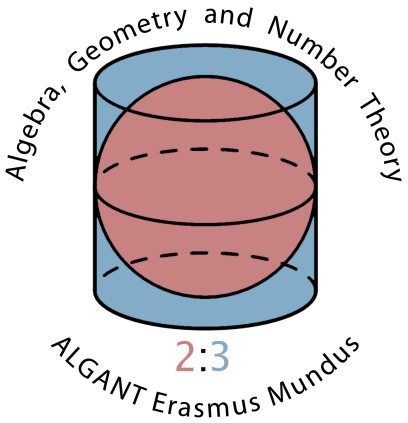


Università degli Studi di Padova
Dipartimento di Matematica "Tullio Levi-Civita"
Corso di Laurea Magistrale in Matematica

Cardinality and Words in Profinite Groups

Thesis advisors: Eloisa Michela Detomi,
Gustavo Adolfo Fernández Alcober

Mikel Eguzki Garciarena Perez

Student number: 2004305

21 luglio 2021

Università degli Studi di Padova

Universiteit Leiden

Academic year 2020-2021

Acknowledgements

First of all, I would like to thank the consistorium of the ALGANT master's program for making it possible for me to live this experience. These two years have been amazing and have helped me to develop as a person and as a mathematician.

I would also like to thank Gustavo Fernández Alcober, who mentioned ALGANT to me, in the first place, and that later has become one of my master thesis advisors. Together with Gustavo, I would also like to thank all the teachers from the University of the Basque Country for showing me the beauty of mathematics and algebra. In particular to Domingo Ramirez Alzola (Txomin), Jon González Sánchez, Marta Macho Stadler, and Javier Duoandikoetxea.

I would like to thank all the teachers from Leiden University who helped me during my first year of ALGANT. Also, I would like to thank all the friends that I made in Leiden, in particular, Kirsten Wilk, Stevell Muller, and Arshay Sheth that made me feel as if I was at home in times of coronavirus.

I would like to thank the University of Padova teachers and all the friends that I made in Padova. In particular, Charlotte Sophie Schell, Lara Galindo, Sergio Navarro, and Ania Rodríguez for making my experience in Italy one of the best of my life.

I would like to thank my mum and dad for always believing in me and supporting me wherever I go. And all my friends from the Basque Country in particular Idoia Orbegozo and Maialen Aginagalde for their support during these two years.

Finally, I would like to thank Gustavo Fernández Alcober and Eloisa Detomi which, in times of coronavirus, have devoted all the time and effort to the best success of this work.

Contents

0 Introduction

In this thesis, we study cardinalities and words in profinite groups. Let $w = w(x_1, \dots, x_r)$ be a word, that is, an element of the free group on $x_1, \dots, x_r$. We are interested in the set of all the w-values in a group G, that is $G_w = \{w(g_1, \dots, g_r) : g_1, \dots, g_r \in G\}$, and the verbal subgroup $w(G)$ generated by it. In particular we are interested in the sizes of these sets when w is a multilinear commutator word and G is a profinite group. A multilinear commutator word is a word obtained by nesting commutators and using each variable only once. For example the simple commutator $[x, y]$ and more generally the higher commutators are multilinear commutator words. The goal of this thesis is to show that for a profinite group G and a multilinear commutator word w, if the cardinality of G_w is infinite then $|G_w| = |w(G)| = 2^{\mathfrak{a}}$ for some cardinal number $\mathfrak{a}$.

The thesis is divided into three chapters. In the first one we will briefly introduce ordinal and cardinal numbers. In the second chapter we will show that the cardinal number of an infinite profinite group is $2^{\mathfrak{a}}$ for some cardinal number $\mathfrak{a}$. In addition, we will prove that if a continuous map from a profinite group to a Hausdorff space has a "small image", then it is constant on a coset of a "big" closed subgroup. Finally in the third chapter we will collect some known results on multilinear commutator groups and we will prove our main results.

1 Ordinal and cardinal numbers

In this chapter we will define cardinal and ordinal numbers and prove some basic properties about them. This will be of great interest later when comparing the sizes of different sets. First we will focus on ordinal numbers, which, as we will see, is a class of sets that can be ordered. Later we will introduce the concept of cardinality, which is an equivalence relation in the class of sets based on the number of elements in the set. Cardinality is essential when working with sets with an infinite number of elements. Finally, we will combine both concepts and introduce alephs which are a sequence of numbers used to represent the size of infinite sets. In this chapter we will be using results from [6, chapters 2 and 3].

1.1 Ordinals

The set of finite sets can be ordered since it is in bijection with an ordered set, namely, the positive integers $\mathbb{Z}_{\geq 0}$:

$$\begin{aligned} \{S : S \text{ is a finite set}\} &\longleftrightarrow \mathbb{Z}_{\geq 0} \\ S &\longmapsto |S|. \end{aligned} \tag{1}$$

Here $|S|$ is the number of elements in S.

In this section we will introduce the ordinal numbers, a subclass of the class of sets that can be ordered similarly to how positive integers are sorted. This is used to order infinite sets as positive integers are used to sort finite sets.

Before formally defining ordinal numbers we need some preliminary definitions.

Definition 1.1. A set T is *transitive* if for every set $X \in T$, then $X \subseteq T$ or equivalently, if $x \in y$ and $y \in T$, then $x \in T$.

Remark 1.2. In set theory, an object that can be an element of a set but is not a set is called urelement. But in modern set theory, it has been show that urelements are not needed because they can easily be modeled in a set theory without urelements. So we will assume that there are not urelements, and thus the previous definition can be rewritten as follows: A set T is transitive if every element in T is also a subset of T.

Below we can see some examples of transitive and not-transitive sets.

Example 1.3. 1. $\emptyset = \{\}$ is trivially a transitive set.

2. The set $\{\ \{\},\ \{\{\}\},\ \{\{\{\}\}\}\ \}$ is also a transitive set.

3. The set $\{a, b\}$ is not transitive because $a \in \{a, b\}$, but $\{a\} \notin \{a, b\}$.

Definition 1.4. We say that a set X is *totally ordered* by the binary relation $\leq$ if the following properties hold for all $a, b, c \in X$:

1. If $a \leq b$ and $b \leq a$, then $a = b$.

2. If $a \leq b$ and $b \leq c$, then $a \leq c$.

3. $a \leq b$ or $b \leq a$.

We will write $a < b$ when $a \leq b$, but $a \neq b$.

Definition 1.5. A set X is *well-ordered* by the binary relation $\leq$ if X is totally ordered and every subset of X has a least element with respect to $\leq$.

From now on, we will assume the Axiom of Choice (see Axiom 4.9), this way we have that all sets can be well-ordered and unless mentioned otherwise, every time we write "set" we will mean "well-ordered set". We are now ready to present the definition of ordinal numbers.

Definition 1.6. A set is an *ordinal number* if it is transitive and well-ordered by $\in$. We will denote ordinal numbers, or just ordinals, by lowercase Greek letters $\alpha, \beta, \gamma, ...$ and the class of all ordinals by *Ord*. We say that

$$\alpha < \beta \quad \text{if and only if} \quad \alpha \in \beta.$$

The following lemma and the consequences are independent from the Axiom of Choice and are essential when working with ordinal numbers.

Lemma 1.7. (i) We set $0 = \emptyset$, then 0 is an ordinal.

(ii) If β is an ordinal and $\alpha \in \beta$, then α is an ordinal.

(iii) If $\alpha \neq \beta$ are ordinals and $\alpha \subset \beta$, then $\alpha \in \beta$.

(iv) If α, β are ordinals, then either $\alpha \subset \beta$ or $\beta \subset \alpha$.

Proof. (i) follows from the definition of ordinal number.

For (ii), note that β is transitive so $\alpha \subset \beta$, and since β is well-ordered, we have that α is a well-ordered set as well. Moreover, $\in$ defines a total

order in β, so, in particular, if $x \in y \in \alpha$, then $x \in \alpha$, which implies that α is also transitive.

For (iii), let γ be the least element in $\beta - \alpha$. Since α is an ordinal number, it follows that $\alpha = \{x \in \beta : x < \gamma\}$. Indeed, if $x \in \{x \in \beta : x < \gamma\}$, then $x \in \alpha$. Otherwise, $x \in \beta - \alpha$ and $x < \gamma$ which is a contradiction. Conversely, if $x \in \alpha$, then $x \in \beta$, moreover, $x < \gamma$. Certainly, suppose $x = \gamma$ or $x > \gamma$. In any case, since α is transitive, $\gamma \in \alpha$ which is a contradiction.
Now, it is enough to prove that $\gamma = \{x \in \beta : x < \gamma\}$, because $\gamma \in \beta$. We claim that if $\gamma \in \beta$, then $\gamma = \{x \in \beta : x < \gamma\}$. On the one hand it is clear that $\{x \in \beta : x < \gamma\} \subseteq \gamma$. On the other hand, by the transitivity of β, if $y \in \gamma$, then $y \in \beta$. So $y \in \{x \in \beta : x < \gamma\}$.

To prove (iv), we claim that if α and β are ordinal numbers, then $\alpha \cap \beta$ is again an ordinal number. It follows from this claim that either $\alpha = \alpha \cap \beta$ or $\beta = \alpha \cap \beta$. Otherwise, using (iii), we deduce that $\gamma \in \alpha$ and $\gamma \in \beta$ which then implies that $\gamma \in \gamma$ which is a contradiction since $\in$ is a strict ordering. It remains to prove the claim. First, we have that $\alpha \cap \beta$ is well-ordered because all subsets of a well-ordered set are well-ordered. Moreover, if $x \in y \in \alpha \cap \beta$, then $x \in y \in \alpha$. Since α is transitive, we observe that $x \in \alpha$. We deduce in a similar way that $x \in \beta$, and so $x \in \alpha \cap \beta$. This shows the transitivity of $\alpha \cap \beta$ and proves the claim. □

A few important consequences arise from this lemma:

- $<$ is a total ordering for the class *Ord*.
- For each ordinal α, we have that $\alpha = \{\beta \in \mathit{Ord} : \beta < \alpha\}$. Indeed, if $x \in \{\beta \in \mathit{Ord} : \beta < \alpha\}$, then $x < \alpha$, which by definition implies $x \in \alpha$. On the other hand, if $x \in \alpha$, then by (ii), it follows that x is an ordinal and so $x < \alpha$.
- For every ordinal α, we have that $\alpha \cup \{\alpha\}$ is an ordinal. Obviously, $\alpha \cup \{\alpha\}$ is well-ordered; and to show that $\alpha \cup \{\alpha\}$ is transitive note that if x belongs to $\alpha \cup \{\alpha\}$ then either $x \in \alpha$, and so $x \subset \alpha$, or $x = \alpha$ in any case $x \subset \alpha \cup \{\alpha\}$.
  Moreover, $\alpha \cup \{\alpha\} = \inf\{\beta \in \mathit{Ord} : \beta > \alpha\}$. This is clear because, $\alpha \cup \{\alpha\}$ is an ordinal and contains α, so $\alpha \cup \{\alpha\} > \alpha$; and if there exists some ordinal number β such that $\alpha < \beta < \alpha \cup \{\alpha\}$, then $\beta \in \alpha$ or $\beta \in \{\alpha\}$ which in any case is a contradiction.

Using the last point we define $\alpha + 1 = \alpha \cup \{\alpha\}$ to be the *successor* of α.

Now that we have defined ordinal numbers and proven some important properties that they possess we want to prove that every set is isomorphic to a unique ordinal number. Informally, we want to generalize the function (1) to all sets. That is,

$$\{S : S \text{ is a set}\} \longrightarrow \{\alpha : \alpha \text{ is an ordinal number}\}. \tag{2}$$

This will enable us to order the class of sets in the same way as the set of finite sets is ordered. To prove this claim we first need to show some lemmas and definitions.
Let P and Q be two sets and suppose that they are well-ordered by $<_P$ and $<_Q$ respectively. We say that a function $f : P \to Q$ is *increasing* if $x <_P y$ implies that $f(x) <_Q f(y)$. Moreover, we say that a bijective function between P and Q is an isomorphism if f and f^{-1} are increasing. In that case we say that P with the binary relation $<_P$ and Q with the binary relation $<_Q$ are isomorphic.
From now on we refer to the set W and and the binary relation $<$, for which W is well-ordered as the set $(W, <)$.

Lemma 1.8. Let $(W, <)$ be a set. If $f : W \to W$ is an increasing function, then $f(x) \geq x$ for each $x \in W$.

Proof. Suppose, for the sake of contradiction, that the set $X = \{x \in W : f(x) < x\}$ is non-empty. Let z be the least element in this set, in particular $f(z) < z$. Since f is an increasing function, we know that $f(f(z)) < f(z)$, which is a contradiction because z is the least element in the set X. □

Let W be a set and assume that u belongs to W. Then we say that $\{x \in W : x < u\}$ is an *initial segment* of W, given by u.

Lemma 1.9. No set is isomorphic to an initial segment of itself.

Proof. By way of contradiction, suppose there exists an isomorphism

$$f : W \longrightarrow \{x \in W : x < u\}$$

for some $u \in W$. Then we have that $f(u) < u$ which contradicts Lemma 1.8. □

We are now ready to prove the result mentioned above.

Theorem 1.10. Every set is isomorphic to a unique ordinal number.

Proof. Let W be a set. We will start by proving that if W is isomorphic to an ordinal number, then this ordinal number is unique. Suppose, for the sake of contradiction, that W is isomorphic to α and β. Without loss of generality, we can assume that $\beta < \alpha$. Then β is the initial segment of α given by the least element in $\alpha - \beta$. By Lemma 1.9, we know that this is a contradiction, since α is not isomorphic to an initial segment of itself.

It remains to show that W is isomorphic to an ordinal number. We construct such an isomorphism as follows. For $x \in W$ we define

$$F(x) = \alpha, \quad \text{where } \alpha \text{ is isomorphic to the initial segment of } W \text{ given by } x.$$

We claim that this function is well defined, in other words, for each $x \in W$ there exists a unique ordinal number α that is isomorphic to the initial segment of W given by x. By the Replacement Axioms, $F(W)$ is a set. Let γ be the least ordinal not in $F(W)$, then $F(W) = \gamma$ and this way we have an isomorphism between W and γ. It remains to prove the claim. Suppose that for each $x \in W$ there exists an ordinal number α that is isomorphic to the initial segment of W given by x. Then we can prove that it is unique in the same way that we have proven that if W is isomorphic to an ordinal number, then this ordinal number is unique. On the other hand, to show that such an α exists, by way of contradiction, suppose that z is the least element for which such an α does not exist. Then the set

$$\{w \in W : \exists \alpha \text{ such that } F(w) = \alpha\}$$

is exactly an initial segment given by z, which is a contradiction. □

We conclude the section about ordinal numbers by presenting some final definitions and a very important theorem that, informally, extends the mathematical induction to sets.

Definition 1.11. Let α be an ordinal. If $\alpha = \beta + 1$ for some ordinal β, then α is a *successor ordinal*. Otherwise, we have that

$$\alpha = \sup\{\beta : \beta < \alpha\} = \bigcup_{\beta<\alpha} \beta,$$

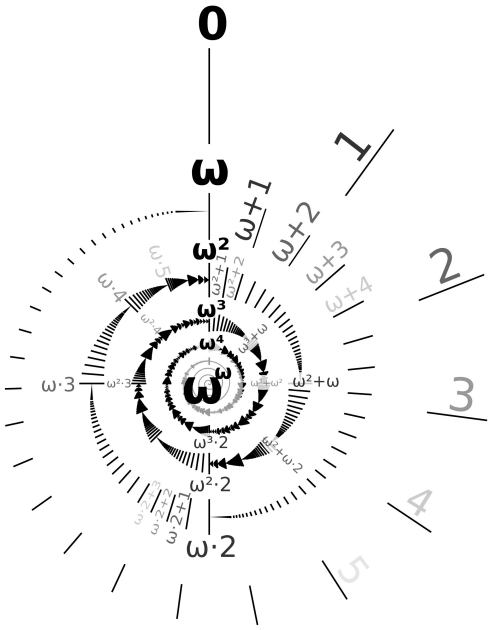
and we call α a *limit ordinal*. We will consider 0 a limit ordinal and we will define $\sup \emptyset = 0$.

Note that the existence of limit ordinals other than 0 follows from the Axiom of Infinity.

Definition 1.12. Let ω be the least nonzero limit ordinal. Then the elements less than ω are called *finite ordinals*, or *natural numbers*. For example

$$0 = \emptyset, \qquad 1 = 0 + 1, \qquad 2 = 1 + 1, \qquad 3 = 2 + 1, ...$$

We say that a set X is finite if there is a bijective map from X to some ordinal less than ω. And we say that X is *infinite* otherwise.



This image is a representation of the first ordinal numbers.

