup of the affine group $AGL(V)$). The following hold:*

(a) $r(H) = \mathrm{rk}\,(AH)$.
(b) *Assume that H contains all (nonzero) scalar operators. Then H is irreducible as a linear group (that is, V has no non-trivial H-invariant subspaces) if and only if AH is primitive as a permutation group.*

Sketch of proof. (a) holds since AH acts transitively on V and H is a point stabilizer in AH (namely the stabilizer of 0).

(b) If V contains a non-trivial H-invariant subspace W then cosets of W form a non-trivial AH-invariant partition of V, so AH is not primitive.

Suppose now that AH is not primitive, and let Ω be a non-trivial AH-invariant partition of V. Let W be the block of Ω containing 0. Then W is H-invariant since H fixes 0. And since AH contains all maps of the form $x \mapsto \lambda x + a$ with $\lambda \in F^\times, a \in V$, it is easy to show that W must be a subspace of V, so H is not irreducible. □

Proof of Proposition 4.3. We first consider the case where H is an irreducible subgroup of $\mathrm{GL}_n(\mathbb{F}_p)$. In this case Proposition 4.3 easily follows from a theorem of Seager [Sea, Theorem 1] whose simplified version is stated below:

Theorem 4.5 ([Sea])**.** *Let P be a solvable primitive permutation group of rank r and degree d. Then one of the following holds:*

(i) *$d \le f_1(r)$ for some absolute function f_1.*
(ii) *There exist a prime p and integers m and k with $k \le f_2(r)$ for some absolute function f_2 such that $d = p^{mk}$ and P embeds into the permutation wreath product $S(p^m) \operatorname{wr} S_k$. Here S_k is the symmetric group on k letters, $S(p^m)$ is the group of all maps $\mathbb{F}_{p^m} \to \mathbb{F}_{p^m}$ of the form $x \mapsto a\sigma(x) + b$ with $a, b \in \mathbb{F}_{p^m}$, $a \ne 0$ and $\sigma \in \mathrm{Aut}(\mathbb{F}_{p^m})$, and the wreath product is taken with respect to the natural action of S_k on $\{1, 2, \dots, k\}$.*

Since H is solvable, the group AH (defined as in Lemma 4.4) is also solvable. Since H is irreducible, AH is primitive, so we can apply Theorem 4.5 to $P = AH$. If (i) holds, then the order of P (and hence also its derived length) is bounded by a function of r, so we are done. Suppose now that (ii) holds. If Q is the projection of P to S_k, then P embeds into $S(p^m) \operatorname{wr} Q$, and since P is solvable, so is Q. It is straightforward to check that $S(p^m)$ is solvable of derived length ≤ 3, whence the derived length of the wreath product $S(p^m) \operatorname{wr} Q$ (and hence also the derived length of P) is bounded by a function of k and hence also by a function of r, as desired. Thus we proved Proposition 4.3 when H is irreducible.

Now consider the general case. Let $V = \mathbb{F}_p^n$, and let $\{0\} = V_0 \subset V_1 \subset \cdots \subset V_t = V$ be a maximal chain of H-invariant subspaces. Note that $t < r = r(H)$ since vectors lying in $V_i \setminus V_{i-1}$ and $V_j \setminus V_{j-1}$ for $i \ne j$ cannot lie in the same orbit of H.

Let H_i be the canonical image of H in $\mathrm{GL}(V_i/V_{i-1})$. Then each H_i is an irreducible solvable linear group with $r(H_i) \le r$ and hence by Proposition 4.3 in the irreducible case, its derived length $\ell(H_i)$ is bounded above by $f_{irr}(r)$ for some absolute function f_{irr}. On the other hand, the kernel K of the natural projection $H \to \prod_{i=1}^{t} H_i$ is a nilpotent

group of class $\leq t-1$ (see the proof below). Hence $\ell(K) \leq \log_2(t-1)$, and therefore $\ell(H) \leq \ell(K) + \ell(\prod H_i) \leq \log_2(t-1) + \max \ell(H_i) < \log_2(r) + f_{irr}(r)$, as desired.

To prove that K is nilpotent of class $\leq t-1$ notice that $K \subseteq 1+I$ where I is the set of all $f \in \mathrm{End}(V)$ such that $f(V_j) \subseteq V_{j-1}$ for all $1 \leq j \leq t$. Clearly I is a ring (without 1) and $I^t = 0$, whence $1+I$ is a group. By direct computation $[1+I^j, 1+I] \subseteq 1+I^{j+1}$ for all j. Hence $\gamma_t K \subseteq \gamma_t(1+I) = \{1\}$, as desired. □

5. Proof of Theorem 1.1

In this section we will prove Theorem 1.1, assuming the other main results of this paper that will be proved later. We will start by proving Theorem 1.1 for finitely generated groups. The proof in this special case is simpler and will have 3 ingredients:

(1) Corollary 4.2.
(2) Theorem 6.1 which asserts that pro-p groups with finite NCC are p-adic analytic (this will be proved in the next section)
(3) Theorem 5.1 below which describes finitely generated discrete linear groups with finite NCC.

The following theorem was proved by von Puttkamer and Wu in [vPW1]:

Theorem 5.1. *Let G be a finitely generated discrete linear group with finite NCC. Then G is infinite cyclic, infinite dihedral or finite.*

Proof of Theorem 1.1 for finitely generated groups. Let G be an infinite finitely generated residually finite discrete group with finite NCC. By Corollary 4.2, G has a finite index subgroup H which is residually nilpotent. Then H embeds in its pronilpotent completion $\widehat{H}_{nilp}$ which is a pronilpotent group and thus is a direct product of its Sylow pro-p subgroups $\widehat{H}_p$. Note that each $\widehat{H}_p$ is the pro-p completion of H. Thus each $\widehat{H}_p$ also has finite NCC.

By Theorem 6.1 each $\widehat{H}_p$ is p-adic analytic and therefore linear. Let H_p denote the image of H in $\widehat{H}_p$. Then H_p is a discrete finitely generated linear group with finite NCC and hence by Theorem 5.1 must be finite, infinite cyclic or infinite dihedral, where the last case may only occur for $p=2$ (since H_p is residually-p and thus cannot have q-torsion for $q \neq p$). If H_p is finite, it must be a finite p-group. If in addition H_p is non-cyclic, its abelianization is also non-cyclic and hence $\mathrm{NCC}(H_p) \geq p+1$. Since $\mathrm{NCC}(H_p) \leq \mathrm{NCC}(H)$, there are only finitely many p for which H_p is finite non-abelian. It follows that H_p is abelian for almost all p and virtually abelian for all p. Since H embeds into $\prod H_p$, it must be virtually abelian. Since H is finitely generated, it is trivially linear, and we are done by applying Theorem 5.1 again. □

We now prove Theorem 1.1 in the general case.

Proof of Theorem 1.1. We start similarly to the finitely generated case except that this time we need to use the full power of Theorem 1.5 instead of Corollary 4.2.

So let G be a discrete residually finite group with finite NCC. Its profinite completion $\widehat{G}$ also has finite NCC and hence by Theorem 1.5 has an open pronilpotent subgroup U (which has finite NCC as well by Lemma 2.2). Then $H = G \cap U$ is a residually nilpotent finite index subgroup of G (also with finite NCC).

Let p be any prime. As in the finitely generated case, we deduce that the pro-p completion $\widehat{H}_p$ has finite NCC and thus is p-adic analytic and in particular linear over $\mathbb{Q}_p$.

Again let H_p be the image of H in $\widehat{H}_p$, and let Λ_p be the set of eigenvalues of elements of H_p (with respect to a fixed embedding of $\widehat{H}_p$ into $\mathrm{GL}_n(\mathbb{Q}_p)$ for some $n \in \mathbb{N}$). Since H_p has finite NCC, Λ_p is a union of finitely many cyclic subgroups of $\overline{\mathbb{Q}_p}^\times$ (where $\overline{\mathbb{Q}_p}$ is the algebraic closure of $\mathbb{Q}_p$). In particular, Λ_p lies in a finitely generated subfield of $\overline{\mathbb{Q}_p}$. The main result of [Be] asserts the following:

Theorem 5.2. *Let A be a linear semigroup in characteristic zero such that the eigenvalues of all elements of A lie in some finitely generated subfield. Then the subgroup generated by A must be virtually solvable.*

Thus, H_p is virtually solvable and therefore (again using that H_p has finite NCC), H_p is virtually cyclic by the aforementioned result of Groves and Wilson [GW]. The latter in particular implies that H_p is finitely generated, and we can finish the proof as in the finitely generated case.

□

6. Further reductions in the pro-p case

In this short section we will obtain several important restrictions on the structure of pro-p groups with finite NCC. Our first result here which has already been applied in the proof of Theorem 1.1 above asserts that pro-p groups with finite NCC are p-adic analytic:

Theorem 6.1. *Any pro-p group with finite NCC is p-adic analytic.*

Proof. Given a group G, let $\{D_n\}_{n=1}^\infty$ be the dimension series of G in characteristic p. It is defined by $D_n = D_n(G) = \{g \in G : g \equiv 1 \mod I^n\}$, where I is the augmentation ideal of the group algebra $\mathbb{F}_p[G]$, and has the following properties:

(a) $[D_n, D_m] \subseteq D_{n+m}$ for all $n, m \in \mathbb{N}$.
(b) $D_n^p \subseteq D_{np}$ for all $n \in \mathbb{N}$.
(c) G is residually-p if and only if $\bigcap_{n \in N} D_n = \{1\}$.

In fact, $\{D_n\}$ is the fastest descending chain of subgroups satisfying (a) and (b), but this will not be important for our purposes. We will use the well-known characterization of p-adic analytic pro-p groups in terms of their dimension series (see, e.g. [DDMS, § 11]):

Theorem 6.2. *A pro-p group G is p-adic analytic if and only if $D_n(G) = D_{n+1}(G)$ for some $n \in \mathbb{N}$.*

Let us now fix a pro-p group G. For any $1 \neq x \in G$ define $\deg(x)$ to be the unique integer n such that $x \in D_n \setminus D_{n+1}$ (such n exists by (c) above). Also set $\deg(1) = \infty$. The following 3 properties of degree are straightforward:

(i) Conjugate elements have the same degree (this holds by (a) above with $m = 1$).
(ii) $\deg(x^p) \geq p\deg(x)$ for all $x \in G$ (this holds by (b)).
(iii) If $\lambda \in \mathbb{Z}_p^\times$ is a unit of $\mathbb{Z}_p$, then $\deg(x) = \deg(x^\lambda)$ for all $x \in G$ (since in this case x and x^λ generate the same procyclic subgroup).

Let us now assume that G has finite NCC, so there exists a finite subset $\{x_1, \ldots, x_k\}$ of G such that every element of G is conjugate to x_i^λ for some $1 \leq i \leq k$ and $\lambda \in \mathbb{Z}_p$. Let $d_i = \deg(x_i)$ (without loss of generality we can assume that $x_i \neq 1$, so $d_i < \infty$), and more generally let $d_{i,j} = \deg(x_i^{p^j})$.

Property (iii) above implies that for each $\lambda \in \mathbb{Z}_p$ we have $\deg(x_i^\lambda) = d_{i,j}$ for some j and hence by (i) (and the choice of $\{x_1, \dots, x_k\}$), the degree of any nonzero element of G is equal to $d_{i,j}$ for some i and j.

On the other hand, $d_{i,j} \geq p^j d_i$ by (ii), so for each $N \in \mathbb{N}$ there are at most $k(\lfloor \log_p(N) \rfloor + 1)$ possible degrees of elements of G which are $\leq N$. Since $k(\lfloor \log_p(N) \rfloor + 1) < N$ for large enough N, there exists $n \in \mathbb{N}$ which is not the degree of any element of G. But this means precisely that $D_n(G) = D_{n+1}(G)$ and hence G is p-adic analytic by Theorem 6.2. □

It is well known that every p-adic analytic pro-p group contains an open subgroup which is uniform, that is, powerful and torsion-free (see [DDMS, §§ 2-4] for the definition of a powerful pro-p group and the proof of this result). Our next lemma shows that in the case of uniform pro-p groups, NCC can be expressed directly in terms of the associated Lie algebra:

Lemma 6.3. *Let G be a uniform p-adic analytic pro-p group and let $L = L(G)$ the associated $\mathbb{Z}_p$-Lie algebra. Then G has finite NCC if and only if L can be written as a union of G-orbits of finitely many cyclic $\mathbb{Z}_p$-submodules (with respect to the natural action of G on L).*

Proof. Since G is uniform, there is a well-defined exponential map $u \mapsto \exp(u)$ which establishes a bijection between L and G. Lemma 6.3 is a direct consequence of the following two basic properties of exp:

(i) $\exp(\lambda u) = \exp(u)^\lambda$ for all $u \in L$ and $\lambda \in \mathbb{Z}_p$.
(ii) $g^{-1} \exp(u) g = \exp(u^g)$ for all $u \in L$, $g \in G$ where u^g denotes the action of g on u.

□

Our last result in this section informally asserts that if G is a uniform pro-p group with finite NCC, then generic elements of its Lie algebra $L(G)$ must have trivial (that is, one-dimensional) centralizers. This result will be used to rule out the majority of semisimple uniform pro-p groups as candidates for having finite NCC.

Lemma 6.4. *Let G be a uniform pro-p group with finite NCC and let $L = L(G)$. Then for any $x \in L \setminus pL$ there exists $y \in L$ s.t. the centralizer of $x + py$ in L is equal to $\mathbb{Z}_p(x + py)$.*

Proof. Fix $x \in L \setminus pL$. Since G has finite NCC, by Lemma 6.3, L is covered by the G-orbits of finitely many cyclic $\mathbb{Z}_p$-submodules. Since G acts trivially on L/pL, the coset $x + pL$ must lie in a finite union $\cup_{i=1}^k \mathbb{Z}_p x_i^G$ where $x_i = x + py_i$ for some $y_1, \dots, y_k \in L$.

For each $m \in \mathbb{N}$ let us estimate the size of the image of $\mathbb{Z}_p x_i^G$ in $L/p^m L$. Since L is torsion-free, $|L/p^m L| = p^{dm}$ where $d = \dim(L)$ (one can define $\dim(L)$ simply as the rank of L as a $\mathbb{Z}_p$-module). The following key claim will be proved below, but first we will use it to finish the proof of Lemma 6.4.

Claim 6.5. *Let $C_i = C(x_i)$ be the centralizer of x_i in L and $c_i = \dim(C_i)$. Then the image of x_i^G in $L/p^m L$ has cardinality at most $p^{(d-c_i)m}$.*

Claim 6.5 immediately implies that the size of the image of $\mathbb{Z}_p x_i^G$ in $L/p^m L$ is bounded above by $p^{(d-c_i+1)m}$. Since the image of $x + pL$ in $L/p^m L$ has size $p^{d(m-1)}$, we have $p^{d(m-1)} \leq \sum_{i=1}^k p^{(d-c_i+1)m}$ or, equivalently, $1 \leq \sum_{i=1}^k p^{(1-c_i)m+d}$ whence $c_i = 1$ for some i.

Since $\dim(C_i) = 1$, we have $C_i = \mathbb{Z}_p u_i$ for some $u_i \in L$. Since $x_i \in C_i$, we have $x_i = \lambda_i u_i$ for some $\lambda_i \in \mathbb{Z}_p$. But x (and hence x_i) does not lie in pL by assumption, whence $\lambda_i \in \mathbb{Z}_p^\times$. Therefore, $C_i = \mathbb{Z}_p x_i$, as desired. □

Proof of Claim 6.5. To simplify the notations below we set $t = c_i$. Since L is a finite rank free module over a PID, there exists a basis $\{b_j\}_{j=1}^d$ of L and $\lambda_1, \dots, \lambda_t \in \mathbb{Z}_p$ such that $\{\lambda_j b_j\}_{j=1}^t$ is a basis of $C_i = C(x_i)$. Since L is torsion-free and $\lambda_j b_j$ commutes with x_i, b_j also commutes with x_i, whence $\{b_j\}_{j=1}^t$ is a basis of C_i.

Now let $g_j = \exp(b_j)$ and fix $g \in G$. A standard application of the Baker-Campbell-Hausdorff formula (see, e.g. [DDMS, § 6.5]) shows that g can be uniquely written as $g = \exp(z) \prod_{j=1}^{d} g_j^{e_j}$ where $z \in p^m L$ and $0 \le e_j \le p^m - 1$ for all j.

On the other hand, consider the well-known identity $v^{\exp(u)} = (\exp(\operatorname{ad}(u)))(v)$ where $\operatorname{ad}(u) = [\cdot, u]$ and $\exp(\operatorname{ad}(u)) = \sum_{j=0}^{\infty} \frac{\operatorname{ad}(u)^j}{j!}$ for all $u, v \in L$. It implies that g_j acts trivially on x_i for $j \le t$ (since $b_j \in C_i$ in this case), and it is easy to check that $x_i^{\exp(z)} \equiv x_i \mod p^m L$. It follows that $x_i^g \equiv x_i^h \mod p^m L$ where $h = \prod_{j=t+1}^{d} g_j^{e_j}$ which immediately implies the claim (recall that $t = c_i$ and $0 \le e_j \le p^m - 1$). □

7. Covering numbers for the multiplicative groups of division algebras and some of their subgroups

We start with a brief outline of this section. Given a finite-dimensional central division algebra D over a field F, we set $\mathrm{GL}_1(D) = D^\times$ and $\mathrm{PGL}_1(D) = D^\times/F^\times$. According to Theorem 1.3, if $F = \mathbb{Q}_p$, D has degree 2 and G is an open torsion-free subgroup of $\mathrm{PGL}_1(D)$, then G has finite NCC, and in the introduction we already explained how this result follows from [Ja] or [BJL]. In this section we will give a slightly different proof of finiteness of NCC for these groups which will allow us to determine the exact value of NCC in some cases.

Instead of computing NCC for these groups directly, we will study a related quantity denoted by NAC and then show that $\mathrm{NAC}(G) = \mathrm{NCC}(G)$ for G as above.

Definition. Let G be a group (discrete or profinite). We define $\mathrm{NAC}(G)$ to be the smallest k such that G can be covered by the conjugacy classes of k *abelian* subgroups.

While it may be interesting to study NAC in general, the main reason we introduce it here is that it is very easy to understand in the case of multiplicative groups of division algebras. As we will explain in § 7.1, if D is a finite-dimensional central division algebra over a field F and G is a subgroup of $\mathrm{GL}_1(D)$ or $\mathrm{PGL}_1(D)$, then under a natural extra condition, $\mathrm{NAC}(G)$ is equal to the number of orbits of the natural conjugation action of G on the set $\mathcal{MF}(D)$ of maximal subfields of D (see Lemma 7.2). This extra condition holds, e.g., if F is a p-adic field (that is, a finite extension of $\mathbb{Q}_p$) and G is an open subgroup of $\mathrm{GL}_1(D)$ or $\mathrm{PGL}_1(D)$. The Skolem-Noether theorem now immediately implies that if $G = \mathrm{GL}_1(D)$ or $\mathrm{PGL}_1(D)$, then $\mathrm{NAC}(G)$ is bounded above by the number of isomorphism classes of degree d extensions of F where $d = \deg(D)$, and it is well known that this number is finite when F is a p-adic field – see Lemma 7.5(a) below.

On the other hand, in § 7.2 we will prove that if $F = \mathbb{Q}_p$ and $d = 2$ (that is, D is the quaternion division algebra over $\mathbb{Q}_p$) and G is an arbitrary open subgroup of $\mathrm{PGL}_1(D)$ for $p > 3$ or a torsion-free open subgroup of $\mathrm{PGL}_1(D)$ for $p = 2, 3$, then $\mathrm{NCC}(G) = \mathrm{NAC}(G) < \infty$ (see Corollary 7.14). Finally, in § 7.3 we will precisely compute NCC for several groups, including $\mathrm{PGL}_1(D)$ and its first congruence subgroup $\mathrm{PGL}_1^1(O_D)$ when $p > 3$ (see Theorem 7.15).

Local Fields. Throughout the paper by a *local field* we will always mean a locally compact non-Archimedean local field, that is, either a finite extension of $\mathbb{Q}_p$ (such fields will be called *p-adic*) or the field of Laurent series with coefficients in a finite field.

7.1. **Division algebras over arbitrary fields.** In this subsection F is an arbitrary field and D is a fixed finite-dimensional central division algebra over F. The following two facts are well known (see Corollary 2.16 and Corollary 3.5 in [Mil]):

Lemma 7.1. *The following hold:*

(a) *The dimension of D is always a perfect square. The integer $d = \sqrt{\dim(D)}$ is called the degree of D and denoted by $\deg(D)$.*
(b) *If $d = \deg(D)$, then every maximal subfield of D has degree d over F.*

Let $\mathcal{MF}(D)$ denote the set of maximal subfields of D, and consider the natural (conjugation) action of $\mathrm{GL}_1(D)$ on $\mathcal{MF}(D)$. Clearly this action factors through $\mathrm{PGL}_1(D)$.

Lemma 7.2. *Let F and D be as above, let G be a subgroup of $\mathrm{GL}_1(D)$ or $\mathrm{PGL}_1(D)$, and let $m(G)$ denote the number of orbits of the action of G on $\mathcal{MF}(D)$. Then $\mathrm{NAC}(G) \leq m(G)$. Moreover, $\mathrm{NAC}(G) = m(G)$ in each of the following two cases:*

(*) *$G \subseteq \mathrm{GL}_1(D)$ and every $W \in \mathcal{MF}(D)$ can be written as $W = F(g)$ for some $g \in G$.*
(**) *$G \subseteq \mathrm{PGL}_1(D)$ and every $W \in \mathcal{MF}(D)$ can be written as $W = F(g^{d!})$ for some $g \in \widetilde{G}$ where $\widetilde{G}$ is the preimage of G in $\mathrm{GL}_1(D)$ and $d = \deg(D)$.*

Remark. In (**) we must have $F(g) = W$ since $F(g)$ is a subfield containing W and W is maximal.

Before proving Lemma 7.2 we will establish another auxiliary result (Lemma 7.3) and then derive an important consequence of Lemmas 7.2 and 7.3 (Corollary 7.4 below).

Lemma 7.3. *Let F be a p-adic field, and let D be as above. If G is an open subgroup of $\mathrm{GL}_1(D)$ (resp. $\mathrm{PGL}_1(D)$), then G satisfies (*) (resp. (**)) in Lemma 7.2 and thus $\mathrm{NAC}(G)$ is equal to the number of orbits of the action of G on $\mathcal{MF}(D)$.*

Proof. Since W/F is a finite extension in characteristic 0, it has finitely many intermediate subfields. Any proper subfield of W containing F is a closed subset of W with empty interior, whence the union of these subfields, call it Ω, also has empty interior. If G is an open subgroup of $\mathrm{GL}_1(D)$, then $W \cap G$ is an open subset of W and hence cannot be contained in Ω. On the other hand, $F(g) = W$ for any $g \in W \setminus \Omega$, so G satisfies (*).

Now assume that G is an open subgroup of $\mathrm{PGL}_1(D)$, and let $\widetilde{G}$ be its preimage in $\mathrm{GL}_1(D)$. The group $\widetilde{G}$ is p-adic analytic. If $L(\widetilde{G})$ denotes its $\mathbb{Q}_p$-Lie algebra, there exists an open compact Lie subring L_H of $L(\widetilde{G})$ such that the exponential map exp is defined on L_H and maps L_H homeomorphically onto an open compact subgroup H of $\widetilde{G}$; in fact, H is profinite. Now let $m = d!$. The set mL_H is an open subset of L_H containing 0 and $\exp(mL_H) = \{h^m : h \in H\}$. Hence $\{h^m : h \in H\}$ is an open subset of $\mathrm{GL}_1(D)$

containing 1, and since H is profinite, it contains an open subgroup H_1. By the first part of Lemma 7.3, any $W \in \mathcal{MF}(D)$ can be written as $W = F(h)$ for some $h \in H_1$. Since $H_1 \subseteq \{g^m : g \in \widetilde{G}\}$, the proof is complete. □

Corollary 7.4. *Let F be a p-adic field, and let D be as above. The following hold:*

(i) *If G is an open subgroup of $\mathrm{PGL}_1(D)$ and $\widetilde{G}$ is the preimage of G in $\mathrm{GL}_1(D)$, then $\mathrm{NAC}(\widetilde{G}) = \mathrm{NAC}(G)$.*
(ii) *Let $H \subseteq G$ be open subgroups of $\mathrm{GL}_1(D)$ or $\mathrm{PGL}_1(D)$. Then $\mathrm{NAC}(H) \geq \mathrm{NAC}(G)$.*

Proof. (i) follows from Lemmas 7.2 and 7.3 since G and $\widetilde{G}$ have the same orbits on $\mathcal{MF}(D)$. Similarly, (ii) follows from Lemma 7.2 and 7.3 since for any action of a group G on a set, the number of G-orbits cannot exceed the number of H-orbits for any subgroup H of G. □

Proof of Lemma 7.2. To prove the inequality $\mathrm{NAC}(G) \leq m(G)$, it suffices to consider the case where G is a subgroup of $\mathrm{GL}_1(D)$. Indeed, if G is a subgroup of $\mathrm{PGL}_1(D)$ and $\widetilde{G}$ is its preimage in $\mathrm{GL}_1(D)$, then G and $\widetilde{G}$ have the same orbits on $\mathcal{MF}(D)$, and $\mathrm{NAC}(G) \leq \mathrm{NAC}(\widetilde{G})$ since G is a quotient of $\widetilde{G}$.

So let us assume that G is a subgroup of $\mathrm{GL}_1(D)$, and let $\{W_i\}_{i\in I} \subseteq \mathcal{MF}(D)$ be a set of representatives of the orbits of the action of G on $\mathcal{MF}(D)$. Since every element of D lies in some maximal subfield, G is covered by the G-conjugacy classes of the abelian subgroups $W_i^\times \cap G$, whence $\mathrm{NAC}(G) \leq |I| = m(G)$.

Let us now prove the reverse inequality $m(G) \leq \mathrm{NAC}(G)$ assuming that G satisfies (*) or (**). Let $k = \mathrm{NAC}(G)$, and assume that $k < \infty$. Thus there exist abelian subgroups $A_1, \ldots, A_k$ of G whose conjugacy classes cover G.

Case 1: G satisfies (*). Recall that in this case $G \subseteq \mathrm{GL}_1(D)$. Since each A_i is commutative, it lies inside some $W_i \in \mathcal{MF}(D)$.

Now take any $W \in \mathcal{MF}(D)$. By our hypotheses $W = F(g)$ for some $g \in G$, and $g = hah^{-1}$ for some $h \in G$ and $a \in A_i$ for some i. Then $h^{-1}Wh = F(a)$ and $F(a) \subseteq W_i$. Since both W and W_i are maximal subfields, we must have $h^{-1}Wh = W_i$, so the action of G on $\mathcal{MF}(D)$ has at most k orbits, as desired.

Case 2: G satisfies (**). Recall that in this case $G \subseteq \mathrm{PGL}_1(D)$ and $\widetilde{G}$ is the preimage of G in $\mathrm{GL}_1(D)$.

Let $\widetilde{A}_i$ be the preimage of A_i in $\mathrm{GL}_1(D)$. Note that the $\widetilde{G}$-conjugates of $\widetilde{A}_i$ cover $\widetilde{G}$. For each $1 \leq i \leq k$ choose $x_i \in \widetilde{A}_i$ such that $V_i = F(x_i)$ has maximal possible dimension. We claim that $\widetilde{A}_i$ lies in $Stab(V_i)$, the stabilizer of V_i in $\widetilde{G}$. Indeed, for any $g \in \widetilde{A}_i$, the elements $[x_i]$ and $[g]$ (the images of x_i and g in G) commute, so $g^{-1}x_ig = x_if$ for some $f \in F$. Hence $V_i = F(g^{-1}x_ig)$, so $gV_ig^{-1} = F(x_i) = V_i$, as desired.

We will now show that any $W \in \mathcal{MF}(D)$ is $\widetilde{G}$-conjugate to V_i for some i. While not every V_i must be maximal, this would imply that the collection $\{V_i\}_{i=1}^k$ intersects every orbit of the action of G on $\mathcal{MF}(D)$, and therefore, $k \geq m(G)$, which would finish the proof.

So take any $W \in \mathcal{MF}(D)$. By (**) and the remark after Lemma 7.2 we can write $W = F(g) = F(g^{d!})$ for some $g \in \widetilde{G}$. We know that g lies in a $\widetilde{G}$-conjugate of $\widetilde{A}_i$ for some i, and replacing g and W by conjugates, we can assume that $g \in \widetilde{A}_i$.

Recall that $\widetilde{A}_i \subseteq Stab(V_i)$, so the conjugation by g induces an element of the Galois group $\mathrm{Gal}\,(V_i/F)$. Since $|\mathrm{Gal}\,(V_i/F)|$ divides $d!$, the element $g^{d!}$ commutes with V_i, and therefore $W = F(g^{d!})$ commutes with V_i. Since W is a maximal subfield, $V_i \subseteq W$. On the other hand, $g \in \widetilde{A}_i$, so by the choice of V_i we must have $\dim W = \dim F(g) \leq \dim V_i$. Therefore, $V_i = W$, as desired. □

Given $d \in \mathbb{N}$, let us denote by $\mathcal{E}_d(F)$ the set of (isomorphism classes of) field extensions of F of degree d. Thus, by Lemma 7.1(b), every maximal subfield of D belongs to $\mathcal{E}_{\deg(D)}(F)$. If F is a local field (which is our main case of interest), the following stronger statement holds.

Lemma 7.5. *The following hold:*

(a) *Let F be a p-adic field. Then $\mathcal{E}_d(F)$ is finite for every d.*
(b) *Let F be an arbitrary local field, and let D be a central division algebra of degree d over F. Then every field from $\mathcal{E}_d(F)$ is embeddable in D.*

Proof. See [Lang, II.Proposition 14] for a proof of (a) and [Mil, Remark 4.4(c)] for (b). □

By the Skolem-Noether Theorem [Mil, Theorem 2.10], any two isomorphic subfields of D containing F are conjugate by an element of $D^\times$. Combining this result with Lemma 7.5 and Lemma 7.2, we obtain the following corollary:

Corollary 7.6. *Assume that F is a p-adic field and let $d = \deg(D)$. Then*

$$\mathrm{NAC}(\mathrm{GL}_1(D)) = \mathrm{NAC}(\mathrm{PGL}_1(D)) = |\mathcal{E}_d(F)| < \infty.$$

Remark. The inequality $\mathrm{NAC}(\mathrm{GL}_1(D)) \leq |\mathcal{E}_d(F)|$ (which implies $\mathrm{NAC}(\mathrm{PGL}_1(D)) \leq |\mathcal{E}_d(F)|$) was previously established in [Ja] and [BJL] (using the same argument).

If G is an open subgroup of $\mathrm{GL}_1(D)$ or $\mathrm{PGL}_1(D)$, we can still compute $\mathrm{NAC}(G)$ using Lemma 7.2 if we understand how the $\mathrm{GL}_1(D)$-orbits on $\mathcal{MF}(D)$ decompose into G-orbits. The following simple observation addresses the latter question:

Observation 7.7. *Let $H \subseteq G$ be subgroups of $\mathrm{GL}_1(D)$ or $\mathrm{PGL}_1(D)$. Suppose that the action of G on $\mathcal{MF}(D)$ has finitely many orbits. Let $K_1, \ldots, K_t$ be representatives of these orbits, and for each $1 \leq i \leq t$ let $S_i = Stab_G(K_i)$ be the stabilizer of K_i in G. For each i let m_i be the number of orbits of the left-multiplication action of H on G/S_i. Then the G-orbit containing K_i decomposes into m_i orbits of H, and hence the total number of orbits of H on $\mathcal{MF}(D)$ is $\sum_{i=1}^{k} m_i$.*

Remark. Note that m_i defined in Observation 7.7 is equal to the number of (H, S_i)-double cosets in G and also to the number of orbits of the left-multiplication action of S_i on G/H. If H is normal in G, then $m_i = [G : HS_i]$.

7.2. **Division algebras over local fields.** In this subsection we will review some basic facts about division algebras over local fields as well as multiplicative groups of p-adic fields. For more details on division algebras over local fields see Riehm's paper [Ri].

Let D be a finite-dimensional central division algebra over a local field (in particular, D could be a local field itself). Then D admits a discrete valuation, that is, a surjective map $\nu : D^\times \to \mathbb{Z} \cup \{\infty\}$ such that

(i) $\nu(a) = \infty$ if and only if $a = 0$.

(ii) $\nu(ab) = \nu(a) + \nu(b)$ for all $a, b \in D$.
(iii) $\nu(a + b) \geq \min\{\nu(a), \nu(b)\}$ for all $a, b \in D$.

The ring of integers of D is $O_D = \{a \in D : \nu(a) \geq 0\}$. It is a local ring with maximal ideal $\mathfrak{m}_D = \{a \in D : \nu(a) > 0\}$. Elements of valuation 1 are precisely the generators of $\mathfrak{m}_D$; such elements are called *uniformizers* of D.

Let us now fix a local field F and its uniformizer τ. Let D be a finite-dimensional central division algebra over F, and let d be its degree. Let W be the unique unramified extension of F of degree d. By Lemma 7.5, W can be embedded in D; for the rest of the section we fix such a copy in D. One can prove that

$$D \text{ has a uniformizer } \pi \text{ such that } \pi^d = \tau \text{ and } \pi W \pi^{-1} = W. \tag{7.1}$$

It is easy to show that

$$D = \bigoplus_{i=0}^{d-1} \pi^i W \quad \text{and} \quad O_D = \bigoplus_{i=0}^{d-1} \pi^i O_W. \tag{7.2}$$

Property (7.1) implies that there exists $\sigma \in \mathrm{Gal}\,(W/F)$ such that $\pi w \pi^{-1} = \sigma(w)$ for all $w \in W$; in fact, σ generates $\mathrm{Gal}\,(W/F) \cong \mathbb{Z}/d\mathbb{Z}$ (for otherwise W would not be a maximal subfield). It is known that the map $D \mapsto \sigma$ is a well-defined bijection between the isomorphism classes of degree d central division algebras over F and generators of $\mathrm{Gal}\,(W/F)$. Thus, the number of such isomorphism classes is equal $\varphi(d)$ (where φ is the Euler function) [Mil, Remark 4.4(b)]. In particular, there exists a unique degree 2 central division algebra over F, called *the quaternion division algebra* over F.

Let $\overline{F} = O_F/\tau O_F$ and $\overline{W} = O_W/\tau O_W$ be the residue fields of F and W, respectively. The second decomposition in (7.2) easily implies that the inclusion map $O_W \to O_D$ induces a ring isomorphism $\iota : \overline{W} \to O_D/\pi O_D$. More generally, for each $i \in \mathbb{Z}_{\geq 0}$ we have

$$\pi^i O_D/\pi^{i+1} O_D \cong \overline{W} \tag{7.3}$$

as $\overline{F}$-vector spaces via (the inverse of) the map $x \mapsto \pi^i \cdot \iota(x)$.

Given a subset L of D and $i \in \mathbb{N}$, let $\rho_i(L) \subseteq \overline{W}$ be the image of $(L \cap \pi^i O_D)/(L \cap \pi^{i+1} O_D)$ (considered as a subset of $\pi^i O_D/\pi^{i+1} O_D$) under the isomorphism (7.3). If L is a vector space over F, it is easy to check that $\rho_i(L)$ is a vector space over $\overline{F}$, and we define $r_i(L) = \dim_{\overline{F}} \rho_i(L)$.

Lemma 7.8. *Let L be a subfield of D containing F, let a be the residue degree of the extension L/F, that is, $a = [\overline{L} : \overline{F}]$, and let b be the ramification degree of L/F (so that $ab = [L : F]$). Then $r_i(L) = a$ if $\frac{d}{b} \mid i$ and $r_i(L) = 0$ otherwise. In particular,*

1. *if L is maximal and L/F is unramified, then $r_i(L) = d$ if $d \mid i$ and $r_i(L) = 0$ otherwise;*
2. *if L is maximal and L/F is totally ramified, $r_i(L) = 1$ for all i.*

Proof. Let $e = \frac{d}{b}$, and let τ_L be a uniformizer of L. Then $\nu(\tau_L) = \frac{\nu(\tau)}{b} = \frac{\nu(\pi^d)}{b} = \frac{d}{b} = e$. Hence for all $i \in \mathbb{Z}$ we have $L \cap \pi^i O_D = \{x \in L : \nu(x) \geq i\} = \tau_L^{\lceil \frac{i}{e} \rceil} O_L$ where $\lceil \cdot \rceil$ is the ceiling function.

Thus if $e \nmid i$, we have $L \cap \pi^i O_D = L \cap \pi^{i+1} O_D$, so $\rho_i(L) = 0$, and if $i = ej$ for some $j \in \mathbb{Z}_{\geq 0}$, then $\rho_i(L) \cong \tau_L^j O_L/\tau_L^{j+1} O_L \cong O_L/\tau_L O_L = \overline{L}$, as desired. □

Let us now consider the following groups:

- $\mathrm{GL}_1(O_D) = O_D^\times$. Note that $\mathrm{GL}_1(O_D) = \{g \in D : \nu(g) = 0\}$.
- For each $i \in \mathbb{N}$ let $\mathrm{GL}_1^i(O_D) = 1 + \pi^i O_D$, the i^{th} congruence subgroup of $\mathrm{GL}_1(D)$. Equivalently, $\mathrm{GL}_1^i(O_D) = \{g \in G : \nu(g-1) \geq i\}$.
- We already defined $\mathrm{PGL}_1(D) = \mathrm{GL}_1(D)/Z(\mathrm{GL}_1(D)) = D^\times/F^\times$. More generally, for any subgroup H of $\mathrm{GL}_1(D)$ we will denote by PH its canonical image in $\mathrm{PGL}_1(D)$.

Lemma 7.9. *The following hold:*

(a) $\mathrm{GL}_1(D) = \langle \pi \rangle \ltimes \mathrm{GL}_1(O_D)$.