Theorem 1.13 (Transfinite Induction)**.** Let C be a class of ordinals. Assume that

(i) $0 \in C$,

(ii) if $\alpha \in C$, then $\alpha + 1 \in C$,

(iii) if α is a nonzero limit ordinal and for all $\beta < \alpha$ we have $\beta \in C$, then $\alpha \in C$.

Then C is the class of all ordinals.

Proof. Let γ be the least ordinal number not in C, then clearly $\gamma \neq 0$. If γ is a successor ordinal, then there exists an ordinal α such that $\alpha + 1 = \gamma$. Then α has to be in C, and by (ii) γ is also in C. Similarly, if γ is a limit ordinal, then for all $\beta < \gamma$ we have that $\beta \in C$, and by (iii) γ is in C. □

1.2 Cardinals

In this section we want to find an equivalence relation in the class of sets based on the number of elements in the sets. Such an equivalence relation is defined as follows. Let X and Y be two sets. If there exists a bijective map from X to Y, we say that these two sets have the same *cardinal number* or *cardinality*. To symbolize this we write

$$|X| = |Y|. \tag{3}$$

If we assume that for each set X we can assign a cardinal number $|X|$ and that two sets have the same cardinality if there exists a bijective function between them, then we have that (3) is an equivalence relation in the class of *Sets*.

In the category of finite sets *FinSets*, it is clear that we can assign to each $X \in Obj(FinSets)$ a cardinal number $|X|$ by writing $|X|$ equal to the number of elements in X. Moreover, if two finite sets X and Y have the same cardinal number, in other words, the same number of elements, then there exists a bijective function between them. In the case of infinite sets, for the moment, we will assume that we can assign a cardinal number to each of them and that two sets have the same cardinal number if there exists a bijective function between them.

Let X and Y be two sets. If there exists an injective map from X to Y, we say that the cardinal number of X is smaller than or equal to the cardinal number of Y, and we write $|X| \leq |Y|$. Moreover, if there does not exist a bijective function between X and Y, we say that that the cardinal number of X is strictly smaller than the cardinal number of Y, and we write $|X| < |Y|$. This shows that sets can be sorted based on their cardinal numbers. Furthermore, we will later prove in Theorem 1.14 and Theorem 1.17 that cardinal numbers are, in fact, totally ordered.

From now on we will refer to cardinal numbers by gothic letters $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \ldots$. The next step is to define an arithmetic over the cardinals. We do this as follows.

$$\begin{aligned}
\mathfrak{a} + \mathfrak{b} &= |A \cup B| && \text{where } |A| = \mathfrak{a},\ |B| = \mathfrak{b} \text{ and } A, B \text{ are disjoint,} \\
\mathfrak{a} \cdot \mathfrak{b} &= |A \times B| && \text{where } |A| = \mathfrak{a},\ |B| = \mathfrak{b}, \\
\mathfrak{a}^{\mathfrak{b}} &= |A^B| && \text{where } |A| = \mathfrak{a},\ |B| = \mathfrak{b}.
\end{aligned}$$

In set theory, A^B is defined as the set of functions from B to A, this is

$$A^B = \{f : B \longrightarrow A\}.$$

By the definitions given above we observe that the properties below hold in the arithmetic of cardinal numbers:

1. $+$ and $\cdot$ are associative, commutative and distributive.
2. If $\mathfrak{a} \leq \mathfrak{b}$, then $\mathfrak{a} + \mathfrak{c} \leq \mathfrak{b} + \mathfrak{c}$.
3. If $\mathfrak{a} \leq \mathfrak{b}$, then $\mathfrak{a} \cdot \mathfrak{c} \leq \mathfrak{b} \cdot \mathfrak{c}$.
4. $(\mathfrak{a} \cdot \mathfrak{b})^{\mathfrak{c}} = \mathfrak{a}^{\mathfrak{c}} \cdot \mathfrak{b}^{\mathfrak{c}}$.
5. $\mathfrak{a}^{\mathfrak{b}+\mathfrak{c}} = \mathfrak{a}^{\mathfrak{b}} \cdot \mathfrak{a}^{\mathfrak{c}}$
6. $(\mathfrak{a}^{\mathfrak{b}})^{\mathfrak{c}} = \mathfrak{a}^{\mathfrak{b}\cdot\mathfrak{c}}$.
7. If $\mathfrak{a} \leq \mathfrak{b}$, then $\mathfrak{a}^{\mathfrak{c}} \leq \mathfrak{b}^{\mathfrak{c}}$.
8. If $0 < \mathfrak{a} \leq \mathfrak{b}$, then $\mathfrak{c}^{\mathfrak{a}} \leq \mathfrak{c}^{\mathfrak{b}}$. This clearly implies that if $\mathfrak{a} \leq \mathfrak{b}$, then $2^{\mathfrak{a}} \leq 2^{\mathfrak{b}}$, but it is not true in general that if $\mathfrak{a} < \mathfrak{b}$, then $2^{\mathfrak{a}} < 2^{\mathfrak{b}}$. This only holds if assume the Generalized Continuum Hypothesis (see Axiom 4.11)
9. $\mathfrak{a}^0 = 1$; $1^{\mathfrak{a}} = 1$; $0^{\mathfrak{a}} = 0$ if $\mathfrak{a} > 0$.

Furthermore, if X is a non-empty set with cardinal number $|X| = \mathfrak{a}$, then $\mathfrak{a}$ is strictly smaller than $2^{\mathfrak{a}}$, as proven below.

Theorem 1.14 (Cantor)**.** Let X be a set, then $|X| < |P(X)|$.

Proof. Consider the function

$$\begin{aligned} \phi : X &\longrightarrow P(X) \\ x &\longmapsto \{x\}. \end{aligned}$$

It is clear that ϕ is an injective function, so by definition $|X| \leq |P(X)|$. To show that the inequality is strict it is enough to show that there does not exist any surjective map from X to $P(X)$. Suppose, for the sake of contradiction, that there exists a surjective function f from X to $P(X)$. Then there must exist some $y \in X$ such that

$$f(y) = \{x \in X : x \notin f(x)\}.$$

But this is not possible because we observe that $y \in \{x \in X : x \notin f(x)\}$ if and only if $y \notin \{x \in X : x \notin f(x)\}$. □

Lemma 1.15. Let A be a set with cardinal number $|A| = \mathfrak{a}$, then $|P(A)| = 2^{\mathfrak{a}}$.

Proof. By definition it is enough to find a bijective function between $P(A)$ and $\{0,1\}^A$. Consider the map

$$\begin{aligned} \Phi : P(A) &\longrightarrow \{0,1\}^A \\ X &\longmapsto \Phi_X : A \longrightarrow \{0,1\} \\ x &\longmapsto \Phi_X(x) = \begin{cases} 0 & \text{if } x \in X, \\ 1 & \text{if } x \notin X. \end{cases} \end{aligned}$$

We claim that Φ is a bijective function from $P(A)$ to $\{0,1\}^A$, and so $|P(A)| = |\{0,1\}^A| = 2^{\mathfrak{a}}$.

To prove the claim we will first show that Φ is injective. Suppose that $\Phi(X) = \Phi(Y)$, for some X and Y belonging to $P(X)$. Then by definition we have that $\Phi_X(x) = \Phi_Y(x)$ for all $x \in A$, in other words, $x \in X$ if and only if $x \in Y$. It follows that $X = Y$. To prove that Φ is surjective suppose that f is a map from A to $\{0,1\}$. Then we define

$$X = \{x \in A : f(x) = 0\}.$$

It is clear that $\Phi(X) = \Phi_X = f$. □

We have seen that for a cardinal number $\mathfrak{a}$, $\mathfrak{a} < 2^{\mathfrak{a}}$. Knowing this, one could ask if there is any cardinal between $\mathfrak{a}$ and $2^{\mathfrak{a}}$. This problem is known as the Generalized Continuum Hypothesis (see Axiom 4.11), which states that there does not exist any set with cardinality between $\mathfrak{a}$ and $2^{\mathfrak{a}}$. A weaker version of this claim is the Continuum Hypothesis which says that there does not exist any set with cardinality between $\aleph_0$ and $2^{\aleph}_0$, where $\aleph_0$ is cardinal of the set $\mathbb{N}$. It is known that this statement is independent of Zermelo–Fraenkel set theory with the Axiom of Choice (ZFC) (see Appendix). This means that either the Continuum Hypothesis or its negation can be added as an axiom to ZFC set theory, with the resulting theory being consistent if and only if ZFC is consistent.

The following two theorems prove that the cardinal numbers are totally ordered.

Theorem 1.16 (Cantor-Bernstein)**.** Let A and B be two sets with cardinality $|A|$ and $|B|$ respectively. If $|A| \leq |B|$ and $|B| \leq |A|$, then $|A| = |B|$.

Proof. Since $|A| \leq |B|$ and $|B| \leq |A|$, we have that there exist two injective functions:

$$f_1 : A \longrightarrow B \quad \text{and} \quad f_2 : B \longrightarrow A.$$

Note that $f_2(B)$ is a subset of A and it has the same cardinal number as B, because f_2 is injective. So it suffices to show that A and $f_2(B)$ have the same cardinal number and we can assume that $B = f_2(B)$. In particular, $B \subseteq A$. Next, we set $A_1 = f_2(f_1(A))$ and we define the following map

$$f = f_2 \circ f_1 : A \longrightarrow A_1.$$

Note that f is a bijection, because on the one hand it is the composition of two injective functions, so it is injective and the image of f is A_1, so it is also surjective. As a consequnce we obtain that $|A| = |A_1|$.

We also define inductively the following sets, for all $n \in \mathbb{N}$,

$$\begin{aligned} A_0 =& A, \qquad A_{n+1} = f(A_n), \\ B_0 =& B, \qquad B_{n+1} = f(B_n), \end{aligned}$$

and the map

$$\begin{aligned} g : A &\longrightarrow B \\ x &\longmapsto \begin{cases} f(x) & \text{if } x \in A_n - B_n \text{ for some } n, \\ x & \text{otherwise.} \end{cases} \end{aligned}$$

We claim that g is the required bijection between A and B.

To prove the claim we start by showing that g is injective. Suppose that $x, y \in A$ and $g(x) = g(y)$. Suppose that $x \notin A_n - B_n$ for any $n \in \mathbb{N}$, then $g(x) = x$. If $y \notin A_n - B_n$ for any $n \in \mathbb{N}$ then we also have that $g(y) = y$, and so $x = y$. On the other hand, if $y \in A_n - B_n$ for some $n \in \mathbb{N}$, we know that $g(y) = f(y)$. From $g(x) = g(y)$ we get that $x = f(y) \in A_{n+1}$. Since $x \notin A_n - B_n$ for any $n \in \mathbb{N}$, we deduce that $x \in B_{n+1}$, and so there must exists some $z \in B_n$ such that $f(z) = x$. It follows that $f(z) = x = f(y)$, and using the injectivity of f we have that $z = y$. But this is a contradiction since $z \in B_n$ and $y \in A_n - B_n$.
Suppose now that $x \in A_n - B_n$ for some $n \in \mathbb{N}$, by the same reason as before, it follows that $y \in A_n - B_n$ for some $n \in \mathbb{N}$, so we have that $g(x) = f(x) = f(y) = g(y)$. Finally since f is injective we conclude that $x = y$.

To show surjectivity suppose that $y \in B - g(A)$. Then $g(y) \neq y$, which means that $y \in A_n - B_n$ for some $n > 0$ (note that $y \in B = B_0$). So we deduce that $y = f(a)$ for some $a \in A_{n-1} - B_{n-1}$. Hence $y = g(a)$. □

Theorem 1.17 (Total ordering of cardinal numbers)**.** Let A and B be two sets with cardinal numbers $|A|$ and $|B|$ respectively. Then we have that $|A| \leq |B|$, or $|B| \leq |A|$.

Proof. We need to find an injective function from A to B, or an injective function from B to A.

We define the set

$$\Omega = \{(C, D, g) : C \subseteq A, D \subseteq B \text{ and } g : C \to D \text{ is a bijection}\}$$

and we give Ω the following order relation:

$$(C, D, g) \prec (C', D', g') \text{ if and only if } C \subseteq C', D \subseteq D' \text{ and } g = g'|_C.$$

We want to show that $(\Omega, \prec)$ satisfies the conditions of Zorn's Lemma. First of all note that Ω is not empty. Indeed, fix $a \in A$ and $b \in B$ and consider the function f sending a to b. Clearly f is a bijection, so $(\{a\}, \{b\}, f)$ is in Ω. Now suppose that $\mathcal{A} = \{(C_i, D_i, g_i) : i \in I\} \subset \Omega$ is a totally ordered subset. We define

$$C = \bigcup_{i \in I} C_i, \qquad D = \bigcup_{i \in I} D_i$$

and g the unique function with the property that $g|_{C_i} = g_i$ for all $i \in I$. Then clearly (C, D, g) is an upper bound of $\mathcal{A}$.

So we have by Zorn's Lemma that Ω has a maximal element, let us denote it by (A_0, B_0, f). We claim that $A_0 = A$ or $B_0 = B$. Suppose otherwise, then take $a \in A - A_0$, $b \in B - B_0$ and consider the function

$$f' : A_0 \cup \{a\} \longrightarrow B_0 \cup \{b\}$$
$$x \longmapsto f'(x) = \begin{cases} f(x) & \text{if } x \in A_0, \\ b & \text{if } x = a. \end{cases}$$

Clearly $(A_0 \cup \{a\}, B_0 \cup \{b\}, f')$ is greater than (A_0, B_0, f), which is a contradiction. We conclude by saying that if $A = A_0$, then $f : A \to B$ is injective, and if $B = B_0$ then $f^{-1} : B \to A$ is injective. □

We end this section by proving some important properties about cardinal numbers.

Lemma 1.18. If $\mathfrak{a}$ is an infinite cardinal and $\mathfrak{a} = \mathfrak{a}^2$, then $\mathfrak{a} = 2\mathfrak{a}$.

Proof. Since $1 \leq 2 \leq \mathfrak{a}$, we have that $\mathfrak{a} \leq 2\mathfrak{a} \leq \mathfrak{a}^2 = \mathfrak{a}$. □

Theorem 1.19. Let A be a set with infinite cardinality $|A|$ and let B be any non-empty set with cardinal number $|B|$. Suppose that $1 \leq |B| \leq |A|$. Then $|A| \cdot |B| = |A|$.

Proof. Is clear that $|A| \leq |B| \cdot |A| \leq |A| \cdot |A|$. So it suffices to show that $|A| = |A| \cdot |A|$. Using Zorn's Lemma we want to find a bijective function $f : A \to A \times A$.

We define the set

$$\Omega = \{(D, f) : D \subseteq A \text{ and } f : D \to D \times D \text{ a bijection}\}$$

with the following order relation

$$(D, f) \prec (D', f') \text{ if and only if } D \subseteq D' \text{ and } f'|_D = f.$$

Since A is an infinite set, there exists a subset D of A with cardinality $\aleph_0$, and it is known that for this set $|D| = |D \times D|$ so Ω is non empty. Consider now $\mathcal{A} = \{(D_i, f_i) : i \in I\} \subset \Omega$ a totally ordered subset. We define

$$D = \bigcup_{i \in I} D_i$$

and $f : D \to D \times D$ the unique function with the property that $f|_{D_i} = f_i$ for all $i \in I$. The function f is clearly injective, and

$$f(D) = f\left(\bigcup_{i \in I} D_i\right) = \bigcup_{i \in I} f|_{D_i}(D_i) = \bigcup_{i \in I} f_i(D_i) = \bigcup_{i \in I} (D_i \times D_i) = D \times D.$$

Note that the last equality is true because for all $i, j \in I$, either $D_i \subseteq D_j$ or $D_j \subset D_i$.
So we have that $(D, f) \in \Omega$ and it is an upper bound of $\mathcal{A}$. By Zorn's Lemma, there is a maximal element in Ω, let us call it (D, f), which by construction satisfies

$$|D| \cdot |D| = |D|. \tag{4}$$

We would like to have that $D = A$, but this is not true in general. Although, it is enough to show that $|A| = |D|$. We will prove this by contradiction.

We know that $|D| \leq |A|$, so assume that $|D| < |A|$. Consider the set $G = A - D$, then we have that

$$|G| + |D| = |A|.$$

Since $|D| < |A|$, we have that $|D| < |G|$. Indeed, suppose otherwise, then $|A| = |G| + |D| \leq |D| + |D| = 2|D|$, and by Lemma 1.18, $|A| \leq 2|D| = |D|$ which is a contradiction. So there exists a subset of G with cardinality $|D|$, let us call this subset E. Now consider the set

$$P = (E \times E) \cup (E \times D) \cup (D \times E).$$

Note that $E \cap D = \emptyset$ so the three subsets above are disjoint. This way we have that

$$|P| = |D| \cdot |D| + |D| \cdot |D| + |D| \cdot |D| = |D| = |E|$$

by (4). So let $g : E \to P$ be a bijection. Moreover, using that $E \cap D = P \cap D \times D = \emptyset$ we can produce a bijection

$$h : D \cup E \longrightarrow P \cup (D \times D)$$

such that $h|_D = f$ and $h|_E = g$. Finally, since $P \cup (D \times D) = (D \cup E) \times (D \cup E)$ we have that the pair $(D \cup E, h) \in \Omega$ which contradicts the maximality of (D, f). □

Corollary 1.20. If $\mathfrak{a}$ is an infinite cardinal number, and if $\mathfrak{b}$ is a cardinal number with $2 \leq \mathfrak{b} \leq 2^{\mathfrak{a}}$, then $\mathfrak{b}^{\mathfrak{a}} = 2^{\mathfrak{a}}$. In particular $\mathfrak{a}^{\mathfrak{a}} = 2^{\mathfrak{a}}$.