(b) $\mathrm{PGL}_1(D)/\mathrm{PGL}_1(O_D)$ *is cyclic of order* d*, generated by the image of* π*.*

(c) *Let* $\zeta \in W$ *be a root of unity of order* $|\overline{W}^\times| = |\overline{W}| - 1$ *(such* ζ *exists by Hensel's lemma). Then*
$$\mathrm{GL}_1(O_D) = \langle \zeta \rangle \ltimes \mathrm{GL}_1^1(O_D).$$

(d) $\mathrm{PGL}_1(O_D)/\mathrm{PGL}_1^1(O_D)$ *is cyclic of order* $\frac{|\overline{W}^\times|}{|\overline{F}^\times|}$*, generated by the image of* ζ*.*

(e) $\mathrm{GL}_1^i(O_D)/\mathrm{GL}_1^{i+1}(O_D) \cong (\overline{W}, +)$ *for all* $i \in \mathbb{N}$*.*

(f) $\mathrm{PGL}_1(D)$ *is a profinite group and* $\mathrm{PGL}_1^1(O_D)$ *is a pro-p group (with respect to the topology induced from* D*). Moreover, if* $p \nmid d$*, then* $\mathrm{PGL}_1^1(O_D)$ *is the unique Sylow pro-p subgroup of* $\mathrm{PGL}_1(D)$ *and thus contains every pro-p subgroup of* $\mathrm{PGL}_1(D)$*.*

(g) *Let* e *be the ramification index of* F *(that is, the ramification degree of* $F/\mathbb{Q}_p$*). Then* $\mathrm{GL}_1^i(O_D)$ *is torsion-free for* $i > \frac{de}{p-1}$*.*

Proof. (a) holds since the valuation map $\nu : \mathrm{GL}_1(D) \to (\mathbb{Z}, +)$ is a group homomorphism with kernel $\mathrm{GL}_1(O_D)$ and sends π to a generator of $(\mathbb{Z}, +)$.

(b) We claim that $F^\times \cdot \mathrm{GL}_1(O_D) = \langle \tau \rangle \times \mathrm{GL}_1(O_D)$. Indeed, the product on the right-hand side is direct by (a) and the fact that $\tau = \pi^d$ is central in $\mathrm{GL}_1(D)$. The containment "$\supseteq$" is obvious, and "$\subseteq$" holds since $F^\times = \langle \tau \rangle \times O_F^\times$ and $O_F^\times \subseteq \mathrm{GL}_1(O_D)$. Hence using (a) we get $\mathrm{PGL}_1(D)/\mathrm{PGL}_1(O_D) \cong \mathrm{GL}_1(D)/(F^\times \cdot \mathrm{GL}_1(O_D)) \cong \langle \pi \rangle / \langle \pi^d \rangle$, as desired.

(c) and (d) Recall that $O_D/\pi O_D \cong \overline{W}$, so there is a surjective ring epimorphism $\varphi : O_D \to \overline{W}$ with $\operatorname{Ker} \varphi = \pi O_D$. The restriction of φ to $\mathrm{GL}_1(D)$ is a group epimorphism onto $\overline{W}^\times$ with kernel $1 + \pi O_D = \mathrm{GL}_1^1(O_D)$ which maps $\langle \zeta \rangle$ isomorphically onto $\overline{W}^\times$. This implies (c), and (d) can be deduced from (c) similarly to how (b) follows from (a).

(e) is a combination of the obvious isomorphism $\mathrm{GL}_1^i(O_D)/\mathrm{GL}_1^{i+1}(O_D) = (1+\pi^i O_D)/(1+\pi^{i+1} O_D) \cong (\pi^i O_D/\pi^{i+1} O_D, +)$ and (7.3).

(f) From the definition of $\mathrm{GL}_1^i(O_D)$ in terms of valuations, it is clear that $\mathrm{GL}_1^i(O_D)$ is normal in $\mathrm{GL}_1(D)$, and hence $\mathrm{PGL}_1^i(O_D)$ is normal in $\mathrm{PGL}_1(D)$. By (b),(d) and (e), each quotient $\mathrm{PGL}_1(D)/\mathrm{PGL}_1^i(O_D)$ is finite and each quotient $\mathrm{PGL}_1^1(O_D)/\mathrm{PGL}_1^i(O_D)$ is a finite p-group. Since the groups $\{\mathrm{PGL}_1^i(O_D)\}$ form a base of neighborhoods of 1 for both $\mathrm{PGL}_1(D)$ and $\mathrm{PGL}_1^1(O_D)$, it follows that $\mathrm{PGL}_1(D)$ is profinite and $\mathrm{PGL}_1^1(O_D)$ is pro-p. If $p \nmid d$, the order of $\mathrm{PGL}_1(D)/\mathrm{PGL}_1^1(O_D)$ is coprime to p by (b) and (d), so $\mathrm{PGL}_1^1(O_D)$ is a Sylow pro-p subgroup of $\mathrm{PGL}_1(D)$, and being normal, it is the unique Sylow pro-p subgroup.

Finally, for a proof of (g) see, e.g. [Er, Proposition 4.3(c)] (the result there is stated for $\mathrm{SL}_1^i(O_D)$, but the proof applies to $\mathrm{GL}_1^i(O_D)$ without any changes). □

Reduced norm and trace. Let $\mathrm{N}_{\mathrm{red}}$ (resp. $\mathrm{T}_{\mathrm{red}}$) denote the reduced norm (resp. reduced trace) map from D to F. One way to characterize $\mathrm{N}_{\mathrm{red}}$ and $\mathrm{T}_{\mathrm{red}}$ is as follows.

Choose any maximal subfield K of D. Then for any $a \in D$ its reduced norm $\mathrm{N}_{\mathrm{red}}(a)$ (resp. reduced trace $\mathrm{T}_{\mathrm{red}}(a)$) is equal to the determinant (resp. trace) of the endomorphism of the left K-vector space D given by $x \mapsto xa$.

One can show that the restriction of $\mathrm{N}_{\mathrm{red}}$ (resp. $\mathrm{T}_{\mathrm{red}}$) to K coincides with the norm (resp. trace) map of the extension K/F (in the case $K = W$ this easily follows from (7.1) and (7.2)). Since every element of D lies in some maximal subfield, both $\mathrm{N}_{\mathrm{red}}$ and $\mathrm{T}_{\mathrm{red}}$ take values in F, and moreover are surjective as maps from D to F.

The following two facts will be frequently used. (7.5) holds by definition, and (7.4) follows immediately from (7.1) and (7.2).

$$\mathrm{N}_{\mathrm{red}}(\pi) = (-1)^{d-1}\tau \tag{7.4}$$

$$\mathrm{N}_{\mathrm{red}}(\alpha) = \alpha^d \text{ for all } \alpha \in F. \tag{7.5}$$

Let $\mathrm{SL}_1(D) \subset \mathrm{GL}_1(D)$ be the subgroup of elements of reduced norm 1. For each $i \in \mathbb{N}$ we set $\mathrm{SL}_1^i(O_D) = \mathrm{GL}_1^i(O_D) \cap \mathrm{SL}_1(D)$, the i^{th} congruence subgroup of $\mathrm{SL}_1(D)$.

Lemma 7.10. *The following hold:*

(a) $\mathrm{SL}_1(D) \subset \mathrm{GL}_1(O_D)$.
(b) *The kernel of the projection* $\mathrm{SL}_1(D) \to \mathrm{PSL}_1(D)$ *is equal to* $\mu_d(F)$*, the group of* d^{th} *roots of unity in* F.
(c) $\mathrm{PGL}_1(D)/\mathrm{PSL}_1(D) \cong F^\times/(F^\times)^d \cong O_F^\times/(O_F^\times)^d \times (\mathbb{Z}/d\mathbb{Z})$.
(d) *If* d *is not divisible by* p*, then for each* $i \in \mathbb{N}$ *the canonical maps* $\mathrm{SL}_1^i(O_D) \to \mathrm{PSL}_1^i(O_D) \to \mathrm{PGL}_1^i(O_D)$ *are both isomorphisms.*

Proof. (a) Take any $g \in \mathrm{SL}_1(D)$ and write $g = \pi^i x$ with $i \in \mathbb{Z}$ and $x \in \mathrm{GL}_1(O_D)$. It is easy to check that $\mathrm{N}_{\mathrm{red}}(x) \in O_W^\times$. On the other hand, $\mathrm{N}_{\mathrm{red}}(\pi^i) = \pm\tau^i$ by (7.4), so since $\mathrm{N}_{\mathrm{red}}(g) = 1$, we must have $i = 0$ whence $g = x \in \mathrm{GL}_1(O_D)$.

(b) is immediate from definitions and (7.5). Since $\mathrm{N}_{\mathrm{red}} : \mathrm{GL}_1(D) \to F^\times$ is surjective with kernel $\mathrm{SL}_1(D)$ and $\mathrm{N}_{\mathrm{red}}(F^\times) = (F^\times)^d$, we have

$$\begin{aligned}\mathrm{PGL}_1(D)/\mathrm{PSL}_1(D) &\cong \mathrm{GL}_1(D)/(F^\times \cdot \mathrm{SL}_1(D)) \\ &\cong (\mathrm{GL}_1(D)/\mathrm{SL}_1(D))/((F^\times \cdot \mathrm{SL}_1(D)/\mathrm{SL}_1(D)) \cong F^\times/(F^\times)^d\end{aligned}$$

which proves the first isomorphism in (c). The second isomorphism in (c) is simply a consequence of the decomposition $F^\times = O_F^\times \times \langle\tau\rangle$.

(d) The map $\mathrm{SL}_1^i(O_D) \to \mathrm{PSL}_1^i(O_D)$ is surjective, and by (b) its kernel is a finite group of order dividing d. Since $p \nmid d$ and $\mathrm{SL}_1^i(O_D)$ is a pro-p group, the kernel must be trivial, so the first map in (d) is an isomorphism. The second map in (d) is injective by definition. We can prove its surjectivity similarly to how we established injectivity of the first map using (c) and the fact that $\mathrm{PGL}_1^i(O_D)$ is a pro-p group. □

Corollary 7.11. *Let* D *be the quaternion division algebra over* $\mathbb{Q}_p$*. Then* $\mathrm{GL}_1^1(O_D)$ *and* $\mathrm{PGL}_1^1(O_D)$ *are torsion-free for* $p > 3$ *and* $\mathrm{GL}_1^2(O_D)$ *and* $\mathrm{PGL}_1^2(O_D)$ *are torsion-free for* $p > 2$.

Proof. The result for $\mathrm{GL}_1^1(O_D)$ and $\mathrm{GL}_1^2(O_D)$ holds by Lemma 7.9(g) (in our case $d = 2$ and $e = 1$). On the other hand, $\mathrm{PGL}_1^i(O_D)$ embeds into $\mathrm{GL}_1^i(O_D)$ for $p > 2$ by Lemma 7.10. □

The next result collects some basic properties of the multiplicative groups of p-adic fields.

Lemma 7.12. *Let K/F be an extension of p-adic fields, $n = [K : \mathbb{Q}_p]$ and $m = [F : \mathbb{Q}_p]$. Let $\overline{K}$ (resp. $\overline{F}$) be the residue field of K (resp. F), and let a and b be the residue degrees of F and K (that is, $a = \log_p|\overline{F}|$ and $b = \log_p|\overline{K}|$). Let e be the ramification degree of the extension K/F, and let e_K be the ramification index of K. The following hold:*

(a) $K^\times/F^\times \cong \mathbb{Z}/e\mathbb{Z} \times \left(\overline{K}^\times/\overline{F}^\times\right) \times (1+\mathfrak{m}_K)/(1+\mathfrak{m}_F)$.
(b) $\mathfrak{m}_K/\mathfrak{m}_F$ *(the quotient of additive groups) is isomorphic to* $\mathbb{Z}_p^{n-m}$.
(c) *The groups* $(1+\mathfrak{m}_K)/(1+\mathfrak{m}_F)$ *and* $\mathfrak{m}_K/\mathfrak{m}_F$ *are commensurable (that is, have isomorphic open subgroups).*
(d) *Assume in addition that* $e_K < p-1$. *Then* $(1+\mathfrak{m}_K)/(1+\mathfrak{m}_F) \cong \mathfrak{m}_K/\mathfrak{m}_F$ *and hence by (a) and (b)*

$$K^\times/F^\times \cong \mathbb{Z}/e\mathbb{Z} \times \mathbb{Z}/(\tfrac{p^b-1}{p^a-1})\mathbb{Z} \times \mathbb{Z}_p^{n-m}.$$

Proof. (a) follows from the fact that for any p-adic field L the group $L^\times$ has decompositions $L^\times = \langle\tau_L\rangle \times O_L^\times = \langle\tau_L\rangle \times \mu_L \times (1+\mathfrak{m}_L)$ where τ_L is a uniformizer of L and μ_L is the group of roots of unity of order coprime to p in L which is isomorphic to $\overline{L}^\times$.

(b) For any p-adic field L we have $O_L \cong \mathbb{Z}_p^{[L:\mathbb{Q}_p]}$ as additive groups. Moreover, O_K is a free O_F-module and admits a basis containing 1, so $O_K/O_F \cong \mathbb{Z}_p^{n-m}$. Finally, since $\mathfrak{m}_K$ is an open subgroup of O_K and $\mathfrak{m}_F = \mathfrak{m}_K \cap O_F$, the quotient $\mathfrak{m}_K/\mathfrak{m}_F = \mathfrak{m}_K/\mathfrak{m}_K \cap O_F \cong (\mathfrak{m}_K + O_F)/O_F$ is open in O_K/O_F and thus is also isomorphic to $\mathbb{Z}_p^{n-m}$.

(c) The power series $\exp(x) = \sum_{i=0}^\infty \frac{x^i}{i!}$ and $\log(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \cdots$ converge on $\mathfrak{m}_K^n$ for sufficiently large n and thereby establish mutually inverse group isomorphisms between $1+\mathfrak{m}_K^n$ and $\mathfrak{m}_K^n$. If $x \in \mathfrak{m}_F$, we have $\log(1+x) \in \mathfrak{m}_F$ and $\exp(x) \in 1+\mathfrak{m}_F$ (whenever $\exp(x)$ converges). It follows that log maps $1+\mathfrak{m}_K^n \cap \mathfrak{m}_F$ isomorphically onto $\mathfrak{m}_K^n \cap \mathfrak{m}_F$. Thus, $(1+\mathfrak{m}_K^n)/(1+\mathfrak{m}_K^n \cap \mathfrak{m}_F)$ which is an open subgroup of $(1+\mathfrak{m}_K)/(1+\mathfrak{m}_K \cap \mathfrak{m}_F) = (1+\mathfrak{m}_K)/(1+\mathfrak{m}_F)$ is isomorphic to $\mathfrak{m}_K^n/(\mathfrak{m}_K^n \cap \mathfrak{m}_F)$ which is an open subgroup of $\mathfrak{m}_K/\mathfrak{m}_F$, as desired.

(d) The hypothesis $e_K < p-1$ ensures that both series in (c) converge already for $n = 1$, so (d) follows from the above argument for (c). □

Corollary 7.13. *Let $F = \mathbb{Q}_p$ and K a quadratic extension of F. Then the group $K^\times/F^\times$ is virtually $\mathbb{Z}_p$. If $p > 3$, then $K^\times/F^\times$ is procyclic.*

Proof. In the notations of Lemma 7.12 we have $n = 2$ and $m = 1$, so $\mathfrak{m}_K/\mathfrak{m}_F \cong \mathbb{Z}_p$ by Lemma 7.12(b), and hence the first assertion of Corollary 7.13 follows from Lemma 7.12(a)(c).

Assume now that $p > 3$. Since $e_K = e \le 2$, we have $e_K < p-1$, so Lemma 7.12(d) is applicable. Again using the notations of Lemma 7.12 we have $a = 1$, and either $(b, e) = (2, 1)$ (if K/F is unramified) or $(b, e) = (1, 2)$. In either case one of the two groups $\mathbb{Z}/e\mathbb{Z}$ and $\mathbb{Z}/(\frac{p^b-1}{p^a-1})\mathbb{Z}$ is trivial and the other has order coprime to p (since $p > 2$). Thus, by Lemma 7.12(d), the group $K^\times/F^\times$ is a direct sum of $\mathbb{Z}_p$ and a cyclic group of order coprime to p, whence $K^\times/F^\times$ is procyclic. □

Corollary 7.14. *Let $F = \mathbb{Q}_p$ and D the quaternion division algebra over F. Let G be an open subgroup of* $\mathrm{PGL}_1(D)$, *and if $p = 2$ or 3, assume in addition that G is torsion-free. The following hold:*

(a) $\mathrm{NCC}(G) = \mathrm{NAC}(G)$.
(b) $\mathrm{NCC}(G) < \infty$.

Proof. (a) Let $\widetilde{G}$ be the preimage of G in $\mathrm{GL}_1(D)$. Since $\mathrm{NAC}(G) = \mathrm{NAC}(\widetilde{G})$ by Corollary 7.4(i), it suffices to show that $\mathrm{NCC}(G) = \mathrm{NAC}(\widetilde{G})$.

If $\{C_i\}$ is a collection of procyclic subgroups of G whose conjugates cover G, then their preimages are abelian (since the kernel of the map $\widetilde{G} \to G$ is central) and their conjugates cover $\widetilde{G}$. Therefore, $\mathrm{NAC}(\widetilde{G}) \leq \mathrm{NCC}(G)$.

To prove the reverse inequality $\mathrm{NCC}(G) \leq \mathrm{NAC}(\widetilde{G})$, it suffices to show that for any abelian subgroup A of $\widetilde{G}$, its image in G is procyclic. So let A be an abelian subgroup of G, and choose a maximal subfield W of D containing A. By Corollary 7.13, $W^\times/F^\times$ is procyclic if $p > 3$ and virtually procyclic if $p = 2$ or 3. But in the latter case we are assuming that G is torsion-free, so $(W^\times/F^\times) \cap G$ is virtually procyclic, torsion-free and abelian and hence obviously procyclic. Since the image of A in G is contained in $(W^\times/F^\times) \cap G$, it is also procyclic, as desired.

(b) follows from (a), the fact that $\mathrm{PGL}_1(D)$ has finite NAC (Corollary 7.6) and the fact that finiteness of NAC is inherited by open subgroups (this is proved exactly as Lemma 2.2). □

7.3. **Explicit NCC computations.** We are now ready to compute NCC for several groups introduced earlier in this section.

Theorem 7.15. *Let D be the quaternion division algebra over $\mathbb{Q}_p$, and assume that $p > 2$. The following hold:*

1. $\mathrm{NAC}(\mathrm{PGL}_1(D)) = \mathrm{NAC}(\mathrm{PGL}_1(O_D)) = 3$.
2. $\mathrm{NAC}(\mathrm{PGL}_1^1(O_D)) = p + 2$.
   (recall that $\mathrm{PGL}_1^1(O_D) \cong \mathrm{PSL}_1^1(O_D) \cong \mathrm{SL}_1^1(O_D)$ by Lemma 7.10(d)).
3. *Let H be an index p subgroup of $\mathrm{PGL}_1^1(O_D)$ (any such subgroup lies strictly between $\mathrm{PGL}_1^1(O_D)$ and the second congruence subgroup $\mathrm{PGL}_1^2(O_D)$). Then $\mathrm{NAC}(H) = 3p$. If $p = 3$, there exists such a subgroup H which is torsion-free (recall that if $p > 3$, already the subgroup $\mathrm{PGL}_1^1(O_D)$ is torsion-free).*

Remark. Recall that by Corollary 7.14 we have $\mathrm{NAC}(G) = \mathrm{NCC}(G)$ for any group G appearing in the statement of Theorem 7.15 if $p > 3$ as well as for any torsion-free G if $p = 3$.

Proof. Throughout the proof, for any element $x \in \mathrm{GL}_1(D)$ the image of x in $\mathrm{PGL}_1(D)$ will be denoted by $[x]$.