Proof. We have that $2^{\mathfrak{a}} \leq \mathfrak{b}^{\mathfrak{a}} \leq (2^{\mathfrak{a}})^{\mathfrak{a}}$. By Theorem 1.19 we get that $(2^{\mathfrak{a}})^{\mathfrak{a}} = 2^{\mathfrak{a} \cdot \mathfrak{a}} = 2^{\mathfrak{a}}$, and by Theorem 1.17 we deduce that $\mathfrak{b}^{\mathfrak{a}} = 2^{\mathfrak{a}}$. □

1.3 Alephs

At the beginning of the previous section we assumed that we can assign a cardinal number $|X|$ to each set X and that two sets have the same cardinal number if there exists a bijective function between them. We will show this fact in the paragraph below.

We say that an ordinal number α is a cardinal number if $|\alpha| \neq |\beta|$ for any $\beta < \alpha$. By Theorem 1.10 every set is isomorphic to a unique ordinal number, so for a set X we have that there exists an ordinal α such that

$|X| = |\alpha|$. So we can define the cardinal of a set X to be the least ordinal with the same cardinal as X. In other words,

$$|X| = \text{the least element in } \{\alpha \in Ord : |\alpha| = |X|\}. \tag{5}$$

We observe that the class of cardinal numbers *Card* is a subclass of the class of ordinal numbers *Ord*. Morover, this clearly shows that we can assign a cardinal number to each set and that two sets have the same cardinality if there exists a bijective function between them. Note that in the case of finite ordinals $|\alpha| \neq |\beta|$ holds for any $\beta < \alpha$, so all finite ordinals are cardinals. Furthermore, if X is a finite set, then the assignment given by (5) agrees with the definitions that we have given on sections Sections 1.1 and 1.2. This is $|X|$ is equal to the number of elements in X.

From the assignment given on (5), we deduce that all infinite cardinals are limit ordinals. Nevertheless, not all limit ordinals are cardinals. For example, even though $\omega \cdot \omega$ is a limit ordinal it is not a a cardinal, since $|\omega \cdot \omega| = |\omega| \cdot |\omega| = |\omega| = \omega$. Recall that ω is the least non-zero limit ordinal or the least infinite cardinal. The infinite ordinals that are cardinals are called *alephs* and denoted by $\aleph$.

Using the fact that ordinals are ordered and that all infinite cardinals are alephs we can define an increasing enumeration of all cardinals as follows. We define $\aleph_0$ to be the first infinite ordinal that is a cardinal, $\aleph_1$ the second infinite ordinal that is a cardinal and so on. This way, if α is an ordinal, then $\aleph_\alpha$ is the infinite cardinal in the position α and we obtain the following chain of cardinals

$$\aleph_0 < \aleph_1 < \aleph_2 < \cdots < \aleph_\omega < \aleph_{\omega+1} < \aleph_{\omega+2} < \cdots < \aleph_{\omega\cdot\omega} < \cdots \tag{6}$$

We end this chapter by saying that any set with cardinal number $\aleph_0$ is said to be *infinite countable*, because it will be in bijection with $\mathbb{N}$ which is an infinite countable set. While any infinite set that has cardinal number different from $\aleph_0$ will be called *uncountable*.

2 Cardinality of profinite groups

In this chapter, we want to prove some results about profinite groups that will be useful in the final chapter. First, we want to show that if G is an infinite profinite group, then $|G| = 2^{\mathfrak{a}}$, where $\mathfrak{a}$ is the cardinal of any fundamental system of neighborhoods of 1 consisting of open subgroups of G (see Definition 2.4). Later we want to show that under certain conditions a map from a profinite group G to a Hausdorff topological space Y is constant on a big enough subset of G. Both of these proofs require some work involving chains of closed normal subgroups of a profinite group G and the cardinality of the fundamental system of neighborhoods of 1 of G.

2.1 Preliminaries on topology and profinite groups

In this section we will present some basic topological definitions and some properties about profinite groups.

Definition 2.1. Let X be a topological space, we say that $Y \subseteq X$ is a *clopen subset* of X, or just clopen, if Y is both closed and open.

Definition 2.2. Let X be a topological space. A *base of open sets* of X is a collection $\mathcal{B}$ of open subsets of X satisfying the following properties:

1. The elements in $\mathcal{B}$ cover X, that is, $\bigcup_{B\in\mathcal{B}} B = X$.
2. Let $B_1, B_2 \in \mathcal{B}$. Then for any $x \in B_1 \cap B_2$ there exists $B_3 \in \mathcal{B}$ such that $x \in B_3 \subseteq B_1 \cap B_2$.

In particular, every open set in X is a union of open subsets in $\mathcal{B}$.

Definition 2.3. Let X be a topological space and suppose that Y is a non-empty subset of X. Then an *open neighborhood* of Y is any open subset of X containing Y. A *neighborhood* of Y is any subset of X containing an open neighborhood of Y. When $Y = \{x\}$ we say neighborhoods of x.

Definition 2.4. Let X be a topological space and suppose that Y is a non-empty subset of X. Then a *fundamental system of neighborhoods* of Y is a family of subsets $\mathcal{U} = \{U_i\}_{i\in I}$ of X, such that every neighborhood of Y contains one of the sets U_i.

Definition 2.5. Let X be a topological space. Then we write $\rho(X)$ for the cardinal of all the clopen subsets of X.

Definition 2.6. If G is a topological group then we write $w_0(G)$ to denote the smallest cardinal of a fundamental system of open neighborhoods of 1 in G.

Definition 2.7. Let G be a profinite group and suppose that X is a subset of G. We say that X *converges* to 1 if every open subgroup U of G contains all but a finite number of the elements in X.

Remark 2.8. Let G be a profinite group and assume that X is a subset of G. Then we write $\langle X \rangle$ for the closure, in the profinite space G, of the abstract subgroup generated by X. Moreover, whenever we refer to a subgroup of G, we will be assuming that the subgroup mentioned is closed, otherwise we will refer to it as abstract subgroup.

Theorem 2.9. Let G be a topological group. Then the following are equivalent.

a) G is a profinite group;

b) G is compact, Hausdorff, totally disconnected;

c) G is compact and the identity element 1 of G admits a fundamental system $\mathcal{U}$ of open neighborhoods U such that $\bigcap_{U \in \mathcal{U}} U = 1$ and each U is an open normal subgroup of G;

d) The identity element 1 of G admits a fundamental system $\mathcal{U}$ of open neighborhoods U such that each U is a normal subgroup of G, and

$$G = \varprojlim_{U \in \mathcal{U}} G/U.$$

Proof. See Theorem 2.1.3 on [9]. □

Proposition 2.10. Let $\{X_i, \varphi_{i,j}, I\}$ be an inverse system of compact Hausdorff spaces and X a compact Hausdorff space. Suppose that $\{\varphi_i : X \to X_i\}_{i \in I}$ is a set of compatible continuous surjective mappings. Then the corresponding induced mapping $\theta : X \to \varprojlim X_i$ is onto.

Proof. See Corollary 1.1.6 on [9]. □

2.2 Fundamental systems of neighborhoods of a profinite group

We start this section showing that if G is an infinite profinite group, then the cardinal of any fundamental system of neighborhoods of 1 consisting of open subgroups of G is equal to $\rho(G)$, in particular, $w_0(G)$ is the cardinal of any fundamental system of neighborhoods of 1 consisting of open subgroups of G.

Proposition 2.11 (See Proposition 2.6.1 on [9])**.** Let G be an infinite profinite group. Then the cardinal of any fundamental system of neighborhoods of 1 consisting of open subgroups of G is equal to $\rho(G)$. In particular, $w_0(G) = \rho(G)$.

Proof. First of all note that by Theorem 2.9 there exists a fundamental system of neighborhoods of 1 consisting of open subgroups of G.
Let $\mathcal{U}$ be a fundamental system of neighborhoods of 1 consisting of open subgroups of G. Note that in a profinite group all open subgroups are also closed, so it is clear that $|\mathcal{U}| \leq \rho(G)$.
To prove the converse note that $\mathcal{B} = \{gU : U \in \mathcal{U} \text{ and } g \in G\}$ is a base of open sets in G. Moreover, $|\mathcal{B}| = |\mathcal{U}|$. Indeed, since all open subgroups of G have finite index, it follows that

$$\begin{aligned} |\mathcal{B}| = |\{gU : U \in \mathcal{U} \text{ and } g \in G\}| &= \left| \bigcup_{U \in \mathcal{U}} \{gU : g \in G\} \right| \\ &\leq \aleph_0 |\mathcal{U}| = |\mathcal{U}|. \end{aligned}$$

We use the fact that the cardinal of $\mathcal{U}$ is infinite, this is because G is infinite.
Next, let W be a clopen subset of G. Then, there exists a collection of elements in $\mathcal{B}$ whose union is W. Moreover, the group G is profinite, so it is compact and Hausdorff. This implies that W is compact and so there exists a finite collection of elements in $\mathcal{B}$ whose union is W. Knowing this fact consider the map

$$\begin{aligned} \Phi : \{W \subseteq G : W \text{ is a clopen subset of } G\} &\longrightarrow \{\mathcal{W} \subseteq \mathcal{B} : \ \mathcal{W} \text{ is finite}\} \\ W &\longmapsto \Phi(W) \end{aligned}$$

where $\Phi(W)$ is a finite collection of elements in $\mathcal{B}$ covering of W. Clearly, Φ is injective, so it follows that $\rho(G) \leq |\{\mathcal{W} \subseteq \mathcal{B} : \ \mathcal{W} \text{ is finite}\}|$, and hence we deduce that

$$\rho(G) \leq |\{\mathcal{W} \subseteq \mathcal{B} : \ \mathcal{W} \text{ is finite}\}| \leq \aleph_0 \cdot |\mathcal{B}| = \aleph_0 \cdot |\mathcal{U}| = |\mathcal{U}|.$$

Here we use again that $|\mathcal{U}|$ is infinite. □

Remark 2.12. It is clear that G is finite if and only if $w_0(G)$ is finite, and if this is the case, then $w_0(G) = 1$.

The following proposition shows that the number of generators and the cardinality of any fundamental system of open neighborhoods of 1 of a profinite group are related.

Proposition 2.13 (See [9], Proposition 2.5.1 and Proposition 2.6.2)**.** Let G be an infinite profinite group.

(a) If X is an infinite closed set of generators of G, then $w_0(G) = \rho(X)$.

(b) If X is an infinite set of generators of G converging to 1, then $|X| = w_0(G)$.

(c) If X is a finite set of generators of G, then $w_0(G) = \aleph_0$.

Proof. (a) Note that by Theorem 2.9 the set of open normal subgroups of G is a a fundamental system of neighborhoods of the identity, and so its cardinal is equal to $w_0(G)$. Moreover, any open normal subgroup of G is the kernel of some surjective continuous homomorphism from G to a finite group.

Let H be a finite group and suppose that $\varphi : G \to H$ is a continuous homomorphism. Then φ is completely determined by its restriction to X. Furthermore, since H has the discrete topology, the continuous map $\varphi : X \to H$ is determined by the images of at most $|H|$ clopen subsets. So we deduce that for each finite group H there exist at most $\rho(X)$ continuous homomorphisms from G to H.

Since X is a closed subset of a profinite space G, it follows that it is also X is also a profinite space and so it is Hausdorff and admits a basis consisting of clopen subsets. These two facts combined with X being infinite imply that X has an infinite number of clopen subsets. The number of non-isomorphic finite groups is countable, so we conclude that the number of surjective continuous homomorphisms from G to a finite subgroup is at most $\rho(X)$. This implies that the number of open normal subgroups of G is less than or equal to the number of clopen subsets of X, this is, $w_0(G) \leq \rho(X)$.
On the other hand, since $X \subseteq G$, we deduce that $\rho(X) \leq \rho(G) = w_0(G)$, where the last equality comes from Proposition 2.11. So $w_0(G) = \rho(X)$.

To prove (b) note that by [9, Exercise 2.4.3] the induced topology on $X - \{1\}$ by G is the discrete topology, and that $\overline{X} = X \cup \{1\}$ is the one-point compactification of $X - \{1\}$. Then by definition, the open sets in the one-point compactification of $X - \{1\}$ are

$$\{U : U \text{ open subset of } X - \{1\}\} \cup \{\overline{X} \setminus C : C \text{ is compact in } X - \{1\}\}.$$

Since $X - \{1\}$ has the discrete topology, it follows that the open subsets in $\overline{X} = X \cup \{1\}$ are

$$\{U : U \subseteq X - \{1\}\} \cup \{\overline{X} \setminus C : C \subseteq X - \{1\} \text{ and finite}\}.$$

So the clopen subsets in $\overline{X} = X \cup \{1\}$ are the finite subsets of $X - \{1\}$ and their complements. Since X is infinite we deduce that $\rho(\overline{X}) = |X|$, and by (a), we get that $|X| = \rho(\overline{X}) = w_0(G)$.

(c) follows from the claim that for any $n \in \mathbb{N}$ there exist only finitely many $N \trianglelefteq_o G$ with index n. Let $\mathcal{N}$ be the set of all open normal subgroups of G and let $\mathcal{N}^{[m]}$ be the set of all open normal subgroups of G with index m. Then we deduce, using the claim, that

$$|\mathcal{N}| = \sum_{n \in \mathbb{N}} |\mathcal{N}^{[n]}| \leq \sum_{n \in \mathbb{N}} \aleph_0 = \aleph_0.$$

Note that $\mathcal{N}$, the set of all open normal subgroups of G, is in particular a fundamental system of neighborhoods of 1 consisting of open subgroups. This implies that $w_0(G) = |\mathcal{N}| \leq \aleph_0$. But since G is infinite, we know that $w_0(G)$ can not be finite so $w_0(G) \geq \aleph_0$. This concludes that $w_0(G) = \aleph_0$.
It remains to prove the claim. Let N be a closed normal subgroup of G and assume that it has index n. Such a group is the kernel of an epimorphism $\varphi : G \to R$, for some finite group R of order n, and such an epimorphism is determined by its values on X. Therefore, for a fixed finite group R there is only a finite number of epimorphisms from G to R. Moreover, for a fixed natural number n there are only finitely many groups of order n. Thus, for a fixed natural number n, there are finitely many open normal subgroups of G of index n. □

The following result is a characterization of the value $w_0(G)$, and it is a powerful tool when proving results by transfinite induction as can be seen in the proofs of Theorem 2.20 and Theorem 2.23.

Theorem 2.14 (See Theorem 2.6.4 in [9])**.** Let G be a profinite group. Let μ be an ordinal and $|\mu|$ its cardinal. Then $w_0(G) \leq |\mu|$ if and only if there exists a chain of closed normal subgroups G_λ of G, indexed by ordinals $\lambda \leq \mu$

$$G = G_0 \geq G_1 \geq ... \geq G_\lambda \geq ... \geq G_\mu = 1 \tag{7}$$

such that

a) $G_\lambda / G_{\lambda+1}$ is a finite group;

b) if λ is a limit ordinal, then $G_\lambda = \bigcap_{\nu<\lambda} G_\nu$.

Moreover, if G is infinite, μ and the chain (7) can be chosen in such a way that

c) $w_0(G/G_\lambda) < w_0(G)$ for $\lambda < \mu$.

To prove this theorem we first need a preliminary lemma.

Lemma 2.15 (See Proposition 2.1.5 in [9])**.** a) Let $\{H_i : I \in I\}$ be a collection of closed subgroups of a profinite group G. Suppose that $\bigcap_{i\in I} H_i$ is contained in some open subgroup U of G. Then there exists a finite subset J of I such that

$$\bigcap_{j\in J} H_j \leq U.$$

b) Let $\{U_i : I \in I\}$ be a collection of open subgroups of a profinite group G, such that $\bigcap_{i\in I} U_i = 1$. Consider the set

$$\mathcal{V} = \left\{ \bigcap_{i\in J} U_i : J \text{ is a finite subset of } I \right\}.$$

Then $\mathcal{V}$ is a fundamental system of neighborhoods of 1 in G.

Proof. To prove a) note that $\{G - H_i : i \in I\}$ is an open cover of $G - U$. Moreover, the group G is profinite, so it is Hausdorff and compact and it follows that the closed subset $G - U$ is compact. We deduce that there exists a finite covering $\{G - H_i : i \in J\}$ of $G - U$, where J is a finite subset of I. It follows that

$$G - U \subseteq \bigcup_{i\in J} G - H_i$$

and by taking complements in G we deduce that

$$\bigcap_{i\in J} H_i \subseteq U.$$

In fact, since we are working with subgroups we get that $\bigcap_{i\in J} H_i$ is a subgroup of U.

For part b) note that any neighborhood of 1 will contain a finite intersection of elements in $\{U_i : i \in I\}$ by part a). And so $\mathcal{V}$ is indeed a fundamental system of neighborhoods of 1 in G. □

Proof of Theorem 2.14. If G is finite the result is clear. Let us assume that G is infinite and let μ be the smallest ordinal whose cardinal is $w_0(G)$. Since $\mu = \{\lambda : \lambda < \mu\}$, any set with cardinality $|\mu|$ can be indexed by ordinals $\lambda < \mu$. In particular any fundamental system of neighborhoods of 1 consisting of open normal subgroups of G. So let $\{U_\lambda : \lambda < \mu\}$ be a fundamental system of open neighborhoods of 1 consisting of open normal subgroups of G indexed by ordinals $\lambda < \mu$. For each $\lambda \leq \mu$ we set

$$G_\lambda = \bigcap_{\nu<\lambda} U_\nu.$$

Clearly G_λ is a closed normal subgroup of G, so G/G_λ is a profinite group. To prove a) note that $G_{\lambda+1} = G_\lambda \cap U_{\lambda+1}$, hence $G_{\lambda+1}$ is an open normal subgroup of G_λ, so it follows that $G_\lambda/G_{\lambda+1}$ is a finite group. For b), if λ is a limit ordinal then $\lambda = \bigcup_{\nu<\lambda} \nu$, so

$$G_\lambda = \bigcap_{\nu<\lambda} \left(\bigcap_{\eta<\nu} U_\eta \right) = \bigcap_{\nu<\lambda} G_\nu.$$

It just remains to show that c) also holds. For each $\lambda < \mu$

$$\{U_\nu/G_\lambda : \nu < \lambda\}$$

is a fundamental system of neighborhoods of the identity consisting of open normal subgroups of G/G_λ. Indeed, the topology in the profinite group G/G_λ agrees with the quotient topology, so in particular, if $\{U_\lambda : \lambda < \mu\}$ is a fundamental system of neighborhoods of 1 consisting of open normal subgroups of G, then $\{U_\lambda G_\lambda/G_\lambda : \lambda < \mu\} = \{U_\nu/G_\lambda : \nu < \lambda\}$ is a fundamental system of neighborhoods of the identity consisting of open normal subgroups of G/G_λ. So $w_0(G/G_\lambda) \leq |\lambda| < |\mu| = w_0(G)$. Note that $|\lambda| < |\mu|$ because μ is the smallest ordinal such that $w_0(G) = |\mu|$.

Conversely, assume that there is a chain like (7) satisfying a) and b). We want to show by transfinite induction that for $\lambda \leq \mu$, $w_0(G/G_\lambda) \leq |\lambda|$. The result is clearly true for $\lambda = 1$, since G/G_1 is finite by a). So assume that the hypothesis holds for all $\nu < \lambda$.

If λ is a successor ordinal then there exists some λ' such that $\lambda' + 1 = \lambda$. By a) we have that $|G_{\lambda'} : G_\lambda|$ is finite. This means that G_λ is open in $G_{\lambda'}$. Since $G_{\lambda'}$ has the induced topology coming from G, we have that there exists some $V \trianglelefteq_o G$ such that $G_\lambda = G_{\lambda'} \cap V$. By induction hypothesis

we have that $w_0(G/G_{\lambda'}) \leq |\lambda'|$, so there exists a fundamental system of neghborhoods of the identity in $G/G_{\lambda'}$

$$\{U/G_{\lambda'} : U \in \mathcal{U}'\} \tag{8}$$

where $\mathcal{U}'$ is a collection of open normal subgroups containing $G_{\lambda'}$ such that $|\mathcal{U}'| \leq |\lambda'|$. Consider $\mathcal{U} = \{U \cap V : U \in \mathcal{U}'\}$, a collection of open normal subgroups containing G_λ that satisfies

$$G_\lambda = \bigcap_{U \in \mathcal{U}} U. \tag{9}$$

Clearly $|\mathcal{U}| = |\mathcal{U}'| \leq |\lambda'| = |\lambda|$. Moreover, $\{U/G_\lambda : U \in \mathcal{U}\}$ is a fundamental system of neighborhoods of the identity in G/G_λ. Indeed, since (8) is a fundamental system of neighborhoods of the identity in $G/G_{\lambda'}$ it follows form Lemma 2.15 and (9) that $\{U/G_\lambda : U \in \mathcal{U}\}$ is a fundamental system of neighborhoods of the identity in G/G_λ. So $w_0(G/G_\lambda) \leq |\lambda|$.

If λ is a limit ordinal, then by induction hypothesis we have that for all $\nu < \lambda$, $w_0(G/G_\nu) \leq |\nu|$. So for each $\nu < \lambda$, there exists a set $\mathcal{U}_\nu$ of open normal subgroups of G containing G_ν such that

$$\{U/G_\nu : U \in \mathcal{U}_\nu\}$$

is a fundamental system of open neighborhoods of the identity in G/G_ν and $|\mathcal{U}_\nu| \leq |\nu|$. Let $\mathcal{U}_\lambda$ be the union of all such $\mathcal{U}_\nu$. Then

$$\bigcap_{U \in \mathcal{U}_\lambda} U = G_\lambda.$$

We set $\mathcal{U}$ as the collection of all finite intersections of groups in $\mathcal{U}_\lambda$. So by Lemma 2.15 we have that

$$\{U/G_\lambda : U \in \mathcal{U}\}$$

is a fundamental system of open neighborhoods of the identity in G/G_λ. Moreover, since λ is infinite

$$|\mathcal{U}| = |\mathcal{U}_\lambda| \leq \sum_{\nu<\lambda} |\mathcal{U}_\nu| \leq \sum_{\nu<\lambda} |\nu| \leq |\lambda|^2 = |\lambda|.$$

□

The corollary below shows that the chain in Theorem 2.14 can be refined so that all inequalities appearing on it are strict.

Corollary 2.16. Let G be a profinite group. Then for some ordinal number μ with $w_0(G) = |\mu|$ there exists a chain of closed normal subgroups G_λ of G, indexed by ordinals $\lambda \leq \mu$

$$G = G_0 \gneq G_1 \gneq \cdots \gneq G_\lambda \gneq \cdots \gneq G_\mu = 1 \tag{10}$$

such that
(a) $G_\lambda/G_{\lambda+1}$ is a finite group;
(b) if λ is a limit ordinal, then $G_\lambda = \bigcap_{\nu<\lambda} G_\nu$.

Proof. Since $|w_0(G)| = \mu$, Theorem 2.14 tells us that there exists a chain

$$G = G_0 \geq G_1 \geq \cdots \geq G_\lambda \geq \cdots \geq G_\mu = 1 \tag{11}$$

satisfying (a) and (b).

Consider the set $\Omega = \{G_\lambda : \lambda \leq \mu\}$ and let Ω' be the class of all the elements in Ω but without repetitions. We define the following class function

$$\begin{aligned} F : \Omega &\longrightarrow \Omega' \\ G_\lambda &\longmapsto [G_\lambda] \end{aligned}$$

where $[G_\lambda]$ is the unique element in Ω' that is equal to G_λ.

By the Axiom Schema of Replacement we have that $F(\Omega) = \Omega'$ is also a set. We index by ordinals all the elements in Ω' respecting the order in (11) so we get a new chain

$$G = G_0 \gneq G_1 \gneq \cdots \gneq G_\lambda \gneq \cdots \gneq G_{\mu'} = 1, \tag{12}$$

but this time all the inequalities have to be strict since there are no repeated elements in Ω'. By the way in which the new chain has been constructed, it is clear that if (11) satisfies (a) and (b), then (12) also satisfies (a) and (b). By Theorem 2.14 we deduce that $w_0(G) \leq |\mu'|$, and since $\mu \geq \mu'$ we conclude that $w_0(G) = |\mu| = |\mu'|$. □

Using Theorem 2.14 it is rather easy to see that if H is a closed normal subgroup of a profinite group G, then the fundamental systems of neighborhoods of the identity in G, H and G/H are related. This is shown in the corollary below.

Corollary 2.17 (See Corollary 2.6.5 in [9])**.** Let G be a profinite group and let H be a closed normal subgroup of G. Then there exists an ordinal number μ and a chain of closed normal subgroups H_λ of H

$$H = H_0 \geq H_1 \geq \cdots \geq H_\lambda \geq \cdots \geq H_\mu = 1$$

indexed by the ordinals $\lambda \leq \mu$, such that

a) $H_\lambda \trianglelefteq_c G$ for each $\lambda \leq \mu$;

b) $H_\lambda / H_{\lambda+1}$ is a finite group;

c) if λ is a limit ordinal, then $H_\lambda = \bigcap_{\nu<\lambda} H_\nu$;

d) if either H or G/H is an infinite group, then

$$w_0(G) = w_0(H) + w_0(G/H).$$

Proof. Let us distinguish two cases: when H is finite and when H is infinite. Assume that H is finite. By Theorem 2.14 we have that for a profinite group G there exists a chain of closed normal subgroups

$$G = G_0 \geq G_1 \geq ... \geq G_\lambda \geq ... \geq G_\mu = 1 \tag{13}$$

indexed by ordinals $\lambda \leq \mu$. Intersecting all G_λ in the chain above with H we obtain a set $\{H \cap G_\lambda : \lambda < \mu\} = \{H_0, H_1, \ldots, H_t\}$ of closed normal subgroups of G. This set clearly forms a chain

$$H = H_0 \geq H_1 \geq \cdots \geq H_t = 1$$

that satisfies a) and b).

Suppose that H is infinite. If $\mathcal{U}$ is the set of all open normal subgroups of G, then

$$\mathcal{U}(H) = \{U \cap H : U \in \mathcal{U}\} \tag{14}$$

is a fundamental system of neighborhoods of 1 consisting of open normal subgroups of H. So $|\mathcal{U}(H)| = w_0(H)$. Let μ be the smallest ordinal number with cardinality $w_0(H)$. We index the elements in $\mathcal{U}(H)$ using the ordinal numbers less than μ to get the set $\{U_\lambda : \lambda < \mu\}$. We define

$$H_\lambda = \bigcap_{\nu<\lambda} U_\nu$$

for all $\lambda \leq \mu$. The elements in (14) are closed normal subgroups in G, since they are the intersection of closed normal subgroups of G, so all H_λ are also closed normal subgroups of G. Furthermore, the subgroups H_λ clearly form a chain

$$H = H_0 \geq H_1 \geq \cdots \geq H_\lambda \geq \cdots \geq H_\mu = 1 \tag{15}$$

that satisfies a), b) and c).

It remain to prove d). Using Theorem 2.14 on the profinite group G/H is clear that the chain (15) can be extended into a chain

$$G = G_0 \geq G_1 \geq \cdots \geq G_\nu = H = H_0 \geq \cdots \geq H_\mu = 1$$

of closed normal subgroups of G satisfying a) and b) on Theorem 2.14. It follows that

$$w_0(G) \leq w_0(G/H) + w_0(H).$$

On the other hand, we have said that $\mathcal{U}$ is the set of all open normal subgroups of G, so, in particular, $\mathcal{U}$ is a fundamental system of open neighborhoods of the identity consisting on open subgroups in G, hence $|\mathcal{U}| = w_0(G)$. Moreover,

$$\{U/H : U \in \mathcal{U}, H \leq U\}$$

is a fundamental system of open neighborhoods of the identity consisting on open subgroups in G/H and

$$\{H \cap U : U \in \mathcal{U}\}$$

is a fundamental system of open neighborhoods of 1 consisting of open subgroups in H. So $w_0(G/H) \leq w_0(G)$ and $w_0(H) \leq w_0(G)$. Since $w_0(G)$ is an infinite cardinal it follows that

$$w_0(G) \geq w_0(G/H) + w_0(H),$$

and so $w_0(G) = w_0(G/H) + w_0(H)$. □

Lemma 2.18. Let G be a profinite group and let $\mathfrak{a}$ be an infinite cardinal number. Assume that $\{V_i\}_{i\in I}$ is a set of closed normal subgroups of G satisfying $w_0(G/V_i) < \mathfrak{a}$. If $|I| < \mathfrak{a}$, then $V = \bigcap_{i\in I} V_i$ is also a closed normal subgroup of G satisfying $w_0(G/V) < \mathfrak{a}$.

Proof. For each V_i we have that $w_0(G/V_i) < \mathfrak{a}$, hence, there exists some set $\mathcal{U}_i$ of open subgroups of G containing V_i such that $\{U/V_i : U \in \mathcal{U}_i\}$ is a fundamental system of open neighborhoods of the identity in G/V_i and clearly $|\mathcal{U}_i| < \mathfrak{a}$. Set $\mathcal{U}_I = \bigcup_{i\in I} \mathcal{U}_i$. Then $\bigcap_{U\in\mathcal{U}_I} U = V$ because $V = \bigcap_{i\in I} V_i$. Now consider the set of finite intersections of groups in $\mathcal{U}_I$, we will call this set $\mathcal{U}$. By Lemma 2.15 it follows that $\mathcal{U}$ is fundamental system of open neighborhoods of the identity in G/V. Furthermore,

$$|\mathcal{U}| = |\mathcal{U}_I| \leq \sum_{i\in I} |\mathcal{U}_i| < \mathfrak{a}.$$

□

It is well known that a profinite group G can be written as the inverse limit of G/U, where all U belong to $\mathcal{U}$, a fundamental system of open neighborhoods consisting of open normal subgroups of G. See, for example, Theorem 2.9 part d). In the following proposition we want to show that a profinite group G can also be written as the inverse limit of G/G_λ where the subgroups G_λ are the elements appearing in the chain (10).

Proposition 2.19. Let G be an infinite profinite group and let

$$G = G_0 \gneq G_1 \gneq \cdots \gneq G_\lambda \gneq \cdots \gneq G_\mu = 1$$

be the chain appearing in Corollary 2.16. Then, G can be written as the following inverse limit:

$$\varprojlim_{\lambda \leq \mu} G/G_\lambda. \tag{16}$$

Proof. To prove this proposition it is enough to show that there exists an isomorphism between G and the inverse limit in (16). Note that any g in G can be mapped to a coherent sequence of the form $(gG_\lambda)_{\lambda \leq \mu}$. This mapping defines a function

$$\begin{aligned} \pi : G &\longrightarrow \varprojlim_{\lambda \leq \mu} G/G_\lambda \\ g &\longmapsto (gG_\lambda)_{\lambda \leq \mu}. \end{aligned}$$

We claim that π is the needed isomorphism. Note that

$$(ghG_\lambda)_{\lambda \leq \mu} = (gG_\lambda)_{\lambda \leq \mu}(hG_\lambda)_{\lambda \leq \mu}$$

so π is a group homomorphism. It remains to prove that it is both injective and surjective. The former is proved by $\ker(\pi) = \cap_{\lambda \leq \mu} G_\lambda = G_\mu = 1$ while the later follows from Proposition 2.10. Indeed, observe that all G/G_λ and G are profinite groups, thus, compact and Hausdorff spaces. In addition $\{G \to G/G_\lambda\}_{\lambda \leq \mu}$ is a set of compatible continuous surjective mappings. Thus, all the hypothesis of Proposition 2.10 are satisfied. □

2.3 Cardinality of profinite groups

In this section we will prove our fist important result, namely that for an infinite profinite group G, the cardinal of G is equal to $2^{w_0(G)}$ where $w_0(G)$ is the cardinal of any fundamental system of neighborhoods of 1 consisting of open subgroups. An alternative proof of this theorem can also be found in [12, Theorem 4.9].

Theorem 2.20. Let G be an infinite profinite group and suppose that $\mathcal{N}$ is a fundamental system of neighborhoods of 1 consisting of open subgroups of G. Then we have that

$$|G| = 2^{|\mathcal{N}|}.$$

Recall that $|\mathcal{N}| = w_0(G)$.