(1a) We start by proving that $\mathrm{NAC}(\mathrm{PGL}_1(D)) = 3$. By Lemma 7.6, we just need to show that

$$|\mathcal{E}_2(\mathbb{Q}_p)| = 3.$$

For any field F of characteristic $\neq 2$, the quadratic extensions all have the form $F(\sqrt{a})$ where a ranges over non-trivial cosets of $F^\times$ mod $(F^\times)^2$; morever distinct cosets yield non-isomorphic fields. In the case $F = \mathbb{Q}_p$ and $p > 2$ we have $F^\times/(F^\times)^2 \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$, so there are 3 quadratic extensions of $\mathbb{Q}_p$, as desired.

For the remainder of the proof we will need to use specific embeddings of these extensions into D, described below.

Recall that W is the chosen unramified quadratic extension of $\mathbb{Q}_p$ inside D. Its residue field has order p^2 and hence contains a primitive root of unity of order $p^2 - 1$. By Hensel's Lemma, W must also contain a primitive root of unity of order $p^2 - 1$, call it ζ. In the

notations of (7.1), we can set $\tau = p$ (recall that τ is the chosen uniformizer of F), so π is a uniformizer of D which satisfies $\pi^2 = p$ and normalizes W. Define

- $K_1 = W$.
- $K_2 = \mathbb{Q}_p(\pi)$.
- $K_3 = \mathbb{Q}_p(\zeta\pi)$.

We need to explain why the fields K_i are pairwise non-isomorphic. It is clear that K_2 and K_3 are ramified while K_1 is unramified, so $K_1 \ncong K_2, K_3$. Recall that $\pi^2 = p$, and by (7.6) below we have $\pi\zeta\pi^{-1} = \zeta^p$ whence $(\zeta\pi)^2 = \zeta(\pi\zeta\pi^{-1})\pi^2 = p \cdot \zeta^{p+1}$. By construction, ζ^{p+1} is a primitive root of unity of order $p-1$, so it lies in $\mathbb{Q}_p^\times$, but not in $(\mathbb{Q}_p^\times)^2$. Thus, π^2 and $(\zeta\pi)^2$ lie in different cosets of $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$ whence the fields K_2 and K_3 are non-isomorphic as explained at the beginning of the proof.

(1b) Next we want to show that $\mathrm{NAC}(\mathrm{PGL}_1(O_D)) = \mathrm{NAC}(\mathrm{PGL}_1(D))$. Since the fields K_1, K_2, K_3 are representatives of the orbits of $\mathrm{PGL}_1(D)$ on $\mathcal{MF}(D)$, by Observation 7.7 we just need to prove that for each $1 \le i \le 3$ we have $\mathrm{PGL}_1(D) = [S_i] \cdot \mathrm{PGL}_1(O_D)$ where S_i is the stabilizer of K_i in $\mathrm{GL}_1(D)$. Equivalently, we need to show that each of the subfields K_1, K_2 and K_3 is invariant under some transversal of $\mathrm{PGL}_1(O_D)$ in $\mathrm{PGL}_1(D)$.

By Lemma 7.9(b), $\mathrm{PGL}_1(D)/\mathrm{PGL}_1(O_D) \cong \mathbb{Z}/2\mathbb{Z}$ and the set $\{1, [\pi]\}$ is a transversal for $\mathrm{PGL}_1(O_D)$ in $\mathrm{PGL}_1(D)$. Since $\zeta \in \mathrm{GL}_1(O_D)$, the set $\{1, [\zeta\pi]\}$ is also a transversal.

Since $\pi \in K_2$, the transversal $\{1, [\pi]\}$ clearly normalizes K_2 and similarly $\{1, [\zeta\pi]\}$ normalizes K_3. Finally, recall that $K_1 = W$ is normalized by π, so K_1 is also invariant under $\{1, [\pi]\}$.

(2) We now turn to proving that $\mathrm{NAC}(\mathrm{PGL}_1^1(O_D)) = p + 2$. Recall that S_i is the stabilizer of K_i in $\mathrm{GL}_1(D)$. We claim that $S_1 = W^\times\langle\pi\rangle$ and $S_i = K_i^\times\langle\zeta^{\frac{p+1}{2}}\rangle$ for $i = 2, 3$.

First note that since K_i is a maximal subfield of D, its centralizer in $\mathrm{GL}_1(D)$ is $K_i^\times$. On the other hand, the quotient $Stab(K_i)/C(K_i) = S_i/K_i^\times$ embeds into the Galois group $\mathrm{Gal}\,(K_i/F)$ which has order 2. Thus to prove the above formulas for S_i it suffices to show that

(i) π normalizes W and $\pi \notin W$.
(ii) $\alpha = \zeta^{\frac{p+1}{2}}$ normalizes K_i and $\alpha \notin K_i$ (equivalently, the conjugation by α induces a non-trivial automorphism of K_i) for $i = 2, 3$.

Condition (i) holds by the choice of π. Since $K_2 = \mathbb{Q}_p(\pi)$ and $K_3 = \mathbb{Q}_p(\zeta\pi)$, to prove (ii), it suffices to determine the image of π under the conjugation by α.

Recall that $\pi w \pi^{-1} = \sigma(w)$ for all $w \in W$ where σ is the generator of $\mathrm{Gal}\,(W/\mathbb{Q}_p)$. The projection $O_W^\times \to \mathbb{F}_{p^2}^\times$ restricts to an isomorphism $\langle\zeta\rangle \to \mathbb{F}_{p^2}^\times$ which is equivariant with respect to the action of σ on the left and the Frobenius map on the right, so $\sigma(\zeta) = \zeta^p$. Hence

$$\pi\zeta\pi^{-1} = \zeta^p, \tag{7.6}$$

so $\zeta^{-1}\pi\zeta = \zeta^{p-1}\pi$ and more generally

$$\zeta^{-j}\pi\zeta^j = \zeta^{(p-1)j}\pi \text{ for all } j. \tag{7.7}$$

In particular, setting $j = \frac{p+1}{2}$, we get $\alpha^{-1}\pi\alpha = \zeta^{\frac{p^2-1}{2}}\pi = -\pi$ (recall that ζ is a root of unity of order $p^2 - 1$ and $\alpha = \zeta^{\frac{p+1}{2}}$), which immediately implies (ii).

We proceed with the proof of (2). We will apply Observation 7.7 with $G = \mathrm{PGL}_1(O_D)$ and $H = \mathrm{PGL}_1^1(O_D)$. Our goal is to show that (in the notations of Observation 7.7) $m_1 = 1$ and $m_2 = m_3 = \frac{p+1}{2}$, whence the number of H-orbits on $\mathcal{MF}(D)$ is equal to $1 + 2 \cdot \frac{p+1}{2} = p + 2$, as desired.

By Lemma 7.9(d), $G/H = \mathrm{PGL}_1(O_D)/\mathrm{PGL}_1^1(O_D)$ is isomorphic to $\mathbb{F}_{p^2}^\times/\mathbb{F}_p^\times$ (so in particular is cyclic of order $p+1$) and is generated by the image of ζ. Hence the projection of $[\alpha] = [\zeta^{\frac{p+1}{2}}]$ to G/H has order 2, so $[H\langle[\alpha]\rangle : H] = 2$.

Since $\zeta \in K_1 \cap G \subset [S_1] \cap G$, we have $G = H\langle[\zeta]\rangle = H([S_1] \cap G)$, and therefore $m_1 = [G : H([S_1] \cap G)] = 1$. If $i = 2$ or 3, by Claim 7.16 below we have $H([S_i] \cap G) = H\langle[\alpha]\rangle$, whence $m_i = [G : H([S_i] \cap G)] = \frac{[G:H]}{[H\langle[\alpha]\rangle:H]} = \frac{p+1}{2}$. This finishes the proof of (2).

Claim 7.16. *Let $i = 2$ or 3. Then $H([S_i] \cap G) = H\langle[\alpha]\rangle$.*

Proof. The inclusion $H\langle[\alpha]\rangle \subseteq H([S_i] \cap G)$ is clear since $\alpha \in S_i \cap \mathrm{GL}_1(O_D)$. For the reverse inclusion, it suffices to prove the corresponding inclusion for the preimages in $\mathrm{GL}_1(D)$, that is, $\mathbb{Q}_p^\times \cdot \mathrm{GL}_1^1(O_D)(S_i \cap \mathrm{GL}_1(O_D)) \subseteq \mathbb{Q}_p^\times \cdot \mathrm{GL}_1^1(O_D) \cdot A$ where $A = \langle\alpha\rangle$.

Since $S_i = K_i^\times A$ as proved above and $A \subseteq \mathrm{GL}_1(O_D)$, we have

$$\mathrm{GL}_1^1(O_D)(S_i \cap \mathrm{GL}_1(O_D)) = \mathrm{GL}_1^1(O_D) \cdot (K_i^\times A \cap \mathrm{GL}_1(O_D)) = \mathrm{GL}_1^1(O_D) \cdot (K_i^\times \cap \mathrm{GL}_1(O_D)) \cdot A.$$

Since K_i is ramified, it is easy to see that $K_i^\times \cap \mathrm{GL}_1(O_D) \subseteq \mathbb{Q}_p^\times \cdot \mathrm{GL}_1^1(O_D)$ and hence $\mathbb{Q}_p^\times \cdot \mathrm{GL}_1^1(O_D)(S_i \cap \mathrm{GL}_1(O_D)) \subseteq \mathbb{Q}_p^\times \cdot \mathrm{GL}_1^1(O_D) \cdot A$, as desired. □

(3) We will again apply Observation 7.7, this time with $G = \mathrm{PGL}_1^1(O_D)$ and H as in Theorem 7.15(3). The proof of (2) shows that G has $p+2$ orbits on $\mathcal{MF}(D)$, with representatives $K_1, K_2, \ldots, K_{p+2}$ (with K_1, K_2 and K_3 defined as before) where $K_2, \ldots, K_{p+2}$ are all ramified. We will show that $m_1 = m_i = p$ for unique $2 \le i \le p+2$ (depending on H) and $m_j = 1$ for $j \neq 1, i$. This would imply that $\mathrm{NAC}(H) = \sum m_i = p + p + p \cdot 1 = 3p$, as desired.

The quotient $Q = \mathrm{PGL}_1^1(O_D)/\mathrm{PGL}_1^2(O_D)$ is a 2-dimensional vector space over $\mathbb{F}_p$. This follows from Lemma 7.9(e) and the fact that $r_1(\mathbb{Q}_p) = 0$ in the notations of Lemma 7.8. For a subfield $K \in \mathcal{MF}(D)$ we set $O_K^1 = K \cap \mathrm{GL}_1^1(O_D)$, and let $Q(K)$ be the projection of O_K^1 to Q. We claim that

(i) if K is unramified, then $Q(K) = \{0\}$;
(ii) if K is ramified, then $|Q(K)| = p$ (so $Q(K)$ is a 1-dimensional subspace of Q);
(iii) the map $\iota : K \mapsto Q(K)$ is a bijection between the G-orbits of ramified subfields $K \in \mathcal{MF}(D)$ and 1-dimensional spaces of Q.

Indeed, it is straightforward to check that $|Q(K)| = p^{r_1(K) - r_1(\mathbb{Q}_p)}$ in the notations of Lemma 7.8. According to that lemma, $r_1(\mathbb{Q}_p) = 0$, and for $K \in \mathcal{MF}(D)$ we have $r_1(K) = 0$ if K is unramified and $r_1(K) = 1$ if K is ramified. This yields (i) and (ii).

Let us now prove (iii). If $K, L \in \mathcal{MF}(D)$ lie in the same G-orbit, we must have $Q(K) = Q(L)$ since $G = \mathrm{PGL}_1^1(O_D)$ acts trivially on Q. Thus, ι is well defined. Since every element of D lies in a maximal subfield, every 1-dimensional subspace V of Q is contained in $Q(K)$ for some $K \in \mathcal{MF}(D)$, and by (i) and (ii) $V = Q(K)$ and K must be ramified. Thus ι is surjective. Finally, Q has $p+1$ one-dimensional subspaces (since $\dim(Q) = 2$) and we already observed that there are $p+1$ G-orbits of ramified maximal subfields. Thus, ι is bijective.

The computation of the subfield stabilizers in (2) shows that $Stab_G(K) = [K^\times] \cap G$ for every $K \in \mathcal{MF}(D)$. Hence $m_i = [G : H \cdot ([K^\times] \cap G)]$ is equal to $[Q : Q(H) + Q(K)]$ where $Q(H)$ is the projection of H onto Q. Since $|Q(H)| = p$, we have $m_i = p$ if either $Q(K_i) = \{0\}$ or $Q(K_i) = Q(H)$ and $m_i = 1$ otherwise. By (i) we have $Q(K_1) = Q(W) = \{0\}$, and by (iii) there exists a unique $2 \le i \le p+2$ such that $Q(K_i) = Q(H)$, which yields the above assertion about the m_i's and proves that $\mathrm{NAC}(H) = 3p$.

It remains to show that for $p = 3$, the group $G = \mathrm{PGL}_1^1(O_D)$ contains a torsion-free subgroup of index $p = 3$. It will be convenient to replace $\mathrm{PGL}_1^1(O_D)$ by $\mathrm{SL}_1^1(O_D)$ (which is isomorphic to $\mathrm{PGL}_1^1(O_D)$ by Lemma 7.10(d)), so that G becomes a subgroup of $\mathrm{GL}_1(D)$.

There exists a unique (up to isomorphism) quadratic extension of $\mathbb{Q}_3$ containing a primitive 3rd root of unity, which will be denoted below by $\sqrt[3]{1}$ (this is because $\sqrt[3]{1}$ has degree 2 over $\mathbb{Q}_3$), and it is straightforward to check that such an extension is ramified (a detailed computation shows that K_3, not K_2, contains $\sqrt[3]{1}$, but this fact will be of no importance for us). Morever, if $K \in \mathcal{MF}(D)$ contains a 3rd root of unity ζ, then ζ has non-trivial projection in Q.

Choose any ramified $L \in \mathcal{MF}(D)$ which does not contain $\sqrt[3]{1}$ and let H be the unique index 3 subgroup of G such that $Q(H) = Q(L)$. Suppose that H contains an element ω of order 3, and let $M = \mathbb{Q}_3(\omega)$. Then $M \ncong L$ (since M contains a primitive 3rd root of unity while L does not), whence $Q(M) \ne Q(L)$ by (iii) above, and therefore, $Q(M) \cap Q(L) = \{0\}$. The latter is impossible since the image of ω lies in both $Q(M)$ and $Q(H) = Q(L)$. Thus, we proved that H has no elements of order 3. Since H is a pro-3 group, it follows that H is torsion-free, as desired. □

8. On values of NCC for infinite pro-p groups and families of finite p-groups

In this section we will prove the results stated in § 1.4 including Theorems 1.6, 1.7 and 1.8. We will start with the proof of Theorem 1.6:

Theorem 1.6. *For any prime p and integer k there are only finitely many infinite pro-p groups G with $\mathrm{NCC}(G) = k$.*

We first establish an auxiliary result.

Lemma 8.1. *Let D be the quaternion division algebra over $\mathbb{Q}_p$. Let G be an open subgroup of $\mathrm{PGL}_1^3(O_D)$, and let H be an open subgroup of index p in G (note that H must be normal in G). Then $\mathrm{NCC}(H) > \mathrm{NCC}(G)$.*

Remark. The group $\mathrm{PGL}_1^3(O_D)$ is torsion-free for all p, so G and H must be torsion-free.

Proof. By Lemma 7.3 and Corollary 7.14, if U is any open torsion-free subgroup of $\mathrm{PGL}_1(D)$, then $\mathrm{NCC}(U)$ is equal to the number of orbits of the action of U on $\mathcal{MF}(D)$. Thus, we just need to show that at least one of the G-orbits decomposes into several H-orbits. By Observation 7.7 and the remark after it, this is equivalent to the existence of $K \in \mathcal{MF}(D)$ such that $G \ne H \cdot Stab_G(K)$.

Claim 8.2. *For any $K \in \mathcal{MF}(D)$ we have $Stab_G(K) = (K^\times/\mathbb{Q}_p^\times) \cap G$.*

Proof. As observed before, $Stab_G(K)/((K^\times/\mathbb{Q}_p^\times) \cap G)$ embeds into $\mathrm{Gal}\,(K/\mathbb{Q}_p)$, so the index $[Stab_G(K) : (K^\times/\mathbb{Q}_p^\times) \cap G]$ is at most 2. Since G is pro-p (and hence so is $Stab_G(K)$), the index is 1 if $p > 2$, and we are done in this case. Now consider the case $p = 2$ and write

$K = \mathbb{Q}_p(\alpha)$ with $\alpha^2 \in \mathbb{Q}_p$. Suppose that there exists $g \in Stab_G(K) \setminus ((K^\times/F^\times) \cap G)$. Then for any lift $\widetilde{g}$ of g, the conjugation by $\widetilde{g}$ induces a non-trivial automorphism of $K/\mathbb{Q}_p$, whence $\widetilde{g}^{-1}\alpha\widetilde{g} = -\alpha$ or, equivalently, $[\alpha, \widetilde{g}] = -1$. Since $G \subseteq \mathrm{PGL}_1^3(O_D)$, we can assume that $\widetilde{g} \in \mathrm{GL}_1^3(O_D)$, and since $\mathrm{GL}_1^3(O_D)$ is normal in $\mathrm{GL}_1(D)$, it follows that $-1 = [\alpha, \widetilde{g}] \in \mathrm{GL}_1^3(O_D)$, a contradiction. □

We proceed with the proof of Lemma 8.1. Since G is not procyclic and H has index p in G, there exists $x \in H \setminus \Phi(G)$. Let $K = F(\widetilde{x})$ where $\widetilde{x} \in D$ is any lift of x. Since G is torsion-free, the group $C = (K^\times/F^\times) \cap G$ is procyclic as shown in the proof of Corollary 7.14. Since C is also pro-p and $x \in C \setminus \Phi(G) \subseteq C \setminus \Phi(C)$, it follows that $C = \overline{\langle x \rangle}$. Hence using Claim 8.2 we get $H \cdot Stab_G(K) = H \cdot \overline{\langle x \rangle} = H \neq G$, as desired. □

Proof of Theorem 1.6. By Theorem 1.3 we can assume that G is an open torsion-free subgroup of $\mathrm{PGL}_1(D)$ where D is the quaternion division algebra over $\mathbb{Q}_p$. Let $U = G \cap \mathrm{PGL}_1^3(O_D)$. Then $[\mathrm{PGL}_1^3(O_D) : U] = p^m$ for some $m \in \mathbb{Z}_{\geq 0}$, and we can find a descending chain $\mathrm{PGL}_1^3(O_D) = H_0 \supseteq H_1 \supseteq \cdots \supseteq H_m = U$ with $[H_i : H_{i+1}] = p$ for all i. By Claim 8.1, $\mathrm{NCC}(U) \geq \mathrm{NCC}(\mathrm{PGL}_1^3(O_D)) + m > m$.

On the other hand, if we set $a = [\mathrm{PGL}_1(D) : \mathrm{PGL}_1^3(O_D)]$, then by Lemma 2.2, $\mathrm{NCC}(U) \leq [G : U] \cdot \mathrm{NCC}(G) \leq a \cdot \mathrm{NCC}(G)$, whence $\mathrm{NCC}(G) \geq \frac{\mathrm{NCC}(U)}{a} > \frac{m}{a}$. Since we also have $[\mathrm{PGL}_1(D) : G] \leq [\mathrm{PGL}_1(D) : U] \leq a \cdot p^m$, it follows that

$$\mathrm{NCC}(G) > \frac{\log_p[\mathrm{PGL}_1(D) : G] - \log_p a}{a}.$$

Since $\mathrm{PGL}_1(D)$ is finitely generated, it has finitely many subgroups of a given finite index, and therefore there are only finitely many G with a given value of NCC. □

Let us now recall the definition of the sets $\mathrm{NCC}_I(p)$ and $\mathrm{NCC}_{II}(p)$:

(i) Let $\mathrm{NCC}_I(p)$ be the set of all $k > 1$ for which there exists an infinite pro-p group G with $\mathrm{NCC}(G) = k$.
(ii) Let $\mathrm{NCC}_{II}(p)$ be the set of all $k > 1$ for which there exists an infinite family of finite p-groups $\{P_i\}$ with $\mathrm{NCC}(P_i) = k$ for all i.