Proof. We say that $2^{|\mathcal{N}|} \leq |G|$ if there exists an injective function going from a set with cardinal number $2^{|\mathcal{N}|}$ to a set with cardinal number $|G|$. Since G is a profinite group, by Corollary 2.16, we know that there exists a chain of closed normal subgroups G_λ of G, indexed by ordinals $\lambda \leq \mu$

$$G = G_0 \gneq G_1 \gneq \cdots \gneq G_\lambda \gneq \cdots \gneq G_\mu = 1$$

where $|\mu| = w_0(G) = |\mathcal{N}|$. Let Ω be the set containing all the subgroups G_λ, then

$$|\Omega| = |\{G_\lambda : \lambda \leq \mu\}| = |\mu| = |\mathcal{N}|.$$

So $\{0,1\}^\Omega$ is a set with cardinal number $2^{|\mathcal{N}|}$. On the other hand, we know from Proposition 2.19 that

$$G \cong \varprojlim_{\lambda \leq \mu} G/G_\lambda.$$

We want to construct an injective map from $\{0,1\}^\Omega$ to $\varprojlim_{\lambda \leq \mu} G/G_\lambda$. Consider an arbitrary map

$$\begin{aligned} f : \Omega &\longrightarrow \{0,1\} \\ G_\lambda &\longmapsto f(G_\lambda) \end{aligned}$$

belonging to $\{0,1\}^\Omega$.

For any $\lambda < \mu$, we have that $G_\lambda/G_{\lambda+1}$ is a non-trivial finite group, so for any $z_\lambda \in G/G_\lambda$ there exist at least two different elements in $G/G_{\lambda+1}$ that are mapped to z_λ by

$$G/G_{\lambda+1} \longrightarrow G/G_\lambda. \tag{17}$$

So for any $\lambda < \mu$ and any $z_\lambda \in G/G_\lambda$ we can define a function

$$\widetilde{z_\lambda} : \{0,1\} \longrightarrow G/G_{\lambda+1}$$

where $\widetilde{z_\lambda}(0)$ and $\widetilde{z_\lambda}(1)$ are the two distinct elements that are mapped to z_λ by (17).

Pick $z_0 = 1 \in G/G_0$, then by transfinite induction on λ we define for each $\lambda < \mu$

$$z_{\lambda+1} = \widetilde{z_\lambda}\left(f(G_\lambda)\right) \in G/G_{\lambda+1}.$$

The sequence $\left(\widetilde{z_\lambda}\left(f(G_\lambda)\right)\right)_{\lambda<\mu}$ is clearly coherent and belongs to $\varprojlim_{\lambda\leq\mu} G/G_\lambda$. Moreover, the mapping

$$\begin{aligned} \{0,1\}^\Omega &\longrightarrow \varprojlim_{\lambda\leq\mu} G/G_\lambda \\ f &\longmapsto \left(\widetilde{z_\lambda}\left(f(G_\lambda)\right)\right)_{\lambda<\mu} \end{aligned}$$

is injective because $\left(\widetilde{z_\lambda}\left(f(G_\lambda)\right)\right)_{\lambda<\mu} = \left(\widetilde{z_\lambda}\left(g(G_\lambda)\right)\right)_{\lambda<\mu}$ if and only if $\widetilde{z_\lambda}\left(f(G_\lambda)\right) = \widetilde{z_\lambda}\left(g(G_\lambda)\right)$ for all $\lambda < \mu$ and this can only happen if $f(G_\lambda) = g(G_\lambda)$ for each $\lambda < \mu$. This proves that

$$2^{|N|} = |\{0,1\}^\Omega| \leq \left|\varprojlim_{\lambda\leq\mu} G/G_\lambda\right| = |G|.$$

The converse follows from the fact below:

$$G = \varprojlim_{N\in\mathcal{N}} G/N \leq \prod_{N\in\mathcal{N}} G/N.$$

Then, it is clear that

$$|G| \leq \left|\prod_{N\in\mathcal{N}} G/N\right| = \prod_{N\in\mathcal{N}} |G/N| \leq \prod_{N\in\mathcal{N}} \aleph_0 = \aleph_0^{|\mathcal{N}|}.$$

Since G is infinite we conclude that $\aleph_0^{|\mathcal{N}|} = 2^{|\mathcal{N}|}$ by Corollary 1.20 . □

2.4 Subsets of profinite groups in which continuous functions are constant

In this section we will prove that if a continuous map from a profinite group to a Hausdorff space has a "small image", then it is constant on a "big" coset. This is a very powerful tool that will allow us to prove results about words in profinite groups in the next chapter. Note that this is a generalization of [1, Proposition 2.1].

Lemma 2.21. Let G be a profinite group and let λ be an ordinal number. Suppose that the family $\mathcal{N} = \{V_\mu\}_{\mu<\lambda}$ of open subgroups of G is a chain, in the sense that $\mu' \geq \mu$ implies $V_{\mu'} \leq V_\mu$. If $\bigcap_{\mu<\lambda} V_\mu = 1$, then $\mathcal{N}$ is a fundamental system of open neighborhoods of the identity in G and so $w_0(G) = |\lambda|$.

Proof. This is a special case of Lemma 2.15. □

Lemma 2.22. Let $\varphi : G \to Y$ be a continuous map, where G is a profinite group and Y is a Hausdorff topological space, and let $\mathcal{N}$ be a fundamental system of open neighborhoods of the identity of G consisting of open normal subgroups. If φ is non-constant, then there exist $g_1, g_2 \in G$ and $V_1, V_2 \in \mathcal{N}$ such that

$$(g_1V_1)\varphi \cap (g_2V_2)\varphi = \varnothing.$$

Proof. By hypothesis there exist two different elements y_1, y_2 in $G\varphi$. Since Y is Hausdorff, we can find two open subsets U_1 and U_2 of Y such that $y_i \in U_i$ for $i = 1, 2$. Then $(U_i)\varphi^{-1}$ is open in G and since $\mathcal{N}$ is a fundamental system of open neighborhoods of the identity, there exists a coset g_iV_i inside $(U_i)\varphi^{-1}$ for some $V_i \in \mathcal{N}$. Now it is clear that $(g_1V_1)\varphi \cap (g_2V_2)\varphi \subseteq U_1 \cap U_2 = \varnothing$. □

Theorem 2.23. Let $\varphi : G \to Y$ be a continuous map, where G is a profinite group and Y is a Hausdorff topological space, and let $\mathcal{N}$ be a fundamental system of open neighborhoods of the identity of G consisting of open normal subgroups. Assume that $|G\varphi| < 2^{\mathfrak{a}}$, where $\mathfrak{a}$ is an infinite cardinal. Then there exists a subgroup V of G such that:

1. V is an intersection of subgroups in $\mathcal{N}$. In particular, $V \trianglelefteq_{\mathrm{c}} G$.
2. $w_0(G/V) < \mathfrak{a}$.
3. φ is constant on a coset gV for some $g \in G$.

Proof. By way of contradiction, we assume that every subgroup V of G satisfying (i) and (ii) does not satisfy (iii), i.e. that φ is non-constant on all cosets of V in G.

Let α be the least ordinal such that $|\alpha| = \mathfrak{a}$.

We claim that for every ordinal $\lambda \leq \alpha$ and every map $\mathbf{i} \in \{1, 2\}^\lambda$ there exist a subgroup $V_\mathbf{i}$ of G and an element $g_\mathbf{i} \in G$ satisfying the following properties:

(P1) $V_\mathbf{i}$ is an intersection of subgroups of $\mathcal{N}$.

(P2) $w_0(G/V_{\mathbf{i}}) \leq |\lambda|$.

(P3) If $\mathbf{j} \in \{1,2\}^\lambda$ and $\mathbf{i} \neq \mathbf{j}$ then

$$(g_{\mathbf{i}}V_{\mathbf{i}})\varphi \cap (g_{\mathbf{j}}V_{\mathbf{j}})\varphi = \varnothing \tag{18}$$

(P4) If $\lambda' < \lambda$ and $\mathbf{i}'$ is the restriction of $\mathbf{i}$ to λ' then $g_{\mathbf{i}}G_{\mathbf{i}} \subseteq g_{\mathbf{i}'}G_{\mathbf{i}'}$ (and consequently $G_{\mathbf{i}} \leq G_{\mathbf{i}'}$).

In the case $\lambda = \alpha$, by taking into account that there are $2^{\mathfrak{a}}$ maps in $\{1,2\}^\alpha$, it follows from (18) that $|G\varphi| \geq 2^{\mathfrak{a}}$. This yields the desired contradiction.

We prove the claim in the previous paragraph by transfinite induction on λ. If $\lambda = 0$ there is nothing to prove, so let us assume that $\lambda \geq 1$.

Suppose first that the ordinal λ is a successor, say $\lambda = \lambda' + 1$. By the induction hypothesis, for every $\mathbf{i}' \in \{1,2\}^{\lambda'}$ there exist a subgroup $V_{\mathbf{i}'}$ of G and an element $g_{\mathbf{i}'} \in G$ such that (P1) through (P4) hold. Let us write $\mathbf{i_1}, \mathbf{i_2} \in \{1,2\}^\lambda$ for the extensions of $\mathbf{i}'$ to λ given by $\mathbf{i_1}(\lambda) = 1$ and $\mathbf{i_2}(\lambda) = 2$, and observe that all elements of $\{1,2\}^\lambda$ appear in this way. Now we apply Lemma 2.22 to the map $\varphi_{\mathbf{i}'} : V_{\mathbf{i}'} \to Y$ given by $v_{\mathbf{i}'}\varphi_{\mathbf{i}'} = (g_{\mathbf{i}'}v_{\mathbf{i}'})\varphi$ for all $v_{\mathbf{i}'} \in V_{\mathbf{i}'}$, together with the following basis of neighborhoods of the identity of $V_{\mathbf{i}'}$:

$$\mathcal{N}_{\mathbf{i}'} = \{U \cap V_{\mathbf{i}'} \mid U \in \mathcal{N}\}.$$

Observe that $\varphi_{\mathbf{i}'}$ is not constant by our standing assumption, since $V_{\mathbf{i}'}$ satisfies (P1) and (P2). Here we use that $\lambda' < \lambda \leq \alpha$ and so by (P2) we have $w_0(G/V_{\mathbf{i}'}) \leq |\lambda'| < \mathfrak{a}$. Then there exist two elements $v_1, v_2 \in V_{\mathbf{i}'}$ and two subgroups $V_{\mathbf{i_1}}, V_{\mathbf{i_2}} \in \mathcal{N}_{\mathbf{i}'}$ such that $(v_1V_{\mathbf{i_1}})\varphi_{\mathbf{i}'} \cap (v_2V_{\mathbf{i_2}})\varphi_{\mathbf{i}'} = \varnothing$ or, what is the same, such that

$$(g_{\mathbf{i}'}v_1V_{\mathbf{i_1}})\varphi \cap (g_{\mathbf{i}'}v_2V_{\mathbf{i_2}})\varphi = \varnothing. \tag{19}$$

If we set $g_{\mathbf{i_1}} = g_{\mathbf{i}'}v_1$ and $g_{\mathbf{i_2}} = g_{\mathbf{i}'}v_2$ then it is clear from (19) and from the induction hypothesis that the collection of subgroups $\{V_{\mathbf{i_1}}, V_{\mathbf{i_2}} \mid \mathbf{i} \in \{1,2\}^{\lambda'}\}$ and elements $\{g_{\mathbf{i_1}}, g_{\mathbf{i_2}} \mid \mathbf{i} \in \{1,2\}^{\lambda'}\}$ satisfy (P1) through (P4) for the ordinal λ. Simply note that (P2) can be proved, for example for $V_{\mathbf{i_1}}$, as follows: since $V_{\mathbf{i_1}}$ is open in $V_{\mathbf{i}'}$ then $w_0(V_{\mathbf{i}'}/V_{\mathbf{i_1}})$ is finite so

$$w_0(G/V_{\mathbf{i_1}}) = w_0(G/V_{\mathbf{i}'}) + w_0(V_{\mathbf{i}'}/V_{\mathbf{i_1}}) \leq |\lambda'| + 1 \leq |\lambda|.$$

Now we assume that λ is a limit ordinal. Let $\mathbf{i} \in \{1,2\}^\lambda$ be arbitrary, and for every ordinal $\mu < \lambda$, let $\mathbf{i}_\mu$ be the restriction of $\mathbf{i}$ to μ. We define

$$V_{\mathbf{i}} = \bigcap_{\mu<\lambda} V_{\mathbf{i}_\mu},$$

which is a closed normal subgroup of G and satisfies (P1). From the induction hypothesis and condition (P4) we obtain that $\{V_{\mathbf{i}_\mu}\}_{\mu<\lambda}$ is a chain. Hence we can apply Lemma 2.21 to the factor group $G/V_{\mathbf{i}}$, and we get $w_0(G/V_{\mathbf{i}}) \leq |\lambda|$. Thus $V_{\mathbf{i}}$ satisfies (P2). Also the family $\{g_{\mathbf{i}_\mu}V_{\mathbf{i}_\mu}\}_{\mu<\lambda}$ has the finite intersection property by (P4). Since G is compact, we get

$$\bigcap_{\mu<\lambda} g_{\mathbf{i}_\mu}V_{\mathbf{i}_\mu} \neq \varnothing.$$

Let $g_{\mathbf{i}}$ be an element in this intersection. Then $g_{\mathbf{i}_\mu}V_{\mathbf{i}_\mu} = g_{\mathbf{i}}V_{\mathbf{i}_\mu}$ for every $\mu < \lambda$, and consequently

$$\bigcap_{\mu<\lambda} g_{\mathbf{i}_\mu}V_{\mathbf{i}_\mu} = \bigcap_{\mu<\lambda} g_{\mathbf{i}}V_{\mathbf{i}_\mu} = g_{\mathbf{i}}\left(\bigcap_{\mu<\lambda} V_{\mathbf{i}_\mu}\right) = g_{\mathbf{i}}V_{\mathbf{i}}.$$

It is now clear that (P4) holds. Finally, suppose that $\mathbf{i} \neq \mathbf{j}$ belong to $\{1,2\}^\lambda$. Since λ is a limit ordinal, we have $\lambda = \bigcup_{\mu<\lambda} \mu$. Hence we necessarily have $\mathbf{i}_\mu \neq \mathbf{j}_\mu$ for some $\mu < \lambda$, and by (P3) applied to μ,

$$(g_{\mathbf{i}_\mu}V_{\mathbf{i}_\mu})\varphi \cap (g_{\mathbf{j}_\mu}V_{\mathbf{j}_\mu})\varphi = \varnothing.$$

Since $g_{\mathbf{i}}V_{\mathbf{i}} \subseteq g_{\mathbf{i}_\mu}V_{\mathbf{i}_\mu}$ and $g_{\mathbf{j}}V_{\mathbf{j}} \subseteq g_{\mathbf{j}_\mu}V_{\mathbf{j}_\mu}$, we also have

$$(g_{\mathbf{i}}V_{\mathbf{i}})\varphi \cap (g_{\mathbf{j}}V_{\mathbf{j}})\varphi = \varnothing.$$

This proves (P3) in this case and completes the proof. □

From now on we will write $G^{(r)}$ instead of $G\times\overset{r}{\cdots}\times G$, and $\mathbf{g} = (g_1, ..., g_r)$ for the elements in $G^{(r)}$. We would also like to recall that the direct product of profinite groups is again a profinite group.

Corollary 2.24. Let $\varphi : G^{(r)} \to Y$ be a continuous map, where G is a profinite group, $r \in \mathbb{N}$, and Y is a Hausdorff topological space. If $|G^{(r)}\varphi| < 2^{\mathfrak{a}}$ for an infinite cardinal $\mathfrak{a}$, then there exist $V \trianglelefteq_{\mathrm{c}} G$ and $\mathbf{g} \in G^{(r)}$ such that $w_0(G/V) < \mathfrak{a}$ and φ is constant on the coset $\mathbf{g}V^{(r)}$.

Proof. Apply Lemma 2.23 with $G^{(r)}$ in the place of G, and with the basis of neighborhoods of the identity of $G^{(r)}$ given by

$$\mathcal{N} = \{U^{(r)} \mid U \trianglelefteq_{\mathrm{o}} G\}.$$

To conclude, simply observe that an intersection of subgroups in $\mathcal{N}$ is of the form $V^{(r)}$ with $V \trianglelefteq_{\mathrm{c}} G$. □

3 Words in profinite groups

In this chapter, we will introduce the concept of group words and prove some results regarding words in profinite groups.

3.1 Free groups, words, verbal subgroups and multilinear commutators

We start this section by giving the definition of a free group.

Definition 3.1. Let F be a group, X a non-empty set and $\sigma : X \to F$ a function. Then F, or more precisely (F, σ), is a a free group on X if for each map $f : X \to G$ there exists a unique homomorphism $\widetilde{f} : F \to G$ such that $f = \sigma\widetilde{f}$. This can be symbolized by the commutative diagram below:

$$\begin{array}{ccc} X & \xrightarrow{\forall f} & G \\ {\scriptstyle\sigma}\downarrow & \nearrow_{\exists!\,\widetilde{f}} & \\ F & & \end{array}$$

Note that $\sigma : X \to F$ is injective. Indeed, let us assume, for the sake of contradiction, that $x_1\sigma = x_2\sigma$ and $x_1 \neq x_2$. Let G be any group with at least two different elements g_1, g_2 and let f be a function that sends $x_1 \mapsto g_1$ and $x_2 \mapsto g_2$. Then $x_1 f \neq x_2 f$ while $x_1\sigma\widetilde{f} = x_2\sigma\widetilde{f}$ which is a contradiction.