We already explained why $\mathrm{NCC}_I(p) \subseteq \mathrm{NCC}_{II}(p)$. The following claim implies that $\mathrm{NCC}_I(p)$ and $\mathrm{NCC}_{II}(p)$ have the same minimal element.

Claim 8.3. *Suppose that for some k there exists an infinite sequence of noncyclic finite p-groups $\{P_i\}$ with $\mathrm{NCC}(P_i) \leq k$ for all i. Then there exists an infinite non-procyclic pro-p group G with $\mathrm{NCC}(G) \leq k$. Moreover, if $d(P_i) = d$ for all i, we can assume that $d(G) = d$.*

Proof. First observe that if P is a finite p-group and $d = d(G)$, then $P/\Phi(P) \cong (\mathbb{Z}/p\mathbb{Z})^d$ whence $\mathrm{NCC}(P) \geq \mathrm{NCC}((\mathbb{Z}/p\mathbb{Z})^d) = \frac{p^d-1}{p-1}$. Hence for any family of finite p-groups with bounded NCC, the sequence $\{d(P_i)\}$ is also bounded. Thus, it suffices to prove Claim 8.3 assuming that there exists $d \in \mathbb{N}$ such that $d(P_i) = d$ for all i.

Consider the following oriented graph $\Gamma_{k,d}(p)$. The vertices of $\Gamma_{k,d}(p)$ are (isomorphism classes of) finite p-groups P with $d(P) = d$ and $\mathrm{NCC}(P) \leq k$ (thus by our hypothesis $\Gamma_{k,d}(p)$ is infinite). There is an oriented edge from P to Q if and only if $Q \cong P/Z$ where $|Z| = p$ and $Z \subseteq \Phi(P)$.

Any finite p-group P with $d(P) = d$ and $P \ncong (\mathbb{Z}/p\mathbb{Z})^d$ has a central subgroup Z of order p lying in $\Phi(P)$. Therefore, for any such P there is a directed path from P to

$(\mathbb{Z}/p\mathbb{Z})^d$ in $\Gamma_{k,d}(p)$. In particular $\Gamma_{k,d}(p)$ is connected and thus contains an infinite path $Q_1 \leftarrow Q_2 \leftarrow Q_3 \leftarrow \cdots$. Let $G = \varprojlim Q_i$. Since $d(Q_i) = d$ for all i, we have $d(G) = d$. Also by Lemma 2.12, $\mathrm{NCC}(G) = \sup\{\mathrm{NCC}(Q_i)\}$, so $\mathrm{NCC}(G) \leq k$, as desired. □

Recall that the common minimal element of $\mathrm{NCC}_I(p)$ and $\mathrm{NCC}_{II}(p)$ is denoted by $\mathrm{NCC}_{min}(p)$. We are now ready to prove Theorem 1.7 giving the formula for $\mathrm{NCC}_{min}(p)$:

Theorem 1.7.

$$\mathrm{NCC}_{min}(p) = \begin{cases} 3 & \text{if } p = 2 \\ 9 & \text{if } p = 3 \\ p+2 & \text{if } p > 3. \end{cases}$$

Proof. Case 1: $p = 2$. The infinite prodihedral group is a non-procyclic pro-2 group with NCC equal to 3. On the other hand, every nonprocyclic pro-p group maps onto $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ whose NCC is $p + 1$. Thus, $\mathrm{NCC}_{min}(2) = 3$.

Case 2: $p > 3$. Let D be the quaternion division algebra over $\mathbb{Q}_p$ and $G = \mathrm{PGL}_1^1(O_D)$. By Theorem 7.15(2) and the remark after it we have $\mathrm{NAC}(G) = \mathrm{NCC}(G) = p + 2$, so $\mathrm{NCC}_{min}(p) \leq p + 2$. On the other hand,

- every infinite non-procyclic pro-p group H with finite NCC is an open subgroup of G by Theorem 1.3 and the remark after it,
- $\mathrm{NCC}(H) = \mathrm{NAC}(H)$ for any such H by Corollary 7.14, and
- $\mathrm{NAC}(H) \geq \mathrm{NAC}(G)$ for any such H by Corollary 7.4(ii).

This proves the reverse inequality $\mathrm{NCC}_{min}(p) \geq p + 2$.

Case 3: $p = 3$. Let D and G be as in Case 2. This time G is not torsion-free and hence has infinite NCC by Proposition 9.2 (which will be proved without relying on any results from § 8). However, by Theorem 7.15(3) G has an index 3 torsion-free subgroup H with $\mathrm{NCC}(H) = 9$. Since G is a pro-3 group, every proper open subgroup of G is contained in an index 3 subgroup, and $\mathrm{NAC}(U) = 9$ for any index 3 subgroup U of G (again by Theorem 7.15(3)). Thus arguing as in Case 2, we deduce that $\mathrm{NCC}_{min}(3) = 9$. □

We now turn to the proof of Theorem 1.8. Part (a) of Theorem 1.8 is an immediate consequence of Lemma 2.12 and Claim 8.3. Part (b) of Theorem 1.8 can be reformulated as follows:

Theorem 8.4. *Fix a prime p. The following hold:*

1. *For any integer $1 \leq d \leq 3$ there exists an infinite pro-p group H with $d(H) = d$ and $\mathrm{NCC}(H) < \infty$.*
2. *Conversely, let H be any infinite pro-p group with $\mathrm{NCC}(H) < \infty$. Then $d(H) \leq 3$ if $p > 3$, $d(H) \leq 4$ if $p = 3$ and $d(H) \leq 6$ if $p = 2$.*

Proof. In both parts of the proof D will denote the quaternion division algebra over $\mathbb{Q}_p$. We also set $G = \mathrm{PGL}_1(D)$ and $G_k = \mathrm{PGL}_1^k(O_D)$ for $k \in \mathbb{N}$.

(1) The assertion is trivial for $d = 1$. For all sufficiently large k, the group G_k is torsion-free and thus has finite NCC; moreover, it is a uniform pro-p group whence $d(G_k) = \dim(G_k) = 3$. Thus we proved (1) for $d = 3$. Finally, G_k is non-abelian and any two non-commuting elements of G_k generate an open subgroup (e.g. since $\mathfrak{sl}_1(D)$, the $\mathbb{Q}_p$-Lie algebra of $\mathrm{PGL}_1(D)$, has no subalgebras of dimension 2). This proves (1) for $d = 2$.

(2) Infinite procyclic pro-p groups and the infinite prodihedral pro-2 group trivially satisfy (2). Thus by Theorem 1.3 we can assume that H is an open torsion-free pro-p subgroup of $G = \mathrm{PGL}_1(D)$.

Case 1: $p > 2$. In this case $H \subseteq G_1$ by Lemma 7.9(f). Also, $G_1 \cong \mathrm{SL}_1^1(O_D)$ by Lemma 7.10(d), so we can apply [Er, Proposition 4.3] which collects various standard results about commutators and p^{th} powers in congruence subgroups of $\mathrm{SL}_1(D)$.

Let $H_2 = H \cap G_2$. The group G_2 is uniform by [Er, Proposition 4.3(b)(c)] whence $d(H_2) \leq d(G_2) = \dim(G_2) = 3$ where the inequality holds by [DDMS, Theorem 3.8]. Therefore, $d(H) \leq d(H_2) + d(H/H_2) = 3 + d(H/H_2)$. The quotient H/H_2 embeds into $G_1/G_2 \cong (\mathbb{Z}/p\mathbb{Z})^2$. If $H = H_2$, we are done. If $|H/H_2| = p^2$, then H projects onto G_1/G_2. Since $G_2 = [G_1, G_1]$ by [Er, Proposition 4.3(b)], it follows that $H = G_1$ whence $d(H) = d(G_1) = d(G_1/G_2) = 2$.

It remains to consider the case $|H/H_2| = p$. In this case we already know that $d(H) \leq 4$, so we proved Theorem 1.8(2) for $p = 3$, and we can assume now that $p > 3$. Fix any $h \in H \setminus H_2$, so that $H = \langle h \rangle H_2$. Since $p > 3$ and $h \in G_1 \setminus G_2$, [Er, Proposition 4.3(c)] implies that $h^p \in G_3 \setminus G_4$. Moreover, $\Phi(H_2) = [H_2, H_2]H_2^p$ is contained in G_4, so $h^p \in H_2 \setminus \Phi(H_2)$, and therefore H_2 contains a minimal generating set S (with $|S| \leq 3$ as already proved) containing h^p. But then $(S \setminus \{h^p\}) \cup \{h\}$ is a generating set for H of the same cardinality as S, so $d(H) \leq 3$, as desired.

Case 2: $p = 2$. In this case G_3 is uniform. Thus, if $H_3 = H \cap G_3$, as in Case 1 we have $d(H) \leq 3 + d(H/H_3)$. By Lemma 7.9, G/G_3 is a group of order 48, and it is easy to check that its 2-Sylow is non-abelian. Hence H/H_3 embeds into a non-abelian group of order 16 whence $d(H/H_3) \leq 3$ and thus $d(H) \leq 6$, as desired. □

We finish this section by connecting Problem 4 (formulated at the end of § 1.4) to the structure of the graph $\Gamma_{k,d}(p)$ from the proof of Claim 8.3. To make the relation more transparent we will work not with $\Gamma_{k,d}(p)$ itself, but with a chosen spanning tree $T_{k,d}(p)$ (in fact, we could replace $\Gamma_{k,d}(p)$ by $T_{k,d}(p)$ already in the proof of Claim 8.3). Note that $T_{k,d}(p)$ is naturally a rooted tree where the root group is $(\mathbb{Z}/p\mathbb{Z})^d$. The edges (as defined in the proof of Claim 8.3) always point from a child to its parent. We will assume that $T_{k,d}(p)$ is drawn upside down, with the root at the top.

The infinite downward paths in $T_{k,d}(p)$ correspond bijectively to infinite pro-p groups G with $d(G) = d$ and $\mathrm{NCC}(G) \leq k$, so by Theorem 1.6 there are finitely many such paths. To answer the stronger question in Problem 4 in the affirmative it suffices to prove that there is a uniform bound on the sizes of finite branches in $T_{k,d}(p)$. A priori it is not even clear whether finite branches exist arbitrarily low in the tree, but there is one case where such branches do exist and can be described explicitly.

Consider the tree $T_{k,2}(2)$ for some $k \geq 3$. One of the infinite paths in this tree corresponds to the infinite prodihderal pro-2 group D_{2^∞} (in fact, if $k = 3$, this is the only infinite path). Given $n \geq 3$, let Q_{2^n} be the generalized quaternion group of order 2^n, and given $n \geq 4$, let SD_{2^n} be the semidihedral group or order 2^n. It is easy to show that $\mathrm{NCC}(Q_{2^n}) = \mathrm{NCC}(SD_{2^n}) = 3$. Neither Q_{2^n} nor SD_{2^n} (with the above restrictions on n) lie on the D_{2^∞} path, but both can be mapped onto $D_{2^{n-1}}$, so they are at distance one from that path. The next result shows that whenever $n > 2k$, the finite branches corresponding to Q_{2^n} and SD_{2^n} have length 1 and there are no other finite branches below the $2k^{\text{th}}$ level connected to the D_{2^∞} path.

Lemma 8.5. *Fix an integer $k \geq 3$. Let P be a group of order 2^n with $n \geq 2k$, and let Q be a group of order 2^{n+1} such that $Q/Z \cong P$ for some subgroup Z of Q of order 2 and $\mathrm{NCC}(Q) \leq k$. The following hold:*

(a) *If $P = D_{2^n}$, then Q is isomorphic to $D_{2^{n+1}}$, $Q_{2^{n+1}}$ or $SD_{2^{n+1}}$.*

(b) *P is not isomorphic to Q_{2^n} or SD_{2^n}.*

Proof. We will prove (a) and (b) simultaneously, so assume that $P = D_{2^n}$, Q_{2^n} or SD_{2^n}. In each case P has a cyclic subgroup of index 2, and let H be the preimage of this subgroup in Q. Then H is either cyclic or isomorphic to $\mathbb{Z}/2^{n-1}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. But in the latter case $\mathrm{NCC}(H) = n + 1$ whence $\mathrm{NCC}(Q) \geq \frac{\mathrm{NCC}(H)}{2} > k$, a contradiction.

Thus, Q is a non-abelian group of order 2^{n+1} with a cyclic subgroup of index 2. It is known that there are only 4 such groups up to isomorphism, including $D_{2^{n+1}}$, $Q_{2^{n+1}}$ and $SD_{2^{n+1}}$. The only other group on this list will be denoted by $M_{2^{n+1}}$. From the standard presentations of these groups, it is clear that for $D_{2^{n+1}}$, $Q_{2^{n+1}}$ and $SD_{2^{n+1}}$ the only quotient of order 2^n is isomorphic to D_{2^n}, and the only quotient of $M_{2^{n+1}}$ of order 2^n is isomorphic to $\mathbb{Z}/2^{n-1}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. This proves both (a) and (b). □

Remark. The trees $T_{k,d}(p)$ also make it easier to explain why the inclusion $NCC_I(p) \subseteq NCC_{II}(p)$ discussed earlier in this subsection may (potentially) be proper. Indeed, suppose that for some $k > 1$ there is an infinite family of finite p-groups $\{P_n\}$ with $d(P_n) = d$ and $NCC(P_n) = k$ which all lie on the branches of $T_{k,d}(p)$. Then the infinite pro-p group G with $d(G) = d$ and $NCC(G) \leq k$ constructed in the proof of Claim 8.3 is not guaranteed to map onto any P_n, so it is possible that $NCC(G) < k$ (in which case G could have been constructed by applying the proof of Claim 8.3 already to $\Gamma_{k-1,d}(p)$).

9. Proof of Theorem 1.3

Throughout this section p will be a fixed prime and D will denote the quaternion division algebra over $\mathbb{Q}_p$. The goal of this section is to prove Theorem 1.3. The proof will be divided into three parts.

- *Part 1:* Prove that any pro-p group with finite NCC must be finite, infinite procyclic, infinite pro-dihedral (with $p = 2$) or isomorphic to an open subgroup of $\mathrm{PGL}_1(D)$. This will be proved in § 9.1.
- *Part 2:* Prove that all groups listed in the previous paragraph do have finite NCC. This has already been established. Indeed, the result is obvious for finite, infinite procyclic and infinite pro-dihedral groups and holds by Corollary 7.14(b) for open torsion-free subgroups of $\mathrm{PGL}_1(D)$.
- *Part 3:* Prove that open pro-p subgroups of $\mathrm{PGL}_1(D)$ with torsion (such groups only exist for $p = 2$ and $p = 3$) have infinite NCC. This will be proved in § 9.2.

9.1. **Proof of Theorem 1.3, part 1.** In this subsection we will complete the first part of the proof of Theorem 1.3 by establishing the following result:

Proposition 9.1. *Let G be a pro-p group with finite NCC. Then G is finite, infinite procyclic, infinite prodihedral (with $p = 2$) or isomorphic to an open subgroup of $\mathrm{PGL}_1(D)$.*

Proof. First of all, by Theorem 6.1 G must be p-adic analytic. Let H be an open uniform subgroup of G. By Lemma 2.2, H also has finite NCC and hence is just-infinite by Corollary 2.7. This easily implies that the $\mathbb{Q}_p$-Lie algebra $L_{\mathbb{Q}_p} = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} L(H)$ has no proper nonzero ideals, that is, $L_{\mathbb{Q}_p}$ is either simple (non-abelian) or one-dimensional (and thus isomorphic to $\mathbb{Q}_p$).

Case 1: $L_{\mathbb{Q}_p} \cong \mathbb{Q}_p$. In this case G must be virtually $\mathbb{Z}_p$. Let Z be an open normal subgroup of G isomorphic to $\mathbb{Z}_p$, and let $\varphi : G \to \mathrm{Aut}(Z)$ be the map induced by conjugation. Since Z is abelian, φ is not injective, and since G is just-infinite, $\mathrm{Im}\,\varphi$ must be

finite; in fact, a finite p-group. It is clear that $\mathrm{Aut}(\mathbb{Z}_p) \cong \mathbb{Z}_p^\times$, and it is well known that $\mathbb{Z}_p^\times \cong \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z}$ for $p > 2$ and $\mathbb{Z}_2^\times \cong \mathbb{Z}_2 \times \mathbb{Z}/2\mathbb{Z}$ (see, e.g. [Go, Corollary 5.8.2]). Thus, if $p > 2$, then $\mathrm{Aut}(Z)$ has no non-trivial finite p-subgroups, so φ must be trivial, and if $p = 2$, then $\mathrm{Aut}(Z)$ has a unique non-trivial finite subgroup which has order 2. It follows that $C_G(Z)$, the centralizer of Z in G (which coincides with $\mathrm{Ker}\,\varphi$) equals the entire G if $p > 2$ and has index at most 2 in G if $p = 2$.

If $C_G(Z)$ contains a (non-trivial) torsion element g, then $\langle g \rangle \times Z$ is an open subgroup of G which is not just-infinite and hence has infinite NCC, contrary to Lemma 2.2. Thus, $C_G(Z)$ is torsion-free. A well-known theorem of Serre [Ser] asserts that a finitely generated pro-p group which is virtually free and torsion-free must be free. Thus, $C_G(Z) \cong \mathbb{Z}_p$. Recall that $C_G(Z) = G$ if $p > 2$, so we are done in the case. If $p = 2$, we know that G contains a subgroup U of index ≤ 2 isomorphic to $\mathbb{Z}_2$. Thus, $G \cong \mathbb{Z}_2$ as well or G contains a torsion element (necessarily of order 2) which acts on U by inversion, in which case G is the infinite prodihedral group.

Case 2: $L_{\mathbb{Q}_p}$ is simple.

Let r be the rank of $L_{\mathbb{Q}_p}$. By one of the definitions of the rank, $\dim C_{L_{\mathbb{Q}_p}}(x) \geq r$ for all $x \in L_{\mathbb{Q}_p}$ where $C_{L_{\mathbb{Q}_p}}(x)$ is the centralizer of x in $L_{\mathbb{Q}_p}$.

Since H has finite NCC, by Lemma 6.4 we must have $r = 1$. There are only two simple Lie algebras of rank 1 over $\mathbb{Q}_p$: $\mathfrak{sl}_2(\mathbb{Q}_p)$ and $\mathfrak{sl}_1(D)$.

First we rule out the possibility $L_{\mathbb{Q}_p} = \mathfrak{sl}_2(\mathbb{Q}_p)$. In this case, after passing to a subgroup of finite index if needed, we can assume that $H = \mathrm{SL}_2^m(\mathbb{Z}_p) = \{g \in \mathrm{SL}_2(\mathbb{Z}_p) : g \equiv I \mod p^m\mathbb{Z}_p\}$ for some m and hence $L(H) = p^m\mathfrak{sl}_2(\mathbb{Z}_p)$ (the action of H on $L(H)$ is by conjugation in the matrix algebra). We will obtain a contradiction similarly to Lemma 2.6.

For each $i \in \mathbb{N}$ let $x_i = p^m e + p^{mi} f \in p^m\mathfrak{sl}_2(\mathbb{Z}_p)$ where $e = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ and $f = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$. Since H has finite NCC, by Lemma 6.3, there exist $i < j$, $x \in L$, $h, h' \in H$ and $\lambda, \mu \in \mathbb{Z}_p$ such that $x_i = \lambda x^h$ and $x_j = \mu x^{h'}$. Since x_i and x_j both have degree m with respect to the congruence filtration $\{p^j\mathfrak{sl}_2(\mathbb{Z}_p)\}_{j=1}^\infty$ and the H-action does not change the degree with respect to this filtration, we deduce that λ and μ must have the same p-adic valuation.

On the other hand, taking the determinants of both sides in $x_i = \lambda x^h$ and $x_j = \mu x^{h'}$ and using the fact that the action of H on L preserves the determinants, we get

$$-p^{m(i+1)} = \lambda^2 \det(x) \quad \text{and} \quad -p^{m(j+1)} = \mu^2 \det(x).$$

Since $i < j$, μ and λ must have different p-adic valuations, a contradiction.

Before considering the case where $L_{\mathbb{Q}_p} = \mathfrak{sl}_1(D)$ we recall the notion of the commensurator of a profinite group which will play a key role in the remainder of the argument.

Definition. Let P be a profinite group. The *commensurator of* P, denoted $\mathrm{Comm}(P)$, is the group of equivalence classes of isomorphisms $\varphi : U \to V$ where U and V are open subgroups of P. Here two isomorphisms $\varphi : U \to V$ and $\varphi' : U' \to V'$ are equivalent if they coincide on an open subgroup of $U \cap U'$.

For any profinite group P the conjugation action of P on itself induces a canonical homomorphism $P \to \mathrm{Comm}(P)$. On the other hand, if Q is another profinite group which is commensurable to P (that is, Q and P have isomorphic open subgroups), then $\mathrm{Comm}(Q) \cong \mathrm{Comm}(P)$, and thus we obtain a homomorphism $\varphi : P \to \mathrm{Comm}(Q)$.

We proceed with the proof of Proposition 9.1. Recall that the only remaining case is $L_{\mathbb{Q}_p} = \mathfrak{sl}_1(D)$. In this case G is commensurable with $\mathrm{SL}_1(D)$, so as we just explained, there is a natural homomorphism $\varphi : G \to \mathrm{Comm}(\mathrm{SL}_1(D))$. The image of φ must be infinite (for otherwise, G is virtually abelian, which is clearly a contradiction) and hence by Corollary 2.7, the kernel of φ must be trivial, so G embeds into $\mathrm{Comm}(\mathrm{SL}_1(D))$.

We claim that $\mathrm{Comm}(\mathrm{SL}_1(D)) \cong \mathrm{PGL}_1(D)$. Indeed, by [BEW, Theorem 3.12], if H is any compact p-adic analytic group, then $\mathrm{Comm}(H)$ is isomorphic to $\mathrm{Aut}_{\mathbb{Q}_p}(L_{\mathbb{Q}_p}(H))$, so $\mathrm{Comm}(\mathrm{SL}_1(D)) \cong \mathrm{Aut}_{\mathbb{Q}_p}(\mathfrak{sl}_1(D))$. By [JT, Proposition 8.1], $\mathrm{Aut}_{\mathbb{Q}_p}(\mathfrak{sl}_1(D))$ is isomorphic to $\mathrm{Aut}_{\mathbb{Q}_p}(D)$, the group of automorphisms of D considered as an associative $\mathbb{Q}_p$-algebra.[6] Finally, $\mathrm{Aut}_{\mathbb{Q}_p}(D) \cong \mathrm{PGL}_1(D)$ by the Skolem-Noether theorem.

Thus, we proved that G is isomorphic to a (closed) subgroup of $\mathrm{PGL}_1(D)$, and since G is commmesurable with $\mathrm{PGL}_1(D)$, this subgroup must be open (e.g. since $\mathrm{PGL}_1(D)$ is compact p-adic analytic, so its closed non-open subgroups have strictly smaller dimension). This completes the proof of Proposition 9.1. □

9.2. **Proof of Theorem 1.3, part 3.** In this subsection we will prove the following result which completes the proof of Theorem 1.3.

Proposition 9.2. *Let G be an open pro-p subgroup of $\mathrm{PGL}_1(D)$ with torsion. Then G has infinite NCC.*

Proof. Since G is a pro-p group with torsion, it must contain an element g_0 of order p (such an element will be fixed for the rest of the proof). We will prove that G has infinite NCC by once again exploiting the idea from the proof of Lemma 2.6.

Claim 9.3. *For any open subgroup U of G there exists $h \in U$ such that $(g_0 h)^p \neq 1$.*

Claim 9.3 can be proved by direct computation, but it also follows from a theorem of Breuillard and Gelander [BG, Proposition 1.9] which asserts that a non-virtually solvable p-adic analytic group cannot satisfy a coset identity (that is, an identity which holds for all elements in a given coset of an open subgroup).

For the rest of the proof, given $g \in G$ we will denote by $\deg(g)$ the degree of g with respect to the congruence filtration, that is, $\deg(1) = \infty$, and if $1 \neq g$, $\deg(g)$ is the unique $k \geq 0$ such that $g - 1 \in \pi^k O_D \setminus \pi^{k+1} O_D$ (recall that π is a uniformizer of D). The following are clear:

(i) Conjugate elements have the same degree.
(ii) Let $1 \neq g \in G$ and $\alpha \in \mathbb{Z}_p$. If $\alpha \notin p\mathbb{Z}_p$, then $\deg(g^\alpha) = \deg(g)$, and if $\alpha \in p\mathbb{Z}_p$, then $\deg(g^\alpha) > \deg(g)$.
(iii) $\deg(gh) \geq \min\{\deg(g), \deg(h)\}$, and equality holds whenever $\deg(g) \neq \deg(h)$.

By Claim 9.3 we can construct an infinite sequence $\{h_k \in G\}_{k=1}^\infty$ such that $\deg(h_k) > \deg(g_0)$ for all k, $\deg(h_k) \to \infty$ and $(g_0 h_k)^p \neq 1$ for all k. Moreover, since $g_0^p = 1$, the element $(g_0 h_k)^p$ lies in the normal subgroup generated by h_k, so we can ensure that the sequence $\{\deg((g_0 h_k)^p)\}_{k=1}^\infty$ is strictly increasing simply by choosing h_k of sufficiently large degree (once all the previous elements have been chosen).

Let $g_k = g_0 h_k$, and suppose that G has finite NCC. Then there exist $i \neq j$ such that g_i and g_j lie in conjugates of the same procyclic subgroup $\overline{\langle g \rangle}$. Thus there exist $a, b \in G$ and $\alpha, \beta \in \mathbb{Z}_p$ such that $g_i^a = g^\alpha$ and $g_j^b = g^\beta$. At least one of the p-adic numbers

[6] The result in [JT] is stated only for $p = 2$, but the proof works for all p.

$\frac{\alpha}{\beta}$ and $\frac{\beta}{\alpha}$ lies in $\mathbb{Z}_p$, and without loss of generality we can assume that $\frac{\alpha}{\beta} \in \mathbb{Z}_p$. Then $g_i^a = g^\alpha = (g^\beta)^{\frac{\alpha}{\beta}} = (g_j^b)^{\frac{\alpha}{\beta}}$. Hence $g_i^c = g_j^\gamma$ for some $c \in G$ and $\gamma \in \mathbb{Z}_p$, namely $c = ab^{-1}$ and $\gamma = \frac{\alpha}{\beta}$.

If $\gamma \in p\mathbb{Z}_p$, we get an immediate contradiction since in this case $\deg(g_j^\gamma) > \deg(g_j)$ by property (ii) above, while using (i), (ii) and (iii) we have $\deg(g_j) = \deg(g_0) = \deg(g_i) = \deg(g_i^c)$. Thus, $\gamma \in \mathbb{Z}_p \setminus p\mathbb{Z}_p = \mathbb{Z}_p^\times$. But then raising both sides of the equality $g_i^c = g_j^\gamma$ to the p^{th} power, we get $(g_i^p)^c = (g_j^p)^\gamma$, whence using (i) and (ii) again $\deg(g_i^p) = \deg((g_i^p)^c) = \deg((g_j^p)^\gamma) = \deg(g_j^p)$. This contradicts our original hypothesis that the sequence $\deg(g_k^p)$ is strictly increasing. □

10. Profinite groups with finite NCC

In this section we complete the proof of Theorem 1.5 by establishing the following result.

Theorem 10.1. *Let G be a prosolvable group with finite NCC, and suppose that $G^{(i)}$ is pronilpotent for some i. Then G is virtually pronilpotent.*

Theorem 10.1 is a fairly easy consequence of the following proposition:

Proposition 10.2. *Let G be a metabelian profinite group with finite NCC, and write G as an extension $1 \to A \to G \to C \to 1$ where both A and C are abelian. Let $\pi : C \to \mathrm{Aut}(A)$ be the map induced by the conjugation action of G on A. Then $\pi(C)$ is finite.*

We will first prove Theorem 10.1 assuming Proposition 10.2 and then prove Proposition 10.2.

Proof of Theorem 10.1. Let us consider the set of all pairs (H, k) where H is an open subgroup of G and $k \in \mathbb{Z}_{\geq 0}$ is such that $H^{(k)}$ is pronilpotent (by hypotheses this set is non-empty). Among all such pairs (H, k) choose one where k is minimal. Theorem 10.1 is equivalent to the assertion that $k = 0$.

First we assume that $k \geq 2$ and consider the metabelian group $Q = H/H^{(2)}$. We claim that Q is virtually procyclic. Indeed, Q has finite NCC (since H does), and hence by Proposition 10.2 (applied with $A = [Q, Q]$ and $C = Q/[Q, Q]$), Q has an open subgroup V such that $[V, [Q, Q]] = \{1\}$. Thus, V is nilpotent of class ≤ 2. The fact that V (and hence Q) is virtually procyclic can be proved by an easy direct argument, but it also follows from the classification of groups with finite NCC in the pronilpotent case (Corollary 1.4) which is already completed at this stage. Indeed, since open subgroups of groups of the form $\mathrm{SL}_1(D)$ are never nilpotent, in the notations of Corollary 1.4 applied to $G = V$, each subgroup H_i must be finite or the prodihedral pro-2 group, so V is a product of finitely many virtually procyclic groups of pairwise corime orders and hence V itself is vritually procyclic.

Thus H has an open subgroup M whose image in Q is procyclic and in particular abelian. Then $[M, M] \subseteq H^{(2)}$, whence $M^{(k-1)} = [M, M]^{(k-2)} \subseteq (H^{(2)})^{(k-2)} = H^{(k)}$, and so $M^{(k-1)}$ is pronilpotent. Since M is open in H and hence in G, this contradicts minimality of k. Thus we proved that $k \leq 1$.

Since $k \leq 1$, the group $K = [H, H]$ is pronilpotent. We will now use this fact to prove directly that H (and hence G) is virtually pronilpotent. By Proposition 10.2 (applied exactly as earlier in the proof), $Q = H/H^{(2)}$ has an open subgroup V such that $[V, [Q, Q]] = \{1\}$. Replacing V by $V[Q, Q]$ (which does not affect the latter condition), we

can assume that $V \supseteq [Q,Q]$. If U is the preimage of V in H, then U is an open subgroup of H containing $K = [H,H]$ such that $[U,[H,H]] \subseteq H^{(2)}$, that is, $[U,K] \subseteq [K,K]$. Then $\gamma_3(U) = [U,[U,U]] \subseteq [U,K] \subseteq [K,K]$.

A well-known theorem of P. Hall asserts that if X is a group which has a normal nilpotent subgroup Y such that $X/[Y,Y]$ is nilpotent, then X itself is nilpotent (see, e.g. [Ro, 5.2.10]). It is straightforward to extend this theorem to pronilpotent groups. We know that K is pronilpotent, and we just showed that $U/[K,K]$ is nilpotent of class ≤ 2. Hence by Hall's theorem U is pronilpotent. Since U is open in G, the proof is complete. □

Before proving Proposition 10.2, we need two more auxiliary results. The first one is a theorem of Schur and Zassenhaus which is classical in the case of finite groups and routinely extends to profinite groups.

Lemma 10.3 (Schur-Zassenhaus)**.** *Let P and Q be profinite groups of coprime orders. Then any extension $1 \to Q \to G \to P \to 1$ splits.*

The next result must also be well known, but we include the proof for completeness.

Lemma 10.4. *Let p and q be distinct primes. Let $G = Q \rtimes C$ where C is a cyclic group of order p^n and Q is a (non-trivial) elementary abelian q-group. Suppose that the image of C in $\mathrm{Aut}(Q)$ has order p^k and $C^{p^{k-1}}$ acts on Q without (nonzero) fixed points. Then G has no element of order $p^{n-k+1}q$.*

Proof. Suppose that $xy \in G$ has order $p^{n-k+1}q$ where $x \in Q$ and $y \in C$. Then $y = c^{p^{k-1}}$ for some generator c of C. Let $\varphi \in \mathrm{Aut}(Q)$ be the conjugation by y. Then for any $m \in \mathbb{N}$ we have $(xy)^m = \psi_m(x)y^m$ where $\psi_m(x) = \prod_{i=0}^{m-1} \varphi^i(x)$ (the order in the product does not matter since Q is abelian). By our hypotheses $\varphi^p = \mathrm{id}_Q$ while φ has no fixed points on Q. The first condition implies that $\psi_p(x)$ is fixed by φ, and hence the second condition implies that $\psi_p(x) = 1$. Thus, $(xy)^p = y^p = c^{p^k}$, whence $(xy)^{p^{n-k+1}} = c^{p^n} = 1$, a contradiction. □

We are finally ready to prove Proposition 10.2. For the convenience of the reader we repeat the statement.

Proposition 10.2. *Let G be a metabelian profinite group with finite NCC, and write G as an extension $1 \to A \to G \to C \to 1$ where both A and C are abelian. Let $\pi : C \to \mathrm{Aut}(A)$ be the map induced by the conjugation action of G on A. Then $\pi(C)$ is finite.*

Proof. First note that C is an abelian profinite group with finite NCC and hence virtually procyclic. Replacing C by an open subgroup, we can assume from now on that C itself is procyclic. Thus, C is a direct product of procyclic pro-p subgroups C_p. Each C_p is either a cyclic group of order p^{n_p} for some $n_p \in \mathbb{Z}_{\geq 0}$ or isomorphic to $\mathbb{Z}_p$, in which case we set $n_p = \infty$. Likewise A is a direct product of its Sylow pro-p subgroups A_p. Let $\pi_p : C \to \mathrm{Aut}(A_p)$ be the map induced by the conjugation action of C on A_p.

We will prove that $\pi(C)$ is finite in 3 steps. In Step 1 we will show that $\pi_p(C)$ is finite for each p. Then in Step 2 we will show that $\pi(C_p)$ is finite for each p. After establishing two more auxiliary results (Claims 10.7 and 10.8) we will finally prove that $\pi(C)$ is finite in Step 3.

Before proceeding, we introduce some additional notations and make some simple observations.

- Let $d_p = d(A_p)$ be the minimal number of generators of A_p. We will show that each d_p is finite (see Claim 10.5 below). Hence $V_p = A_p/A_p^p$ is a vector space over $\mathbb{F}_p$ of dimension d_p. Let $\rho_p : C \to \mathrm{GL}(V_p)$ be the composition of $\pi_p : C \to \mathrm{Aut}(A_p)$ with the canonical map $\mathrm{Aut}(A_p) \to \mathrm{GL}(V_p)$, and let K_p be the kernel of the natural projection $\pi_p(C) \to \rho_p(C)$.
- If P is any set of primes, define C_P (resp. A_P) to be the subgroup of C (resp. A) generated by all C_p (resp. A_p) with $p \in P$. Let F_P be the full preimage of C_P under the natural projection $G \to C$. Note that F_P is always a normal subgroup of G.
- Given two sets of primes P and Q, let $G_{Q,P} = F_P/A_{Q'}$ where Q' is the set of all primes not in Q. Note that $G_{Q,P}$ can be written as an extension
$$1 \to A_Q \to G_{Q,P} \to C_P \to 1$$
where for any $p \in P, q \in Q$ the conjugation action of C_p on A_q coincides with the corresponding action in G. Note that by Lemma 10.3, $G_{Q,P} = A_Q \rtimes C_P$ whenever P and Q are disjoint. Finally, by Lemma 2.1(i)(ii) we have
$$\mathrm{CC}(G_{Q,P}, G) \leq \mathrm{CC}(G, G) = \mathrm{NCC}(G)$$
(the action of G on $G_{Q,P}$ is induced from the conjugation action of G on F_P).

Claim 10.5. *Each d_p is finite.*

Proof. Fix a prime p, and let $\{G_i\}_{i=1}^{\infty}$ be any descending chain of open normal subgroups of G which form a base of neighborhoods of identity. Recall that $V_p = A_p/A_p^p$, and let $\{V_{p,i}\}_{i\in\mathbb{N}}$ be the filtration of V_p induced by $\{G_i\}$. Since G_i are open and normal in G, the subspaces $V_{p,i}$ are C-invariant and have finite codimension in V_p.

Suppose now that $d_p = \infty$. Then we can find an infinite sequence $i_1 < i_2 < \cdots$ such that the subspaces V_{p,i_k} are all distinct. Choose $v_k \in V_{p,i_k} \setminus V_{p,i_{k+1}}$. Then the subspaces $\mathbb{F}_p v_i$ and $\mathbb{F}_p v_j$ cannot be in the same C-orbit for $i \neq j$, so C acts on the set of 1-dimensional subspaces of V_p with infinitely many orbits. On the other hand, the number of such orbits is exactly $\mathrm{CC}(V_p, C)$, and by Lemma 2.1(i)(ii) $\mathrm{CC}(V_p, C) \leq \mathrm{NCC}(G)$. Since $\mathrm{NCC}(G) < \infty$, we reached a contradiction. □

Claim 10.6. *For each p, the group K_p is pro-p. Moreover, $\pi_p(C)$ is virtually pro-p and $|\pi_p(C_q)| = |\rho_p(C_q)|$ for any prime $q \neq p$.*

Proof. It will be convenient to write A_p additively (just in this proof). We first clarify the definition of topology on $\mathrm{Aut}(A_p)$. It is well known that whenever H is a finitely generated profinite group, its automorphism group $\mathrm{Aut}(H)$ is also profinite (see, e.g. [DDMS, Corollary 5.3]). Moreover, if $\{U_n\}$ is any chain of open characteristic subgroups of H which form a base of neighborhoods of 1 (such $\{U_n\}$ exists since H is finitely generated), the groups
$$\mathrm{Aut}(H; U_n) = \{g \in \mathrm{Aut}(H) : g(x) \equiv x \mod U_n \text{ for all } x \in H\}$$
form a base of neighborhoods of 1 in $\mathrm{Aut}(H)$. In our case $H = A_p$ is an abelian pro-p group which is finitely generated by Claim 10.5, so we can simply take $U_n = p^n A_p$.