Proposition 3.2. For each set X there exists a unique free group (F, σ) on X.

Proof. We start by proving that if (F, σ) is a free group on X, then it is unique up to unique isomorphism. Suppose that (F, σ) and (F', σ') are free groups on X. By definition we have the following commutative diagram:

$$\begin{array}{ccccc} & & X & & \\ & {\scriptstyle\sigma}\swarrow & \downarrow{\scriptstyle\sigma'} & \searrow{\scriptstyle\sigma} & \\ F & \xrightarrow[\alpha]{} & F' & \xrightarrow[\beta]{} & F \end{array}$$

where α is the unique homomorphism from F to F' satisfying $\sigma' = \sigma\alpha$ and β is the unique homomorphism from F' to F satisfying $\sigma = \sigma'\beta$. Moreover, again by definition there exists a unique homomorphism, let us call it γ, from F to F satisfying $\sigma = \sigma\gamma$. Clearly γ has to be the identity map in F. Since $\alpha\beta$ is a homomorphism satisfying $\sigma = \sigma\alpha\beta$ we deduce that $\alpha\beta = \mathrm{id}_F$. Using the same reasoning we prove that $\beta\alpha = \mathrm{id}_{F'}$. So indeed there exists

a unique isomorphism from F to F', namely α.

Next we prove the existence of a free group on X. Let X^{-1} be a disjoint copy of the set X. For notation purposes we will denote it as $X^{-1} = \{x^{-1} : x \in X\}$, where x^{-1} is just a symbol. We define a *word* w in X to be a finite string of symbols from $X \cup X^{-1}$. In other words,

$$w = x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n}$$

where $x_i \in X$ and $\varepsilon_i = \pm 1$ for all $i \in \{1, ..., n\}$ and $n \geq 0$, is a word in X. If $n = 0$ we say that w is the *empty word* and we write $w = 1$. Let $w_1 = x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n}$ and $w_2 = y_1^{\eta_1} \cdots y_m^{\eta_m}$ be two words in X, then we say that $w_1 = w_2$ if and only if $m = n$, $x_i = y_i$ and $\varepsilon_i = \eta_i$ for all $i \in \{1, ..., n\}$. We define the product of two words in X to be the concatenation, this is,

$$w_1 w_2 = x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n} y_1^{\eta_1} \cdots y_m^{\eta_m},$$

with the convention that $1w = w = w1$. The inverse of a word is

$$w^{-1} = (x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n})^{-1} = x_1^{-\varepsilon_1} \cdots x_n^{-\varepsilon_n}.$$

Let $\widetilde{F}$ be the set of all words in X. We define the following equivalence relation in $\widetilde{F}$: we say that two words w_1 and w_2 are equivalent in $\widetilde{F}$, and we write $w_1 \sim w_2$ if it is possible to pass from w_1 to w_2 by a finite sequence of the following operations:

1. Inserting xx^{-1} or $x^{-1}x$ at any point in the word, where $x \in X$;
2. deleting xx^{-1} or $x^{-1}x$ at any point in the word.

Clearly $\sim$ is an equivalence relation. We define F to be $\widetilde{F}/\sim$. We want to make F into a group. First of all note that if $w_1 \sim w_2$ and $v_1 \sim v_2$, then $w_1 v_1 \sim w_2 v_2$. So if we define $[w]$ to be the equivalence class of w, then an operation can be defined in F as

$$[w][v] = [wv]. \tag{20}$$

Moreover, $[w][1] = [w] = [1][w]$ and $[w][w^{-1}] = [ww^{-1}] = [1]$. It is clear that the product of elements in F is associative, since the product of elements in $\widetilde{F}$ is associative. So it follows that F is a group with the binary operation defined in (20), that $[1]$ is the identity element and that $[w^{-1}]$ is the inverse of $[w]$.

We define the function $\sigma : X \longrightarrow F$ by $x\sigma \mapsto [x]$, so it just remains to show that indeed (F, σ) is the free group on X. Let G be a group and $f : X \to G$ a function. We define a map from the set of all words in X to G as follows

$$\begin{aligned} f^{\#} : \widetilde{F} &\longrightarrow G \\ w = x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n} &\longmapsto (x_1 f)^{\varepsilon_1} \cdots (x_n f)^{\varepsilon_n}. \end{aligned}$$

Note that if $w \sim v$ then $wf^{\#} = vf^{\#}$, because in G, the elements gg^{-1} and $g^{-1}g$ equal the identity. So it makes sense to define

$$\begin{aligned} \widetilde{f} : F &\longrightarrow G \\ [w] &\longmapsto wf^{\#}. \end{aligned}$$

Moreover, $\widetilde{f}$ is a group homomorphism because

$$[wv]\widetilde{f} = (wv)f^{\#} = wf^{\#}vf^{\#} = [w]\widetilde{f}[v]\widetilde{f}$$

and it satisfies $x\sigma\widetilde{f} = [x]\widetilde{f} = xf^{\#} = xf$. So, indeed, $f = \sigma\widetilde{f}$. □

Now that we are familiarized with the definition of free group and word we will explain what is the value of a word in a group. Let F be a free group on a countably infinite set $\{x_1, x_2, ...\}$ and let G be any group. Assume that $w = x_1^{\varepsilon_1} \cdots x_r^{\varepsilon_r}$ is a word in F. Then, for a tuple $(g_1, ..., g_r)$ of elements in G we define the value of w at $(g_1, ..., g_r)$ (or simply the w-value of $(g_1, ..., g_r)$) to be

$$w(g_1, ..., g_r) = g_1^{\varepsilon_1} \cdots g_r^{\varepsilon_r} \in G.$$

We define the set of all w-values in a group G as

$$G_w = \{w(g_1, ..., g_r) : g_1, ..., g_r \in G\}.$$

Lemma 3.3. Let $w = x_1^{\varepsilon_1} \cdots x_r^{\varepsilon_r}$ be a word and let G be a profinite group. Then the map

$$\begin{aligned} w : G^{(r)} &\longrightarrow G \\ (g_1, ..., g_r) &\longrightarrow g_1^{\varepsilon_1} \cdots g_r^{\varepsilon_r} \end{aligned}$$

is continuous and closed. Moreover, $\mathrm{Im}(w) = G_w$.

Proof. For a topological group G, the maps defined by $(x, y) \mapsto xy$ and $x \mapsto x^{-1}$ are continuous. Hence, the map defined by w is continuous, since it is a finite composition of maps of the form $(x, y) \mapsto xy$ and $x \mapsto x^{-1}$.

On the other hand, every product of (arbitrarily many) profinite groups is profinite, so $G^{(r)}$ is profinite. Since a profinite group is both compact and Hausdorff and a continuous map from a compact space to a Hausdorff space is closed, it follows that the map above is closed. The fact that $\mathrm{Im}(w) = G_w$ is self-evident. □

We call *verbal subgroup* of G determined by w to the subgroup of G generated by G_w and we write it as $w(G)$. In other words, $w(G) = \langle G_w \rangle$.

We will now give some easy examples of w-values in a group and some verbal subgroups.

Example 3.4. Consider the word $w = [x_1, x_2] = x^{-1}x_2^{-1}x_1x_2 = x_1^{-1}x_1^{x_2}$. Then for any group G, we have that $G_w = \{[g_1, g_2] : g_1, g_2 \in G\}$ and $w(G) = G'$.
For the word $w = x^n$ we have that $G_w = \{g^n : g \in G\}$ and $w(G) = G^n$.

It is clear that G_w is always contained in $w(G)$, but in general they will not be equal.

For a word w in a free group generated by $\{x_1, x_2, ...\}$, we say that a normal subgroup N of G is w-marginal in G if

$$w(g_1, .., g_{i-1}, ag_i, g_{i+1}, ..., g_r) = w(g_1, .., g_{i-1}, g_i, g_{i+1}, ..., g_r)$$

for all $g_i \in G$, $a \in N$. Note that the w-marginal subgroups of G generate a normal subgroup which is still w-marginal. We call this subgroup the w-marginal subgroup of G and we write it as

$$w^*(G).$$

Now we will focus our attention on what are called multilinear commutators, sometimes also called outer commutators. Multilinear commutators are group words obtained by nesting commutators and using each variable only once. For example

$$[[x_1, x_2, x_3], [x_4, x_5], x_6]$$

is a multilinear commutator, while

$$[x, y, y]$$

is not. Since we will be working with commutators we would like to recall some useful properties that they satisfy.

Property 3.5. Let G be a group and suppose that N is a normal subgroup of G. For $x, y \in G$ we have that

(i) $xy = yx^y = y^{x^{-1}}x$;

(ii) $[x, y]^{-1} = [y, x]$;

(iii) $[xy, z] = [x, z]^y[y, z]$;

(iv) $[x, yz] = [x, z][x, y]^z$;

(v) if x or y belong to N, then $[x, y] \in N$.

Proof. For (i) it is enough to write down the calculations. (ii),(iii) and (iv) follow by the definition of commutator. To prove (v) note that

$$[x, y] = x^{-1}y^{-1}xy = (y^{-1})^x y = x^{-1}x^y.$$

Since N is normal it follows that if x or y belong to N, then $[x, y]$ also belongs to N. □

3.2 Conciseness and strong conciseness

Let w be a word, we say that w is *concise* in a class of groups $\mathcal{C}$, if for every G in $\mathcal{C}$, the fact that G_w is finite implies that $w(G)$ is also finite. Philip Hall conjectured in 1960 (for example, see [13]) that all words where concise in the class of all groups. This was later disproved by Ivanov in 1989 [5]. Although, it is still interesting to find classes of groups in which words are or are not concise. For example, it is known that words are concise in the class of linear groups, because of that one could also ask if words are concise in the class of residually finite groups or profinite groups.

In [2] Detomi, Morigi and Shumyatsky suggested a stronger version of Philip Hall's conjecture for the class of profinite groups. They theorized that for every word w and every profinite group G, if $|G_w| \leq \aleph_0$ then $w(G)$ is finite. Note that since we are working with profinite groups, the verbal subgroup $w(G)$ is the closure of the subgroup generated by G_w, not the abstract subgroup generated by G_w. Later in [1] Detomi, Klopsch and Shumyatsky introduced the following definition: a word w is *strongly concise* in the class of profinite groups if $|G_w| < 2^{\aleph_0}$ implies that $w(G)$ is finite. They conjectured that all words are strongly concise in the class of profinite groups.

In [1] Detomi, Klopsch and Shumyatsky proved that multilinear commutators words and words of the form $x^2, x^3, x^6, [x^3, y], [x, y, y]$ are strongly concise.

A natural question arises when paying attention to the definition of strong conciseness. Since the cardinal number of a profinite group is either finite or grater than or equal to $2^{\aleph_0}$, we have that if a profinite group has cardinality less than $2^{\aleph_0}$, then is finite. So for a profinite group G, it follows that $|w(G)| < 2^{\aleph_0}$ if and only if $w(G)$ is finite. Knowing this we can think about a generalization of the conjecture introduced by Detomi, Klopsch and Shumyatsky.

Conjeture 3.6. Let w be a group word, and suppose that G is any group in the class of profinite groups. Then, if $|G_w| < 2^{\mathfrak{a}}$ for some cardinal $\mathfrak{a}$, we have that $|w(G)| < 2^{\mathfrak{a}}$.

There are certainly some classes of groups that satisfy Conjeture 3.6. For example the class of abelian profinite groups.

Proposition 3.7 (See Proposition 2.3 in [1])**.** Let w be a group word and G an abelian profinite group. If $|G_w| < 2^{\mathfrak{a}}$ for some infinite cardinal number $\mathfrak{a}$, then $|w(G)| < 2^{\mathfrak{a}}$.

Proof. Let G be an abelian profinite group and let w be a group word in r variables. Since G is abelian we can write

$$w(g_1, ..., g_r) = g_1^{a_1} \cdots g_r^{a_r}, \qquad \text{where all } a_i \in \mathbb{Z},$$

for any $g_1, ..., g_r \in G$. Consider the following map:

$$\begin{aligned} f : G^{(r)} &\longrightarrow G \\ (g_1, ..., g_r) &\longmapsto g_1^{a_1} \cdots g_r^{a_r}. \end{aligned}$$

We have that f is a group homomorphism because G is abelian, hence, $\mathrm{Im}(f)$ is an abstract subgroup of G. Moreover, by Lemma 3.3 we know that $\mathrm{Im}(f)$ is closed in G. Thus, we have that $G_w = \mathrm{Im}(f) = \langle G_w \rangle = w(G)$. So indeed $|w(G)| < 2^{\mathfrak{a}}$.

□

3.3 Multilinear commutator words

In this final section we want to use all the tools that we have been developing in the thesis to prove some results regarding the cardinal number of

the set of word values G_w, the verbal subgroup $w(G)$ and the w-marginal subgroup $w^*(G)$ for a profinite group G and a multilinear commutator word w. Specifically we want to show that if w is a multilinear commutator word, and G is a profinite group, then either G_w is finite, and so $w(G)$ is also finite as it was proven in [14, Theorem 1], or $|G_w| = 2^{\mathfrak{a}}$ for some infinite cardinal $\mathfrak{a}$ and in that case $|w(G)| = |G_w|$. As we will see this is a consequences of Thoerem 3.8 below.
In this section, to avoid confusions with the verbal subgroup $w(G)$, we will use $\rho(G)$, the cardinality of the set of all clopen substsets of G, instead of $w_0(G)$, the cardinal number of any fundamental system of neighborhoods of 1 consisting of open subgroups of G. Because $\rho(G) = w_0(G)$ by Proposition 2.11.
Before we start, would like to mention that some results would be easier to prove or even trivially true if we assume the Generalized Continuum Hypothesis, but as we will see there is no need to assume this axiom.

The result that we want to prove, which will allow us to prove the main result of this thesis, is the following:

Theorem 3.8. Let w be a multilinear commutator word and let G be an infinite profinite group and suppose that $|G_w| < 2^{\mathfrak{a}}$, for some infinite cardinal number $\mathfrak{a}$. Then $\rho(G/w^*(G)) < \mathfrak{a}$, where $w^*(G)$ is the w-marginal subgroup of G.

The first step in the proof of Theorem 3.8 is to prove the theorem below.

Theorem 3.9. Let w be a multilinear commutator word. Suppose that $|G_w| < 2^{\mathfrak{a}}$, for some infinite cardinal number $\mathfrak{a}$. Then there exists some closed normal subgroup V of G with the property that $\rho(G/V) < \mathfrak{a}$ and $w(V) = 1$.

But first we need to introduce some notation and prove some results. We fix $r \in \mathbb{N}$ and the following multilinear commutator

$$w = w(x_1, ..., x_r).$$

Suppose that G is a profinite group and let $A_1, ..., A_r$ be a family of subsets of G. Then we write $\chi_w(A_1, ..., A_r)$ for the subset of G containing all the w-values $w(a_1, ..., a_r)$ where $a_i \in A_i$. Furthermore, we write $w(A_1, ..., A_r)$ for the subgroup generated by $\chi_w(A_1, ..., A_r)$, this is

$$w(A_1, ..., A_r) = \langle \chi_w(A_1, ..., A_r) \rangle = \langle w(a_1, ..., a_r) : a_1 \in A_1, ..., a_r \in A_r \rangle.$$

Moreover, let I be a subset of $\{1,..,r\}$ and $\overline{I} = \{1,..,r\} \setminus I$. Then, for the tuples $\boldsymbol{y} = (y_i)_{i\in I}$ and $\boldsymbol{z} = (z_i)_{i\in\overline{I}}$ we define

$$w_I(\boldsymbol{y},\boldsymbol{z}) = w(u_1,..,u_r) \quad \text{where} \quad u_i = \begin{cases} y_i & \text{if } i \in I, \\ z_i & \text{if } i \notin I. \end{cases}$$

We will write $w_I(y_i, z_i)$ instead of $w_I(\boldsymbol{y},\boldsymbol{z})$ for short. The notation can be extended to families $\boldsymbol{A} = (A_i)_{i\in I}$, $\boldsymbol{B} = (B_i)_{i\in\overline{I}}$ of subsets of G by setting

$$w_I(\boldsymbol{A},\boldsymbol{B}) = \langle w_I(y_i,z_i) : y_i \in A_i, z_i \in B_i\rangle.$$

Again, for short, we will write $w_I(A_i, B_i)$ instead of $w_I(\boldsymbol{A},\boldsymbol{B})$.