Recall that K_p is the kernel of the projection $\pi_p(C) \to \rho_p(C)$, $\pi_p(C) \subseteq \mathrm{Aut}(A_p)$ and $\rho_p(C)$ is the image of $\pi_p(C)$ in $\mathrm{Aut}(A_p/pA_p)$. Thus in the above notations $K_p \subseteq \mathrm{Aut}(A_p; pA_p)$, and so every element $g \in K_p$ can be written as $g = 1 + v$ where v is a homomorphism from A_p to pA_p. Then for every $n \in \mathbb{N}$ we have $g^{p^n} = 1 + v_n$ where v_n

maps A_p to $p^n A_p$. Based on the above description of the topology on $\mathrm{Aut}(A_p)$, this means that $g^{p^n} \to 1$ as $n \to \infty$. Therefore every finite quotient of K_p is a p-group. Since K_p is profinite (being a closed subgroup of the profinite group $\mathrm{Aut}(A_p)$), we can conclude that K_p is pro-p.

Since d_p is finite, $\rho_p(C)$ is also finite and hence $\pi_p(C)$ is virtually pro-p. Finally, if q is a prime different from p, the intersection $\pi_p(C_q) \cap K_p$ must be trivial since $\pi_p(C_q)$ is a pro-q group. Therefore, $|\pi_p(C_q)| = |\rho_p(C_q)|$. □

We proceed with the rest of the proof in several steps.

Step 1: Each $\pi_p(C)$ is finite. Suppose that $\pi_p(C)$ is infinite. Since $\pi_p(C)$ is virtually pro-p, $\pi_p(C_p)$ must be infinite. Then $C_p \cong \mathbb{Z}_p$ (since C_p is procyclic). Also note that A_p is infinite (in particular, non-trivial) since $\pi_p(C) \subseteq \mathrm{Aut}(A_p)$. Thus we reach a contradiction applying Lemma 2.6 with $H = A$.

Step 2: Each $\pi(C_p)$ is finite. Once again, we will argue by contradiction, but this step is more involved. After initial preparations we will apply Lemma 10.4 and then Lemma 2.8 to derive a contradiction.

Suppose that $\pi(C_p)$ is infinite for some p. By Step 1, $\pi_q(C_p)$ is finite for all q. Since $\pi(C_p)$ embeds into the product $\prod_q \pi_q(C_p)$, we must have an infinite sequence of primes $q_1, q_2, \dots$ such that $|\pi_{q_i}(C_p)| \to \infty$ as $i \to \infty$ (otherwise, $\pi(C_p)$ has finite exponent and therefore is finite since by our initial assumption C and hence also C_p is procyclic). Without loss of generality we can assume that $p \notin \{q_i\}$. Also if we write $|\pi_{q_i}(C_p)| = p^{m_i}$, we can assume that $m_i > 0$ for all i and the sequence $\{m_i\}$ is strictly increasing.

Recall that $|\rho_q(C_p)| = |\pi_q(C_p)|$ for all $q \neq p$ by Claim 10.6. Thus $|\rho_{q_i}(C_p)| = p^{m_i}$ for all i. Let W_{q_i} be the set of elements of V_{q_i} fixed by $C_p^{p^{m_i-1}}$. Note that W_{q_i} is C_p-invariant. Since $q_i \neq p$, the representation of C_p on V_{q_i} is completely reducible by Maschke's theorem, so we can decompose $V_{q_i} = U_{q_i} \oplus W_{q_i}$ where U_{q_i} is C_p-invariant. Note that $U_{q_i} \neq 0$ by definition of m_i. Moreover, if $\lambda_{q_i}(C_p)$ is the projection of $\rho_{q_i}(C_p) \subseteq \mathrm{GL}(V_q)$ to $\mathrm{GL}(U_{q_i})$, then $|\lambda_{q_i}(C_p)| = |\rho_{q_i}(C_p)| = p^{m_i}$.

Let us now fix $k \in \mathbb{N}$, choose any $M \geq m_k$, and consider the group $G_{Q_k,\{p\}}$ where $Q_k = \{q_1, q_2, \dots, q_k\}$. By Lemma 10.3, $G_{Q_k,\{p\}} \cong (A_{q_1} \times \cdots \times A_{q_k}) \rtimes C_p$ and therefore $G_{Q_k,\{p\}}$ projects onto $(V_{q_1} \times \cdots \times V_{q_k}) \rtimes \widetilde{C_p}$ which, in turn, projects onto $R_k = (U_{q_1} \times \cdots \times U_{q_k}) \rtimes \widetilde{C_p}$ where $\widetilde{C_p} = C_p / C_p^{p^M}$. The advantage of using U_{q_j} rather than V_{q_j} in the definition of R_k is that Lemma 10.4 becomes applicable to the subgroup $U_{q_j} \rtimes \widetilde{C_p}$ (for any j).

Let c be a generator of $\widetilde{C_p}$. Since $C_p \cong \mathbb{Z}_p$ (otherwise, $\pi(C_p)$ could not be infinite), c has order p^M. Define the integers $e_1, \dots, e_k$ as follows:

$$e_1 = p^{M-m_1} q_1,\ e_2 = p^{M-m_2} q_1 q_2, \quad \dots, \quad e_k = p^{M-m_k} q_1 q_2 \cdots q_k.$$

All e_i are orders of elements of R_k. Indeed, choose non-trivial elements $y_i \in U_{q_i}$ for each i. Then by assumption $c^{p^{m_i}}$ acts trivially on U_{q_j} for $j \leq i$, so in particular commutes with y_j for $j \leq i$ and hence the element $c^{p^{m_i}} y_1 \cdots y_i$ has order e_i.

Moreover, we claim that e_i is a maximal element order (see the definition in § 2.3). Indeed, a quick verification shows that if some e_i is not maximal, then R_k must contain an element of order $p^{M-m_j+1} q_j$ for some j. Since $U_{q_j} \rtimes \widetilde{C_p}$ is a $\{p, q_j\}$-Hall subgroup of

R_k and is also normal, it contains all elements of order $p^a q_j^b$ in R_k. Thus, $U_{q_j} \rtimes \widetilde{C_p}$ must contain an element of order $p^{M-m_j+1}q_j$, which contradicts Lemma 10.4.

Thus we showed that $e_1, \dots, e_k$ are all maximal element orders of R_k and therefore $\mathrm{CC}(R_k, C) \geq k$ by Lemma 2.8. On the other hand, we have $\mathrm{CC}(R_k, C) \leq \mathrm{NCC}(G)$ by Lemma 2.1(i)(ii). Since k is arbitrary, we again have a contradiction. This completes Step 2.

Before finishing the proof, we establish two more auxiliary results. For each prime p choose a Sylow pro-p subgroup S_p of G. Note that S_p contains A_p, and the image of S_p in C is equal to C_p.

To avoid too much notation, for the rest of the proof the compositions of the maps $\pi_p : C \to \mathrm{Aut}(A_p)$ and $\rho_p : C \to \mathrm{Aut}(V_p)$ with the natural projection $G \to C$ will be denoted by the same symbols (π_p and ρ_p, respectively).

Claim 10.7. *The following hold:*

(a) *Let q be a prime, $1 \neq g \in S_q$, and let $J(g)$ be the set consisting of q and all primes $p \neq q$ such that g acts non-trivially on V_p. Then $x^g \equiv x \mod A_{J(g)}$ for all $x \in G$.*

(b) *Let p and q be distinct primes, $1 \neq g \in S_q$ and $1 \neq h \in S_p$. Then $[g, h] \in A_{J(g) \cap J(h)}$.*

Proof. (a) Let $I(g)$ be the set of all primes not in $J(g)$, and take any $p \in I(g)$. By assumption $p \neq q$ and $\rho_p(g)$ is trivial, so $\pi_p(g)$ lies in K_p, the kernel of the projection $\pi_p(G) \to \rho_p(G)$. But K_p is a pro-p group while g is a pro-q element, so $\pi_p(g)$ must be trivial as well.

Now let φ denote the conjugation by g. We just showed the following:

(*) φ is trivial on A_p for all $p \in I(g)$.

For any $x \in G$ we have $\varphi(x) \equiv x \mod A$, so there exists some $a \in A_{I(g)}$ such that $\varphi(x) \equiv xa \mod A_{J(g)}$. By (*) φ fixes a. Thus, applying φ to both sides we get

$$\varphi^2(x) \equiv \varphi(x)a \equiv xa^2 \mod A_{J(g)},$$

and by routine induction $\varphi^k(x) \equiv xa^k \mod A_{J(g)}$ for all $k \in \mathbb{N}$.

Now let N be any open normal subgroup of G. Since g is a pro-q element, φ induces an automorphism of order q^i on G/N for some $i \in \mathbb{Z}_{\geq 0}$. Thus, $xa^{q^i} \equiv x \mod A_{J(g)}N$. Equivalently, $a^{q^i} \equiv a_q \mod N$ for some $a_q \in A_{J(g)}$. Let α_q (resp. α) be the projection of a_q (resp. a) to G/N. Then $\alpha^{q^i} = \alpha_q$. Since α_q is a pro-$J(g)$ element and α is a pro-$I(g)$ element, by Observation 2.5(c) we must have $\alpha = \alpha_q = 1$, so $a \in N$. Since N is arbitrary, it follows that $a = 1$, so $\varphi(x) \equiv x \mod A_{J(g)}$ as desired.

(b) follows directly from (a) since $[g, h] = g^{-1}g^h = (h^{-1})^g h$. □

We will use the next claim to prove that $\pi(C)$ is finite by contradiction.

Claim 10.8. *Assume that $\pi(C)$ is infinite. Then there exist two infinite disjoint sets of primes $Q = \{q_1, q_2, \dots\}$ and $P = \{p_1, p_2, \dots\}$ such that each C_{p_i} acts non-trivially on A_{q_i} and trivially on A_{q_j} for all $j \neq i$.*

Proof. It will be convenient to use the following terminology. A prime p will be called

- *passive* if C_p acts trivially on all A_q;
- *isolated* if C_p acts non-trivially on A_p, but trivially on A_q for all $q \neq p$;

- *active* otherwise, that is, if C_p acts non-trivially on A_q (and hence also on V_q) for some $q \neq p$.

We construct the sets Q and P inductively. Suppose that for some $k \in \mathbb{Z}_{\geq 0}$ we constructed distinct primes $q_1, q_2, \ldots, q_k$ and $p_1, p_2, \ldots, p_k$ satisfying the above conditions for $i, j \leq k$. Our goal is to add q_{k+1} and p_{k+1} preserving the same conditions (the base case $k = 0$ is vacuously true).

Let U be the set containing all p_i and q_i for $i \leq k$ as well as all primes p such that either C_p acts non-trivially on A_{q_i} or A_{p_i} for some $i \leq k$ or C_{p_i} acts non-trivially on A_p for some $i \leq k$. By Steps 1 and 2, U is finite.

Since $\pi(C_p)$ is finite for each p by Step 2 while $\pi(C)$ is infinite, there must exist infinitely many primes $p \notin U$ such that C_p acts non-trivially on A, that is, p is active or isolated. If at least one $p \notin U$ is active, then C_p acts non-trivially on A_q for some $q \neq p$, and by construction $q \notin \{p_i, q_i\}_{i=1}^k$ as well, so we can set $p_{k+1} = p$ and $q_{k+1} = q$, completing the induction step.

Thus the only remaining possibility (which we will eventually rule out) is that

(**) there are no active primes outside of U and infinitely many isolated primes $r_1, r_2, \ldots$ outside of U.

By definition C_{r_i} acts non-trivially on A_{r_i} and trivially on A_q for all $q \neq r_i$.

(***) It is possible that C_p acts non-trivially on A_{r_i} for some $p \neq r_i$; however, any such p must be active and hence by (**) must lie in U.

Now for each prime t set $\widetilde{S}_t = S_t$ if $t \notin U$ and $\widetilde{S}_t = \operatorname{Ker} \pi \cap S_t$ if $t \in U$ and let $H = \prod_t \widetilde{S}_t$. Even though $\widetilde{S}_t$ need not be normal, it is straightforward to check that H is a group independent of the order in which the product is taken since H clearly contains A and G/A is abelian. It is also clear that $\widetilde{S}_t$ is a t-Sylow subgroup of H. Since $\pi(S_t)$ is finite for each t by Step 2 and U is finite, H is an open subgroup of G and hence $\mathrm{NCC}(H) < \infty$ by Lemma 2.2.

Let $r \notin U$ be an isolated prime. We claim that the r-Sylow $S_r = \widetilde{S}_r$ commutes with the t-Sylow $\widetilde{S}_t$ for all $t \neq r$ and thus $\widetilde{S}_r$ is a direct factor of H. Indeed, take any $1 \neq g \in S_r$ and $1 \neq h \in \widetilde{S}_t$, $t \neq r$. Then using the notations from Claim 10.7(a) we have $J(g) = \{r\}$ (since r is isolated) and $r \notin J(h)$ – the latter holds by definition of $\widetilde{S}_t$ if $t \in U$ and by (***) if $t \notin U$. Hence $J(g) \cap J(h) = \emptyset$ and so $[h, g] = 1$ by Claim 10.7(b).

Thus, we proved that each S_{r_i} is a direct factor of H, and since S_{r_i} is an r_i-Sylow subgroup of H, the product $\prod_{i=1}^{\infty} S_{r_i}$ is also a direct factor of H. Hence by Lemma 2.3, $\mathrm{NCC}(H) \geq \prod_{i=1}^{\infty} \mathrm{NCC}(S_{r_i})$. By definition of an isolated prime each S_{r_i} is non-abelian whence $\mathrm{NCC}(S_{r_i}) \geq 2$. This is impossible since $\mathrm{NCC}(H) < \infty$. Thus we proved Claim 10.8. □

We proceed with the proof of Proposition 10.2.

Step 3: We now prove that $\pi(C)$ is finite by contradiction. Suppose that $\pi(C)$ is infinite, and let $Q = \{q_1, q_2, \ldots\}$ and $P = \{p_1, p_2, \ldots\}$ be as in the conclusion of Claim 10.8. Fix $k \in \mathbb{N}$, let $Q_k = \{q_1, \ldots, q_k\}$, $P_k = \{p_1, \ldots, p_k\}$ and consider the group $G_{Q_k, P_k} = A_{Q_k} \rtimes C_{P_k}$. If we view C_{p_i} with $1 \leq i \leq k$ as a subgroup of G_{Q_k, P_k}, then by construction C_{p_i} commutes with A_{q_j} for $i \neq j$. Hence the subgroups $G_{p_i, q_i} = A_{q_i} \rtimes C_{p_i}$, $1 \leq i \leq k$

pairwise commute and G_{Q_k,P_k} decomposes as a direct product $G_{Q_k,P_k} = \prod_{i=1}^{k} G_{p_i,q_i}$. By Lemma 2.1 and Lemma 2.3 we have $\mathrm{NCC}(G) \geq \mathrm{CC}(G_{Q_k,P_k}, G) \geq \prod_{i=1}^{k} \mathrm{CC}(G_{q_i,p_i}, G)$. Since k is arbitrary, to get a contradiction it suffices to show that $\mathrm{CC}(G_{q_i,p_i}, G) \geq 2$ for each i.

Fix i. Recall that $V_{q_i} = A_{q_i}/A_{q_i}^{q_i}$ and $\rho_{q_i}(C_{p_i})$ is the image of C_{p_i} in $\mathrm{Aut}(V_{q_i})$. Suppose that $\rho_{q_i}(C_{p_i})$ has order $p_i^{m_i}$ (we have $m_i > 0$ since C_{p_i} acts non-trivially on V_{q_i}), and let $R = V_{q_i} \rtimes (C_{p_i}/C_{p_i}^{p_i^{m_i}})$. Note that R is a quotient of G_{p_i,q_i}, so it suffices to show that $C(R, G) \geq 2$. We consider 2 cases:

Case 1: $C_{p_i}^{p_i^{m_i-1}}$ fixes a non-trivial element $v \in V_{q_i}$. By definition of m_i some $w \in V_{q_i}$ is not fixed by $C_{p_i}^{p_i^{m_i-1}}$. Hence the cyclic subgroups $\langle v \rangle$ and $\langle w \rangle$ of R lie in different orbits of G, so $\mathrm{CC}(V_{q_i}, G) \geq 2$ and thus $\mathrm{CC}(R, G) \geq 2$ by Lemma 2.1(i).

Case 2: $C_{p_i}^{p_i^{m_i-1}}$ does not fix any non-trivial element of V_{q_i}. Then by Lemma 10.4 R has no element of order $p_i^{m_i} q_i$. Thus, if m is the largest integer such that R has an element of order $p_i^m q_i$ (possibly $m = 0$), then $m < m_i$, so $p_i^m q_i$ and $p_i^{m_i}$ are both maximal element orders of R. Hence $\mathrm{CC}(R, G) \geq 2$ by Lemma 2.8, which finishes the proof. □

11. Profinite groups with (BVC)

11.1. **Variations of finiteness of NCC and connections with topology.** The following terminology was introduced in [vPW2]:

Definition. A discrete or profinite group G has *property (bCyc)* if G has finite NCC.

In this subsection we will introduce two variations of property (bCyc) denoted (bVC) and (BVC) and discuss how they are related to (bCyc) and to each other. We will then explain how properties (bCyc) and (BVC) naturally arise in the study of certain classifying spaces for families of subgroups.

We start with a very general definition.

Definition. Let G be a group and let $\mathcal{F}$ be a class of groups closed under isomorphisms and subgroups. We will say that

(i) G has *property (b$\mathcal{F}$)* if there exist finitely many subgroups of G which lie in $\mathcal{F}$ and whose conjugacy classes cover G.
(ii) G has *property (B$\mathcal{F}$)* if there exist finitely many subgroups $H_1, \ldots, H_k$ of G which lie in $\mathcal{F}$ and such that every subgroup of G lying in $\mathcal{F}$ is conjugate to a subgroup of H_i for some i.

When G is discrete, we will be interested in these properties primarily for the classes Cyc of all cyclic groups and VC of all virtually cyclic groups (so the previously introduced property (bCyc) is precisely (b$\mathcal{F}$) for $\mathcal{F} = Cyc$). Note that properties (bCyc) and (BCyc) are obviously equivalent. The notation (BVC) was introduced in [GW], while properties (bCyc) and (bVC) were formally introduced in [vPW2] (the notation for (bVC) in [vPW1] is (bVCyc)).

We define properties (bCyc)=(BCyc), (BVC) and (bVC) for profinite groups in the obvious way, replacing cyclic (resp. virtually cyclic) groups by procyclic (resp. virtually procyclic) in the above definition.

The following observation is immediate from definitions.

Observation 11.1. *The following hold:*

(a) *If $\mathcal{F}$ contains all cyclic groups, then ($B\mathcal{F}$) implies ($b\mathcal{F}$).*
(b) *If $\mathcal{F}_1 \subseteq \mathcal{F}_2$, then ($b\mathcal{F}_1$) implies ($b\mathcal{F}_2$).*
(c) *If $\mathcal{F}$ is closed under quotients, then any quotient of a group with ($b\mathcal{F}$) has ($b\mathcal{F}$).*

Thus either of the properties (BVC) and (BCyc)=(bCyc) implies (bVC). Somewhat surprisingly, (BVC) is not inherited by quotients, and (bCyc) does not imply (BVC) (see Example 1.12 and Corollary 4.22 in [vPW1]). There are plenty of groups which have (BVC), but not (bCyc), e.g. any virtually cyclic group which is not finite, cyclic or infinite dihedral. However, discrete torsion-free groups with (BVC) have (bCyc) since a torsion-free virtually cyclic group must be cyclic. The latter holds, for instance, since any infinite virtually cyclic group V has a unique maximal finite normal subgroup N such that V/N is infinite cyclic or infinite dihedral [JPL, Proposition 4].[7] Further, residually finite groups with (BVC) are not far from having (bCyc):

Lemma 11.2. *Let G be a discrete residually finite (resp. profinite) group with (BVC). Then some finite index (resp. open) subgroup H of G has (bCyc).*

Proof. Lemma 11.2 in the discrete case has already been established [vP, Lemma 5.0.2], but for completeness we repeat the argument. So let G be a discrete residually finite group which has (BVC) and hence also (bVC). Since virtually cyclic groups have finitely many conjugacy classes of torsion elements (e.g. by [JPL, Proposition 4] stated above), the same is true of G; let us denote such conjugacy classes in G by $K_1, \dots, K_m$. Since G is residually finite, it has a finite index normal subgroup H which intersects each K_i trivially. Then H is a torsion-free group with (bVC), and as we already observed, for discrete torsion-free groups (bVC), (BVC) and (bCyc) are all equivalent.

The argument in the profinite case is even easier. Suppose that G is a profinite group with (BVC) and $V_1, \dots, V_n$ the virtually procyclic subgroups exhibiting (BVC). For each i let C_i be an open procyclic subgroup of V_i. Since the topology on V_i is induced from G, there exist open subgroups H_i of G such that $C_i = G \cap H_i$. The subgroup $\cap H_i$ is open and hence (since G is compact) contains an open normal subgroup H. It is now straightforward to check that H is covered by the conjugacy classes of the procyclic subgroups $(V_i \cap H)^t$ where t ranges over some transversal of H in G, so H has (bCyc). □

In view of Lemma 11.2, Theorem 1.1 yields a complete characterization of discrete residually finite groups with (BVC) – these are precisely virtually cyclic groups. Likewise Theorem 1.5 implies that any profinite group with (BVC) has an open pronilpotent subgroup with (bCyc) (recall that such groups are completely classified by Theorem 1.3 and Corollary 1.4). We will prove that the latter property actually characterizes profinite groups with (BVC):

Theorem 11.3. *A profinite group has (BVC) if and only if it has an open pronilpotent subgroup with (bCyc).*

In view of Theorem 1.5, this implies that (bCyc) implies (BVC) for profinite groups. Theorem 11.3 will be proved in the next subsection.

[7] More generally, Stallings proved that virtually free torsion-free discrete groups must be free.

Connection with topology. Property (B$\mathcal{F}$) naturally arises in the study of the classifying space $\mathcal{E}_{\mathcal{F}}(G)$ defined as follows:

Definition. Let G be a discrete group and let $\mathcal{F}$ be as above. A classifying space $\mathcal{E}_{\mathcal{F}}(G)$ is a G-CW complex (that is, a CW complex with a cellular action of G) such that for every subgroup H of G, the H-fixed point space $\mathcal{E}_{\mathcal{F}}(G)^H$ is empty if $H \notin \mathcal{F}$ and contractible (in particular, non-empty) if $H \in \mathcal{F}$.

It is known that $\mathcal{E}_{\mathcal{F}}(G)$ is unique up to G-homotopy.

A G-CW complex is said to be *finite type* if it has finitely many G-orbits of cells in each dimension and *finite* if it is of finite type and finite-dimensional. Juan-Pineda and Leary [JPL, Conjecture 1] conjectured that a classifying space $\mathcal{E}_{VC}(G)$ cannot be finite unless G is virtually cyclic. A similar question of Lück, Reich, Rognes and Varisco [LRRV, Question 4.9] asks whether $\mathcal{E}_{Cyc}(G)$ cannot be of finite type unless G is finite, cyclic or dihedral.

The following result establishes the basic relation between property (B$\mathcal{F}$) for G and the classifying space $\mathcal{E}_{\mathcal{F}}(G)$:

Claim 11.4. *G admits $\mathcal{E}_{\mathcal{F}}(G)$ with finitely many 0-cells if and only if G has (B$\mathcal{F}$).*

Claim 11.4 in the case $\mathcal{F} = VC$ is Lemma 1.3 in [vPW1]. The proof in the general case is identical.

Corollary 11.5. *Let G be a residually finite group. Then*

(a) [JPL, Conjecture 1] *holds for G and*
(b) [LRRV, Question 4.9] *has positive answer for G.*

Proof. Suppose that $\mathcal{E}_{Cyc}(G)$ has finite type. Then by Claim 11.4 G has (BCyc)=(bCyc), so (b) follows directly from Theorem 1.1. To prove (a) we use the same argument in conjunction with Lemma 11.2. □

11.2. **Proof of Theorem 11.3.** The forward direction in Theorem 11.3 is a direct consequence of Theorem 1.5 and Lemma 11.2 (recall that by definition a group G has (bCyc) if and only if $\mathrm{NCC}(G) < \infty$). To establish the backwards direction we need several auxiliary results.

Lemma 11.6. *Let D be a quaternion division algebra over $F = \mathbb{Q}_p$ and G an open subgroup of $\mathrm{PGL}_1(D)$. Then G has (BVC).*

Proof. Since (BVC) is inherited by open subgroups, it suffices to prove the result for $G = \mathrm{PGL}_1(D)$.

(i) Since G is a compact p-adic analytic group, it has finitely many conjugacy classes of finite subgroups [DDMS, Theorem 4.23].

Thus, in the proof of (BVC) we only need to consider infinite virtually procyclic subgroups. We claim that

(ii) If K is any maximal subfield of D, then $Stab_G(K)$ (the stabilizer of K under the natural conjugation action of G on D) is virtually procyclic. (Note that since $\deg(D) = 2$, any subfield of D properly containing $F = \mathbb{Q}_p$ is maximal.)
(iii) Any infinite virtually procyclic subgroup of G is contained in $Stab_G(K)$ for some maximal subfield K.

As we already observed in § 7, the action of G on the set $\mathcal{MF}(D)$ of maximal subfields of D has finitely many orbits, so there are finitely many conjugacy classes of subgroups of the form $Stab_G(K)$, with K a maximal subfield. Therefore, (i), (ii) and (iii) would imply that G has (BVC).

Let K be a maximal subfield. In the proof of Theorem 7.15(2), we already showed that $Stab_G(K)$ contains $K^\times/F^\times$ as a subgroup of index 2. Since $K^\times/F^\times$ is virtually procyclic by Corollary 7.13, it follows that $Stab_G(K)$ is also virtually procyclic. Thus we proved (ii).

We turn to the proof of (iii). Let H be an infinite virtually procyclic subgroup of G, and let C be a non-trivial normal procyclic subgroup of H (which is also infinite and in particular non-trivial). Let $\widetilde{H}$ and $\widetilde{C}$ be the preimages of H and C in $\mathrm{GL}_1(D)$, respectively. Since C is non-trivial procyclic and the kernel of the map $\widetilde{C} \to C$ is central, $\widetilde{C}$ is a commutative subset of D not contained in F and hence generates some maximal subfield K. Since $\widetilde{H}$ normalizes $\widetilde{C}$, it must be contained in $Stab_{\widetilde{G}}(K)$, and hence $H \subseteq Stab_G(K)$, as desired. □

Definition. We will say that profinite groups A and B have *virtually coprime orders* if they have open subgroups C and D, respectively, whose orders are coprime.

Lemma 11.7. *Let $G_1, \dots, G_k$ be profinite groups whose orders are pairwise virtually coprime, and suppose that each G_i has (BVC). Then $G = G_1 \times \cdots \times G_k$ also has (BVC).*

Proof. For each $1 \le i \le k$ let $\{H_{i,j}\}_{j=1}^{n_i}$ be a finite collection of virtually procyclic subgroups of G_i which exhibits (BVC).

Let V be any virtually procyclic subgroup of G, and let V_i be the projection of V onto G_i. Then each V_i is procyclic and thus must be contained in $H_{i,j_i}^{g_i}$ for some $1 \le j_i \le n_i$ and $g_i \in G_i$. Then V is contained in $V' = V_1 \times \cdots \times V_k$, while V' is contained in $H^{(g_1,\dots,g_k)}$ where $H = H_{1,j_1} \times \cdots \times H_{k,i_k}$. Since each H_{i,j_i} is virtually procyclic and $G_1, \dots, G_k$ have pairwise coprime orders, H is also virtually procyclic. Since there are only finitely many possiblities for H, we proved that G has (BVC). □

Lemma 11.8. *Let G be a profinite group and N a closed normal subgroup of G. Suppose that G/N has (BVC), the orders of N and G/N are virtually coprime, and there exists an open subgroup H of G such that $N \cap H$ is procyclic and central in H. Then G has (BVC).*

Proof. Let $Q_1, \dots, Q_m$ be a finite collection of virtually procyclic subgroups of G/N which exhibits (BVC), and let $\pi : G \to G/N$ be the natural projection.

Now let V be any virtually procyclic subgroup of G. Then $\pi(V)$ is a virtually procyclic subgroup of G/N. By assumption $\pi(V)$ is conjugate to a subgroup of Q_i for some i, whence $V \subseteq \pi^{-1}(\pi(V))$ is conjugate to a subgroup of $G_i = \pi^{-1}(Q_i)$. To finish the proof we just need to explain why each G_i is virtually procyclic.

Since N and G_i/N have virtually coprime orders and $G_i/N \cong Q_i$ is virtually procyclic, after making the subgroup H in the statement of Lemma 11.8 smaller if needed, we can assume that for each i the groups $N \cap H$ and $(G_i \cap H)/(N \cap H)$ have coprime orders and $(G_i \cap H)/(N \cap H)$ is procyclic. Since by assumption, $N \cap H$ is procyclic and central in H, it follows that $G_i \cap H$ is procyclic, whence G_i is virtually procyclic, as desired. □

We are now ready to prove the backwards direction of Theorem 11.3:

Proof. Let G be a profinite group which has an open pronilpotent subgroup H with (bCyc). By Corollary 1.4, $H = C \times \prod_{i=1}^{k} H_i$ where C is a procyclic group and there exist distinct primes $p_1, \ldots, p_k$ not dividing $|C|$ such that each H_i is a non-procyclic pro-p_i group with (bCyc). By Theorem 1.3 each H_i is

(i) finite,
(ii) infinite prodihedral (if $p_i = 2$) or
(iii) isomorphic to an open subgroup of $\mathrm{PGL}_1(D_i)$ where D_i is the quaternion division algebra over $\mathbb{Q}_{p_i}$.

Making H smaller if needed, we can assume that case (iii) occurs for all i (if an infinite prodihedral subgroup, say H_i, is present, we can first replace it by $H_i' \cong (\mathbb{Z}_2, +)$ and then replace C by $C \times H_i'$ which will still be procyclic).

Now let $U = H_1 \times \cdots \times H_k$, so that $H = C \times U$. It is straightforward to check that U is characteristic in H, so the conjugation action of G on itself induces a map $\iota : G \to Comm(U)$ (where as before $Comm(U)$ is the commensurator of U).

It is routine to check that $Comm(U) = Comm(H_1) \times \cdots \times Comm(H_k)$. As shown in the proof of Proposition 9.1, $Comm(H_i) \cong \mathrm{PGL}(D_i)$ for each i. Thus, $Comm(H_i)$ has (BVC) by Lemma 11.6. Moreover, the isomorphisms $Comm(H_i) \cong \mathrm{PGL}(D_i)$ imply that

(a) the groups $\{Comm(H_i)\}$ have pairwise virtually coprime orders, whence $Comm(U)$ has (BVC) by Lemma 11.7 and
(b) $\iota(G)$ is open in $Comm(U)$, whence by (a) $\iota(G)$ also has (BVC).

Finally, it is clear that $\operatorname{Ker}\iota \cap H = C$, so $\operatorname{Ker}\iota \cap H$ is procyclic and central in H and the orders of $\operatorname{Ker}\iota$ and $\iota(G)$ are virtually coprime. Hence G has (BVC) by Lemma 11.8. □

References

[AS] Cristina Acciarri and Pavel Shumyatsky, *Commutators and commutator subgroups in profinite groups.* J. Algebra 473 (2017), 166–182.

[BEW] Yiftach Barnea, Mikhail Ershov and Thomas Weigel, *Abstract commensurators of profinite groups.* Trans. Amer. Math. Soc. 363 (2011), no. 10, 5381–5417.

[Be] Janez Bernik, *On groups and semigroups of matrices in spectra in a finitely generated field.* Linear Multilinear Algebra 53 (2005), no. 4, 259–267.

[BJL] Sigrid Böge, Sigrid, Moshe Jarden and Alexander Lubotzky, *Sliceable groups and towers of fields.* J. Group Theory 19 (2016), no. 3, 365–390.

[BG] Emmanuel Breuillard and Tsachik Gelander, *A topological Tits alternative.* Ann. of Math. (2) 166 (2007), no. 2, 427–474.

[BPS] Daniela Bubboloni, Cheryl E. Praeger and Pablo Spiga, *Linear bounds for the normal covering number of the symmetric and alternating groups.* Monatsh. Math. 191 (2020), no. 2, 229–247.

[BSW] Daniela Bubboloni, Pablo Spiga and Thomas Weigel, *Normal 2-converings of the finite simple groups and their generalization.* preprint (2022), `https://arxiv.org/abs/2208.08756`.

[Bu] William Burnside, *The theory of groups of finite order.* Cambridge University Press (1897).

[CRRZ] Pietro Corvaja, Andrei Rapinchuk, Jinbo Ren and Umberto Zannier, *Non-virtually abelian anisotropic linear groups are not boundedly generated.* Invent. Math. 227 (2022), 1–26.

[DDMS] John Dixon, Marcus du Sautoy, Avinoam Mann and Daniel Segal, *Analytic pro-p groups.* Second edition. Cambridge Studies in Advanced Mathematics, 61. Cambridge University Press, Cambridge, 1999.

[Er] Mikhail Ershov, *On the second cohomology of the norm one group of a p-adic division algebra,* with an appendix by Mikhail Ershov and Thomas Weigel, Mich. Math. J. 72 (2022), 261–330.

[Go] Fernando Q. Gouvea, *p-adic numbers. An introduction.* Third edition. Universitext, Springer, 2020, vi+373 pp.

[GW] J. R. J. Groves and John S. Wilson, *Soluble groups with a finiteness condition arising from Bredon cohomology.* Bull. London Math. Soc. 45 (2013) 89–92.

[HNN] Graham Higman, Bernhard Neumann and Hanna Neumann, *Embedding theorems for groups.* J. London Math. Soc. 24 (1949), 247–254.

[Ja] Andrei Jaikin-Zapirain, *On the number of conjugacy classes in finite p-groups.* J. London Math. Soc. (2) 68 (2003), no. 3, 699–711.

[JN] Andrei Jaikin-Zapirain and Nikolay Nikolov, *An infinite compact Hausdorff group has uncountably many conjugacy classes.* Proc. Amer. Math. Soc. 147 (2019), no. 9, 4083–4089.

[JT] Andrei Jaikin-Zapirain and Joan Tent, *Finite 2-groups with odd number of conjugacy classes.* Trans. Amer. Math. Soc. 370 (2018), no. 5, 3663–3688.

[Jo] Camille Jordan, *Recherches sur les substitutions.* J. Math. Pures Appl. (2) 17 (1872), 351–367.

[JPL] Daniel Juan-Pineda and Ian Leary, *On classifying spaces for the family of virtually cyclic subgroups.* Recent developments in algebraic topology, 135–145, Contemp. Math., 407, Amer. Math. Soc., Providence, RI, 2006.

[LRRV] Wolfgang Lück, Holger Reich, John Rognes, and Marco Varisco, *Assembly maps for topological cyclic homology of group algebras.* J. Reine Angew. Math. 755 (2019), 247–277.

[Lang] Serge Lang, *Algebraic number theory.* Second Edition. Graduate Texts in Mathematics, 110. Springer-Verlag, New York, 1994. xiv+357 pp.

[LG] Charles R. Leedham-Green, *The structure of finite p-groups.* J. London Math. Soc. (2) 50 (1994), no. 1, 49–67.

[Min] Ashot Minasyan, *Some examples of invariably generated groups.* Isr. J. Math. 245 (2021), no. 1, pp. 231–257.

[Mil] J. S. Milne, *Class field theory,* available at `https://www.jmilne.org/math/CourseNotes/CFT.pdf`

[Ol] Alexander Ol'shanskii, *Geometry of defining relations in groups.* Moscow, Nauka, 1989 (in Russian); English translation in Mathematics and its Applications (Soviet Series), 70. Kluwer Academic Publishers Group, Dordrecht, 1991.

[Os] Denis Osin, *Small cancellations over relatively hyperbolic groups and embedding theorems.* Ann. of Math. (2) 172 (2010), no. 1, 1–39.

[PR] Gopal Prasad and Andrei Rapinchuk, *Existence of irreducible $\mathbb{R}$-regular elements in Zariski-dense subgroups.* Math. Res. Lett. 10 (2003), 21–32.

[vP] Timm von Puttkamer, *On the Finiteness of the classifying space for virtually cyclic subgroups.* Ph.D. Thesis (2018), available at `https://bonndoc.ulb.uni-bonn.de/xmlui/bitstream/handle/20.500.11811/7608/5151.pdf?sequence=1&isAllowed=y`

[vPW1] Timm von Puttkamer and Xiaolei Wu, *On the finiteness of the classifying space for virtually cyclic subgroups.* Groups Geom. Dyn. 13 (2019), 707–729.

[vPW2] Timm von Puttkamer and Xiaolei Wu, *Linear groups, conjugacy growth, and classifying spaces for families of subgroups.* Int. Math. Res. Not. IMRN 2019, no. 10, 3130–3168.

[Ri] Carl Riehm, *The norm 1 group of* $\mathfrak{p}$*-adic division algebra.* Amer. J. of Math. 92 (1970), no. 2, 499–523.

[Ro] Derek J. S. Robinson, *A course in the theory of groups.* Second edition. Graduate Texts in Mathematics, 80. Springer-Verlag, New York, 1996. xviii+499 pp.

[Sea] Suzanne M. Seager, *A bound on the rank of primitive solvable permutation groups.* J. Algebra 116 (1988), no. 2, 342–352.

[Ser] Jean-Pierre Serre, *Sur la dimension cohomologique des groupes profinis.* Topology 3 (1965), 413–420.

[Wes] Phillip Wesolek, *Conjugacy class conditions in locally compact second countable groups.* Proc. Amer. Math. Soc. 144 (2016), no. 1, 399–409.

[Wil1] John S. Wilson, *Profinite groups with few conjugacy classes of p-elements.* Proc. Amer. Math. Soc. 150 (2022), no. 8, 3297–3305.

[Wil2] John S. Wilson, *Profinite groups with few conjugacy classes of elements of infinite order.* preprint (2022), `https://arxiv.org/abs/2209.14753`

[Ze] Efim I. Zelmanov, *On periodic compact groups.* Israel J. Math. 77 (1992), no. 1-2, 83–95.

Yiftach Barnea, Department of Mathematics, Royal Holloway, University of London, Egham, Surrey TW20 0EX, UK
Email address: y.barnea@rhul.ac.uk

Rachel Camina, Fitzwilliam College, Cambridge, CB3 0DG, UK
Email address: rdc26@cam.ac.uk

Mikhail Ershov, Department of Mathematics, University of Virginia, 141 Cabell Drive, Charlottesville, VA 22903, USA
Email address: ershov@virginia.edu

Mark L. Lewis, Department of Mathematical Sciences, Kent State University, Kent, OH 44242 USA
Email address: lewis@math.kent.edu