Lemma 3.10 (See [3], Lemma 2.4)**.** Let G be a group and suppose that $A_1, A_2, ..., A_r$ and H are normal subgroups of G. Let $a_i \in A_i$ and $h_i \in A_i \cap H$ for all $i = 1,..,r$. Let $j \in \{1,..,r\}$ and set $I = \{1,..,n\} \setminus \{j\}$. Then there exists an element

$$x \in \chi_w\left(a_1(A_1 \cap H), ..., a_r(A_r \cap H)\right)$$

such that

$$w(a_1h_1, ..., a_rh_r) = x\ w_I(a_ih_i, h_j). \tag{21}$$

Proof. We want to prove this by induction on r, the number of variables appearing in w. For $r = 1$ there is nothing to prove because a multilinear commutator word in one variable is just $w(x) = x$. So it follows that $w(a_1h_1) = a_1h_1 = a_1w(h_1)$, where $a_1 \in \chi_w(a_1(A_1 \cap H))$. So (21) holds for $r = 1$.

Now assume that $r \geq 2$. By the definition of multilinear commutator word, we have that w can be written as

$$w = [w_1, w_2]$$

where w_1, w_2 are both multilinear commutators. We can assume that w_1 has s variables and that w_2 has $r - s$ variables, where $s < r$. Let

$$y = w(a_1h_1, ..., a_rh_r) = [y_1, y_2],$$

where $y_1 = w_1(a_1h_1, ..., a_sh_s)$ and $y_2 = w_2(a_{s+1}h_{s+1}, ..., a_rh_r)$. Assuming that $j > s$ we just need to prove that

$$w(a_1h_1, ..., a_rh_r) = x\,[y_1, w_2(a_{s+1}h_{s+1}, ..., a_{j-1}h_{j-1}, h_j, a_{j+1}h_{j+1}, ..., a_rh_r)]$$

where $x \in \chi_w\left(a_1(A_1 \cap H), ..., a_r(A_r \cap H)\right)$.

By induction hypothesis, since $r - s < r$, we have that $y_2 = xh$, where $x \in \chi_{w_2}\left(a_{s+1}(A_{s+1} \cap H), ..., a_r(A_r \cap H)\right)$ and

$$h = w_2(a_{s+1}h_{s+1}, ..., a_{j-1}h_{j-1}, h_j, a_{j+1}h_{j+1}, ..., a_r h_r) \in H.$$

Note that by Property 3.5.(i) and 3.5.(iv) we have that

$$y = [y_1, y_2] = [y_1, xh] = [y_1, h][y_1, x]^h = [y_1, x]^{h[y_1,h]^{-1}}[y_1, h]$$

so we just need to prove that $[y_1, x]^{h[y_1,h]^{-1}}$ belongs to $\chi_w\left(a_1(A_1 \cap H), ..., a_r(A_r \cap H)\right)$.

We write $\widetilde{h} = h[y_1, h]^{-1} = h^{y_1} \in H$, so for any $a_i \in A_i$, it follows from Property 3.5.(v) that $[a_i, \widetilde{h}] \in A_i \cap H$. Now, note that for $\widetilde{h_i} \in A_i \cap H$ and $i \in 1, ..., r$

$$(a_i\widetilde{h_i})^{\widetilde{h}} = a_i^{\widetilde{h}}\widetilde{h_i}^{\widetilde{h}} = a_i a_i^{-1}a_i^{\widetilde{h}}\widetilde{h_i}^{\widetilde{h}} = a_i a_i^{-1}\widetilde{h}^{-1}a_i\widetilde{h}\widetilde{h_i}^{\widetilde{h}} = a_i[a_i, \widetilde{h}]\widetilde{h_i}^{\widetilde{h}}. \tag{22}$$

So $(a_i\widetilde{h_i})^{\widetilde{h}} \in a_i(A_i \cap H)$ for all $\widetilde{h_i} \in A_i \cap H$ and $i \in 1, ..., r$.

Since $x \in \chi_{w_2}\left(a_{s+1}(A_{s+1} \cap H), ..., a_r(A_r \cap H)\right)$ we have that

$$x = w_2(a_{s+1}\widetilde{h}_{s+1}, ..., a_r\widetilde{h}_r)$$

for some $\widetilde{h_i} \in A_i \cap H$. So

$$\begin{aligned}
[y_1, x]^{\widetilde{h}} =& [w_1(a_1h_1, ..., a_sh_s), w_2(a_{s+1}\widetilde{h}_{s+1}, ..., a_r\widetilde{h}_r)]^{\widetilde{h}} \\
=& w(a_1h_1, ..., a_sh_s, a_{s+1}\widetilde{h}_{s+1}, ..., a_r\widetilde{h}_r)^{\widetilde{h}} \\
=& w\left((a_1h_1)^{\widetilde{h}}, ..., (a_sh_s)^{\widetilde{h}}, (a_{s+1}\widetilde{h}_{s+1})^{\widetilde{h}}, ..., (a_r\widetilde{h}_r)^{\widetilde{h}}\right)
\end{aligned} \tag{23}$$

is an element of $\chi_w\left(a_1(A_1 \cap H), ..., a_r(A_r \cap H)\right)$. Recall that in (22) we have proven the equality $(a_ih_i)^{\widetilde{h}} = a_i[a_i, \widetilde{h}]h_i^{\widetilde{h}} \in a_i(A_i \cap H)$.

Now suppose that $1 \leq j \leq s$. As before we have that by induction $y_1 = xh$ where

$$h = w_1(a_1h_1, ..., a_{j-1}h_{j-1}, h_j, a_{j+1}h_{j+1}, ..., a_sh_s)$$

and $x \in \chi_{w_1}(a_1(A_1 \cap H), ..., a_s(A_s \cap H))$. Note that similarly to the case above using Property 3.5.(iii)

$$y = [y_1, y_2] = [xh, y_2] = [x, y_2]^h[h, y_2].$$

So it just remains to prove that $[x, y_2]^h$ belongs to $\chi_{w_1}(a_1(A_1 \cap H), ..., a_r(A_r \cap H))$. Since $h \in H$ and $a_i \in A_i$ reasoning as in (22), we have that $(a_i \widetilde{h}_i)^h \in a_i(A_i \cap H)$. Finally as we saw in (23), we have that $[x, y_2]^h$ is an element of $\chi_w(a_1(A_1 \cap H), ..., a_r(A_r \cap H))$. □

Lemma 3.11 (See [3], Lemma 2.5)**.** Let G be a group and suppose that $A_1, A_2, ..., A_r$ and H are normal subgroups of G. Let V be a subgroup of G and $g \in G$. Assume that for some $a_i \in A_i$

$$\chi_w\left(a_1(A_1 \cap H), ..., a_r(A_r \cap H)\right) \subseteq gV.$$

Let I be a proper subset of $\{1, .., r\}$. Then

$$w_I(a_i(A_i \cap H); A_l \cap H) \leq V.$$

Proof. We will prove this by induction on $r - |I|$. So first consider $I = \{1, .., r\} \setminus \{j\}$ for some $j \in \{1, .., r\}$ and set $H_i = A_i \cap H$, for $i = 1, ..., r$. Consider the w-value $w(g_1, ..., g_r)$, where $g_i \in a_i H_i$ if $i \neq j$, and $g_j \in H_j$. Then by Lemma 3.10 there exists an element

$$x \in \chi_w(a_1 H_1, ..., a_r H_r)$$

such that

$$w(g_1, .., g_{j-1}, a_j g_j, g_{j+1}, ..., g_r) = x w(g_1, ..., g_r).$$

Note that

$$x, w(g_1, .., g_{j-1}, a_j g_j, g_{j+1}, ..., g_n) \in \chi_w(a_1 H_1, ..., a_r H_r)$$

and by hypothesis $\chi_w(a_1 H_1, ..., a_r H_r) \leq gV$. So it follows that $w(g_1, ..., g_r) \in V$, and since V is a subgroup of G, we have that the subgroup generated by all such words $w(g_1, ..., g_r)$, namely $w_I(a_i H_i; H_i)$, belongs to V. So we have that the lemma holds for $|I| = r - 1$.

Assume that $|I| \leq r - 2$, and set $I^* = I \cup \{j\}$ for some $j \notin I$. Consider $w(g_1, ..., g_r)$ where $g_i \in a_i H_i$ for every $i \in I$ and $g_i \in H_i$ for every $i \notin I$. Note that

$$w(g_1, ..., g_{j-1}, a_j g_j, g_{j+1}, ..., g_r) \in w_{I^*}(a_i H_i, H_i).$$

By Lemma 3.10 we have that there exists

$$x \in \chi_w(g_1 H_1, ..., g_{j-1} H_{j-1}, a_j H_j, g_{j+1} H_{j+1}, ..., g_r H_r)$$

such that

$$w(g_1, ..., g_{j-1}, a_j g_j, g_{j+1}, ..., g_r) = xw(g_1, ..., g_r).$$

Is clear that x belongs to $w_{I^*}(a_i H_i; H_i)$, and by induction hypothesis $w_{I^*}(a_i H_i; H_i) \leq V$. So it follows that $w(g_1, ..., g_r) \in V$, and again, using that V is a subgroup, we have that

$$w_I(a_i H_i; H_i) \leq V.$$

□

By replacing all A_i by G and taking $V = 1$ on Lemma 3.11 we deduce the corollary below which allows us to prove Theorem 3.9.

Corollary 3.12 (See [1], Corollary 3.1)**.** Let G be a group and assume that H is a normal subgroup of G. Suppose that $g_1, ..., g_r \in G$ and $g \in G$ satisfy $w(g_1 h_1, ..., g_r h_r) = g$ for all $h_1, .., h_r \in H$. Then $w_I(g_i H; H) = 1$ for any proper proper subset $I \subsetneq \{1, ..., r\}$.

Proof of Theorem 3.9. Consider the following map given by w

$$\begin{aligned} \varphi_w : G^{(r)} &\longrightarrow G \\ (g_1, ..., g_r) &\longmapsto w(g_1, ..., g_r). \end{aligned}$$

Note that $|G_w| = |\left(G^{(r)}\right)\varphi_w| < 2^{\mathfrak{a}}$, so by Corollary 2.24 we have that there exist $V \trianglelefteq_{\mathrm{c}} G$ and $\mathbf{g} \in G^{(r)}$ such that $\rho(G/V) < \mathfrak{a}$ and φ_w is constant on the coset $\mathbf{g}V^{(r)}$. In other words, there exist $\mathbf{g} = (g_1, ..., g_r) \in G^{(r)}$ and $g \in G$ such that

$$w(g_1 v_1, ..., g_r v_r) = g$$

for all $\mathbf{v} = (v_1, ..., v_r) \in V^{(r)}$. By Corollary 3.12 taking $I = \emptyset \subsetneq \{1, ..., r\}$ we conclude that

$$w_\emptyset(g_i V; V) = w(V) = 1.$$

□

The next step for the proof of Theorem 3.8 is to prove the following lemma, which generalizes [1, Lemma 3.3].

Lemma 3.13. Let G be an infinite profinite group and assume that $|G_w| < 2^{\mathfrak{a}}$ for some cardinal number $\mathfrak{a}$. If there exist a closed normal subgroup H of G with the property that $\rho(G/H) < \mathfrak{a}$ and a set $I \subsetneq \{1, ..., r\}$ such that

$$w_J(G; H) = 1 \quad \text{for all } J \subsetneq I.$$

Then for an arbitrary family $(g_i)_{i\in I}$ of elements in G there exists $V \trianglelefteq_c G$, contained in H, satisfying $\rho(G/V) < \mathfrak{a}$, such that

$$w_I(g_i; V) = 1.$$

The proof of Lemma 3.13 requires some preliminary results:

Lemma 3.14 (See [2], Lemma 2.4)**.** Let G be a group and suppose that H is a normal subgroup of G. Let $g_1, ..., g_n$ be some elements in G, h an element of H and fix $j \in \{1, ..., r\}$. Then for every $i \in \{1, ..., r\}$ there exists $y_i \in g_i^H$ such that

$$\begin{aligned} w(g_1, ..., g_{j-1}, g_j h, g_{j+1}, ..., g_r) \\ = w(y_1, ..., y_r) w(g_1, ..., g_{j-1}, h, g_{j+1}, ..., g_r). \end{aligned} \tag{24}$$

Proof. We want to prove this lemma by induction on r the number of variables appearing in w. For $r = 1$ is clear that $w(x) = x$ since w is a multilinear commutator word, so it follows that

$$w(gh) = gh = w(g)w(h).$$

Note that $g \in g^H$.

Assume $r \geq 2$, then we can write $w = [w_1, w_2]$ where w_1 and w_2 are two multilinear commutator words. Suppose that the number of variables appearing in w_1 is l and that $j \leq l$. Then we have by induction hypothesis that

$$w_1(g_1, ..., g_{j-1}, g_j h, g_{j+1}, ..., g_l) = w_1(y_1, ..., y_l) w_1(g_1, ..., g_{j-1}, h, g_{j+1}, ..., g_l).$$

Set $\overline{h} = w_1(g_1, ..., g_{j-1}, h, g_{j+1}, ..., g_l)$ and note that by Property 3.5.(v) $\overline{h} \in H$.

Using some commutator properties we have that

$$\begin{aligned} w(g_1, ..., g_{j-1}, g_j h, g_{j+1}, ..., g_r) \\ &= [w_1(g_1, ..., g_{j-1}, g_j h, g_{j+1}, ..., g_l), w_2(g_{l+1}, .., g_r)] \\ &= [w_1(y_1, ..., y_l)\overline{h}, w_2(g_{l+1}, .., g_r)] \\ &= [w_1(y_1, ..., y_l), w_2(g_{l+1}, .., g_r)]^{\overline{h}} [\overline{h}, w_2(g_{l+1}, .., g_r)] \\ &= [w_1(y_1^{\overline{h}}, ..., y_l^{\overline{h}}), w_2(g_{l+1}^{\overline{h}}, .., g_r^{\overline{h}})][\overline{h}, w_2(g_{l+1}, .., g_r)]. \end{aligned}$$

Since $y_i^{\overline{h}} \in g_i^H$ for all $i = 1, ..., l$ and $g_i^{\overline{h}} \in g_i^H$ for all $i = l+1, ..., r$ we see that (24) holds.

Now suppose that $l < j$. By induction hypothesis we have that

$$\begin{aligned} w_2(g_{l+1},...,g_{j-1},&g_jh,g_{j+1},...,g_r) \\ &=w_2(y_{l+1},...,y_r)w_2(g_{l+1},...,g_{j-1},h,g_{j+1},...,g_r). \end{aligned}$$

As before we write $\overline{h} = w_2(g_{l+1},...,g_{j-1},h,g_{j+1},...,g_r) \in H$. Using commutator properties we deduce that

$$\begin{aligned} w(g_1,...,g_{j-1},&g_jh,g_{j+1},...,g_r) \\ &=[w_1(g_1,...,g_l),w_2(g_{l+1},...,g_{j-1},g_jh,g_{j+1},...,g_r)] \\ &=[w_1(g_1,...,g_l),w_2(y_{l+1},...,y_r)\overline{h}] \\ &=[w_1(g_1,...,g_l),\overline{h}][w_1(g_1,...,g_l),w_2(y_{l+1},...,y_r)]^{\overline{h}} \\ &=[w_1(g_1,...,g_l),w_2(y_{l+1},...,y_r)]^{\overline{h}[w_1(g_1,...,g_l),\overline{h}]^{-1}}[w_1(g_1,...,g_l),\overline{h}]. \end{aligned}$$

Note that $\widetilde{h} = \overline{h}[w_1(g_1,...,g_l),\overline{h}]^{-1}$ belongs to H, so as before we have that

$$\begin{aligned} w(g_1,...,g_{j-1},&g_jh,g_{j+1},...,g_r) \\ &=[w_1(g_1,...,g_l),w_2(y_{l+1},...,y_r)]^{\widetilde{h}}[w_1(g_1,...,g_l),\overline{h}] \\ &=[w_1(g_1^{\widetilde{h}},...,g_l^{\widetilde{h}}),w_2(y_{l+1}^{\widetilde{h}},...,y_r^{\widetilde{h}})][w_1(g_1,...,g_l),\overline{h}] \end{aligned}$$

where $g_i^{\widetilde{h}} \in g_i^H$ for all $i = 1,...,l$ and $y_i^{\widetilde{h}} \in g_i^H$ for all $i = l+1,...,r$. So we see that (24) holds. □

Lemma 3.15 (See [2], Lemma 4.1)**.** Let G be a group and suppose that $A_1, A_2, ..., A_r$ and H are normal subgroups of G. Let I be a subset of $\{1,..,r\}$ and assume that for any proper subset J of I

$$w_J(A_i; A_l \cap H) = 1.$$

Then for any set of elements $g_i \in A_i$ with $i \in I$ and $h_k \in A_k \cap H$ with $k \in \{1,..,r\}$ we have that

$$w_I(g_ih_i; h_l) = w_I(g_i; h_l).$$

Proof. We write

$$\overline{w} = w_I(g_ih_i; h_l) = w(c_1,...,c_r)$$

where $c_i = g_ih_i$ if $i \in I$ and $c_i = h_i$ if $i \notin I$. Now fix $j \in I$, and consider $J = I \setminus \{j\}$. We write

$$g_jh_j = \overline{h}g_j \quad \text{where } \overline{h} = h_j^{g_j^{-1}}.$$

By Lemma 3.14 we have that

$$w(c_1, ..., c_{j-1}, \overline{h}g_j, c_{j+1}, ..., c_r) = w(y_1, ..., y_r)w(c_1, ..., c_{j-1}, g_j, c_{j+1}, ..., c_r)$$

where $y_i \in c_i^H = (g_i h_i)^H \subseteq A_i$ for $i \in J$, $y_i \in c_i^H = h_i^H \subseteq A_i \cap H$ for $i \notin I$ and $y_j \in \overline{h}^H \subseteq A_j \cap H$. Note that

$$w(y_1, ..., y_r) \in w_J(A_i; A_l \cap H)$$

which implies that $w(y_1, ..., y_r) = 1$, since $w_J(A_i; A_l \cap H) = 1$ by hypothesis. So we have that

$$w(c_1, ..., c_{j-1}, \overline{h}g_j, c_{j+1}, ..., c_r) = w(c_1, ..., c_{j-1}, g_j, c_{j+1}, ..., c_r).$$

We end the proof by repeating the same argument for all $s \in I$. □

By replacing all A_i by G in Lemma 3.15 we get the corollary below which is needed to prove Lemma 3.13.

Corollary 3.16 (See [1], Corollary 3.2)**.** Let G be a group and assume that H is a normal subgroup of G. If $I \subseteq \{1, ..., r\}$ is such that $w_J(G; H) = 1$ for all $J \subsetneq I$, then $w_I(g_i h_i; h_i) = w_I(g_i; h_i)$ for all $g_i \in G$, and all $h_1, .., h_r \in H$.

Proof of Lemma 3.13. Consider the continuous map

$$\begin{aligned} \psi : H^{(r)} &\longrightarrow G \\ (h_1, ..., h_r) &\longmapsto w_I(g_i h_i; h_i). \end{aligned}$$

The image of ψ is clearly a subset of G_w, hence $|H^{(r)}\psi| < 2^{\mathfrak{a}}$. Corollary 2.24 yields some closed normal subgroup V of G, contained in H and some $\mathbf{b} = (b_1, .., b_r) \in H^{(r)}$ such that $\rho(H/V) < \mathfrak{a}$ and ψ is constant on the coset $\mathbf{b}V^{(r)}$. So we have that

$$w_I(g_i b_i v_i; b_i v_i) = w_I(g_i b_i; b_i) \quad \text{for all } v_1, ..., v_r \in V.$$

Note that $g_i b_i$, b_i and $w_I(g_i b_i; b_i)$ belong to G, and I is a proper subset of $\{1, ..., r\}$. Hence, it follows from Corollary 3.12 that

$$w_I(g_i b_i V; V) = 1. \tag{25}$$

Note that $b_i V$ is contained in H for all $i \in I$. Moreover, by hypothesis we have that $w_J(G; H) = 1$ for all proper subsets $J \subsetneq I$ so by Corollary 3.16 it follows that

$$w_I(g_i b_i V; V) = w_I(g_i; V). \tag{26}$$

Combining (25) and (26) we deduce that that

$$w_I(g_i; V) = w_I(g_i b_i V; V) = 1.$$

We use Corollary 2.17 to conclude that

$$\rho(G/V) \leq \rho(G/H) + \rho(H/V) < \mathfrak{a} + \mathfrak{a} = \mathfrak{a}.$$

□

The next two lemmas are the final step for the proof of Theorem 3.8.

Lemma 3.17. Let G be an abstract group and assume that R is a generating set of G. If R is an infinite set, then $|G| = |R|$.

Proof. Note that every element of the group G can be expressed as a combination (under the group operation) of finitely many elements of the set R and their inverses. Consider the set $R^{-1} = \{x^{-1} : x \in R\}$, then any element in G can be expressed as a combination of finitely many elements of the set $R \cup R^{-1}$. For each $n \geq 1$ we write $(R \cup R^{-1})^{[n]} = \{x_1 \cdots x_n : x_i \in R \cup R^{-1}\}$. Note that for any $n \in \mathbb{Z}_{\geq 1}$

$$|(R \cup R^{-1})^{[n]}| \leq |R \cup R^{-1}|^n = (2|R|)^n = |R|$$

since $|R|$ is an infinite cardinal. On the other hand, is clear that

$$G = \bigcup_{n \in \mathbb{Z}_{\geq 1}} (R \cup R^{-1})^{[n]}.$$

Hence, we deduce that

$$|G| = \left| \bigcup_{n \in \mathbb{Z}_{\geq 1}} (R \cup R^{-1})^{[n]} \right| \leq \sum_{n \in \mathbb{Z}_{\geq 1}} \left|(R \cup R^{-1})^{[n]}\right| \leq \sum_{n \in \mathbb{Z}_{\geq 1}} |R| = \aleph_0 |R| = |R|.$$

□

Lemma 3.18. Let R be a subset of a profinite group G and let $\widetilde{R}$ be the abstract subgroup generated by R. Let $I \subsetneq \{1, ..., r\}$ and $V \trianglelefteq_c G$. Assume that

$$w_I(g_i; V) = 1 \qquad \text{for all families } \mathbf{g} = (g_i)_{i \in I} \in \widetilde{R}^{(r)}.$$

Then

$$w_I(g_i; V) = 1 \qquad \text{for all families } \mathbf{g} = (g_i)_{i \in I} \in \langle R \rangle^{(r)}.$$

Note that $\langle R \rangle$ is the profinite subgroup of G generated by R.

Proof. Let N be a normal open subgroup of G. Then for every $g_i \in \langle R \rangle$ we can write $g_i N$ as a finite product of cosets of elements of R. Thus, for every $g_i \in \langle R \rangle$ there exists $h_i \in \widetilde{R}$ such that $g_i N = h_i N$. Thus

$$w_I(g_i; V)N = w_I(g_i N; VN) = w_I(h_i N; VN) = w_I(h_i; V)N = N.$$

So

$$w_I(g_i; V) \leq \bigcap_N w_I(g_i; V)N \leq \bigcap_N N = 1$$

where the intersection runs over the set of all open normal subgroups of G. □

We are finally ready to prove Theorem 3.8.

Proof of Theorem 3.8. We claim that there exists $V \trianglelefteq_c G$ such that $\rho(G/V) < \mathfrak{a}$ and

$$w_J(G; V) = 1 \qquad \text{for every proper subset } J \subsetneq \{1, ..., r\}.$$

Then it follows from Corollary 3.16, by taking $I = \{1, ..., r\}$, that

$$w(g_1 v_1, ..., g_r v_r) = w(g_1, ..., g_r) \qquad \text{for all } g_i \in G \text{ and all } v_i \in V.$$

This implies that $V \leq w^*(G)$. Moreover, using Corollary 2.17 we deduce that

$$\rho(G/w^*(G)) \leq \rho(w^*(G)/V) + \rho(G/w^*(G)) = \rho(G/V) < \mathfrak{a}.$$

It remains to prove the claim. By induction on $|I|$, where $I \subsetneq \{1, ..., r\}$, we want to show that there exists $U_I \trianglelefteq_c G$ such that $\rho(G/U_I) < \mathfrak{a}$ and $w_I(G; U_I) = 1$. Then we can take

$$V = \bigcap_{I \subsetneq \{1,...,r\}} U_I.$$

Indeed, V is closed and normal since all U_I are closed and normal, also $\rho(G/V) < \mathfrak{a}$ by Lemma 2.18 and $w_J(G; V) = 1$, for every proper subset $J \subsetneq \{1, ..., r\}$, by construction.

If $I = \emptyset$ then from Theorem 3.9 we know that there exists $H \trianglelefteq_c G$ satisfying $w(H) = 1$ and $\rho(G/H) < \mathfrak{a}$, so take $U_\emptyset = H$. Now suppose that $|I| \geq 1$. For each $J \subsetneq I$ induction yields $U_J \trianglelefteq_c G$ such that $\rho(G/U_J) < \mathfrak{a}$

and $w_J(G;U_J)=1$. Then $U=\bigcap\{U_J : J\subsetneq I\}\trianglelefteq_c G$ satisfies $\rho(G/U)<\mathfrak{a}$, by Lemma 2.18, and

$$w_J(G;U)=1 \qquad \text{for every proper subset } J\subsetneq I. \tag{27}$$

Let $L=\{sU : s\in S\}$ be a set of generators of G/U converging to 1. If S is finite, then $|S|<\mathfrak{a}$. Otherwise, by Proposition 2.13, we have that $|S|=\rho(G/U)<\mathfrak{a}$. Let $\widetilde{S}$ be the abstract subgroup of G generated by S, note that $|\widetilde{S}|<\mathfrak{a}$ by Lemma 3.17. If $\mathbf{g}=(g_i)_{i\in I}$ is a family in $\widetilde{S}$, by (27), Lemma 3.13 yields $U_{\mathbf{g}}\trianglelefteq_c G$, with $U_{\mathbf{g}}\subseteq U$, such that $\rho(G/U_{\mathbf{g}})<\mathfrak{a}$ and $w_I(g_i;U_{\mathbf{g}})=1$. Consider now the set $\mathcal{U}=\{U_{\mathbf{g}} : \mathbf{g}=(g_i)_{i\in I} \text{ is a family in } \widetilde{S}\}$. We have that

$$U_I=\bigcap_{U_{\mathbf{g}}\in\mathcal{U}} U_{\mathbf{g}}\trianglelefteq_c G$$

is contained in U and satisfies $\rho(G/U_I)<\mathfrak{a}$ by Lemma 2.18, because $|\mathcal{U}|\leq r|\widetilde{S}|<r\mathfrak{a}=\mathfrak{a}$. Moreover, by construction

$$w_I(g_i;U_I)=1 \qquad \text{for all families } \mathbf{g}=(g_i)_{i\in I} \text{ in } \widetilde{S}^{(r)}.$$

So by Lemma 3.18 it follows that

$$w_I(g_i;U_I)=1 \qquad \text{for all } \mathbf{g}=(g_i)_{i\in I} \text{ in } \langle S\rangle^{(r)}.$$

Moreover, from (27) and Corollary 3.16 we have that

$$w_I(g_iU;U_I)=w_I(g_i;U_I)=1 \qquad \text{for all families } \mathbf{g}=(g_i)_{i\in I} \text{ in } \langle S\rangle.$$

Finally, since

$$G=\bigcup_{s\in\widetilde{S}} sU$$

it follows that

$$w_I(G;U_I)=\langle\bigcup w_I(g_iU;U_I)\rangle=1,$$

which concludes the proof of the claim. □

We conclude this chapter with two corollaries of Theorem 3.8.

Corollary 3.19. Let G be an infinite profinite group and suppose that $|G_w|<2^{\mathfrak{a}}$, for some infinite cardinal number $\mathfrak{a}$. Then $|w(G)|<2^{\mathfrak{a}}$.

Proof. Let $\mathfrak{b}$ be the least element in the set $\{\mathfrak{c} \in Card : 2^{\mathfrak{c}} = 2^{\mathfrak{a}}\}$. We can assume that $\mathfrak{b} > \aleph_0$, since it has been proven that multilinear commutator words are strongly concise [1, Theorem 1.1], hence, if $|G_w| < 2^{\aleph_0}$, then clearly $|w(G)| < 2^{\aleph_0}$.

From Theorem 3.8 we know that $\rho(G/w^*(G)) < \mathfrak{b}$, where $w^*(G)$ is the w-marginal subgroup of G. Let R be a set of generators converging to 1 of $G/w^*(G)$. By [4, Exercise 17.1] there exists a set $S \subseteq G$ converging to 1, such that $|S| = |R|$ and $G = \langle S \rangle w^*(G)$ (S is a set of representatives of the cosets in R). Note that $w(\langle S \rangle)$ is a subgroup of (the closed subgroup) $\langle S \rangle$, so $|w(\langle S \rangle)| \leq |\langle S \rangle|$. By the definition of the w-marginal subgroup of G

$$w(g_1 v_1, ..., g_r v_r) = w(g_1, ..., g_r), \qquad \text{for all } g_i \in \langle S \rangle \text{ and } v_i \in w^*(G).$$

Therefore

$$G_w \subseteq w(\langle S \rangle).$$

It follows that

$$w(G) = \langle G_w \rangle \leq w(\langle S \rangle),$$

hence

$$|w(G)| \leq |w(\langle S \rangle)|.$$

Let us now distinguish two cases. If R, the set of generators converging to 1 of $G/w^*(G)$, is finite then so is S. So we have that $\langle S \rangle$ is a finitely generated profinite group, by Proposition 2.13 the number of open subgroups of $\langle S \rangle$ is countable, and so $\rho(\langle S \rangle) \leq \aleph_0$. This imples that $|\langle S \rangle| = 2^{\rho(\langle S \rangle)} \leq 2^{\aleph_0}$, which is smaller than $2^{\mathfrak{b}}$.

On the other hand, if R is infinite, then $|R| = |S| = \rho(G/w^*(G))$ by Proposition 2.13. Furthermore, S is an infinite set generators converging to 1 of $\langle S \rangle$, so again by Proposition 2.13, we deduce that $|\langle S \rangle| = 2^{|S|} = 2^{\rho(G/w^*(G))} < 2^{\mathfrak{b}}$. □

This proves Conjeture 3.6 for multilinear commutator words.

We conclude this chapter and the thesis by proving the following result:

Corollary 3.20. Let G be a profinite group. Then we have that G_w and $w(G)$ are finite or $|G_w| = |w(G)| = 2^{\mathfrak{a}}$ for some infinite cardinal number $\mathfrak{a}$.

Proof. If G_w is finite, then $w(G)$ is also finite, since w is concise (see [14, Theorem 1]).
On the other hand, if G_w is infinite, then $w(G)$ is also infinite, as $|G_w| \leq |w(G)|$. Moreover, $w(G)$ is an infinite profinite group so by Theorem 2.20 we know that $|w(G)| = 2^{\mathfrak{a}}$ for some infinite cardinal number $\mathfrak{a}$. Now if $|G_w| < |w(G)| = 2^{\mathfrak{a}}$, it follows from Corollary 3.19 that $|w(G)| < 2^{\mathfrak{a}}$ which is a contradiction. So $|G_w| = |w(G)| = 2^{\mathfrak{a}}$. □

4 Appendix 1: Axioms

4.1 Axioms of Zermelo-Fraenkel (ZF)

Axiom 4.1 (Axiom of Extensionality)**.** If X and Y have the same elements, then $X = Y$.

Axiom 4.2 (Axiom of Pairing)**.** For any a and b there exists a set $\{a, b\}$ that contains exactly a and b.

Axiom 4.3 (Axiom Schema of Separation)**.** If P is a property (with parameter p), then for any X and p there exists a set $Y = \{u \in X : P(u, p)\}$ that contains all those $u \in X$ that have property P.

Axiom 4.4 (Axiom of Union)**.** For any X there exists a set $Y = \bigcup X$, the union of all elements of X.

Axiom 4.5 (Axiom of Power Set)**.** For any X there exists a set $Y = P(X)$, the set of all subsets of X.

Axiom 4.6 (Axiom of Infinity)**.** There exists an infinite set.

Axiom 4.7 (Axiom of Regularity)**.** Every nonempty set has an $\in$-minimal element.

Axiom 4.8 (Axiom Schema of Replacement)**.** If a class F is a function, then for any X there exists a set $Y = F(X) = \{F(x) : x \in X\}$.

4.2 Axiom of choice (C)

Axiom 4.9 (Axiom of choice)**.** For any set X of nonempty sets, there exists a choice function f defined on X.

4.3 Continuum Hypotheiss

Axiom 4.10 (Continuum Hypothesis)**.** There is no set whose cardinal number is strictly between that of the integers and the real numbers.

In Zermelo–Fraenkel set theory with the axiom of choice (ZFC), this is equivalent to the following equation in aleph numbers:

$$2^{\aleph_0} = \aleph_1$$

Axiom 4.11 (Generalized Continuum Hypothesis)**.** If the cardinality of an infinite set lies between that of an infinite set S and that of the power set $P(S)$ of S, then it has the same cardinality as either S or $P(S)$.

In Zermelo–Fraenkel set theory with the axiom of choice (ZFC), this is equivalent to the following equation in aleph numbers:

$$\aleph_{\alpha+1} = 2^{\aleph_\alpha} \qquad \text{for every ordinal number } \alpha.$$

References

[1] E. Detomi, B. Klopsch and P. Shumyatsky, 'Strong conciseness in profinite groups'. J. London Math. Soc. (2) 00 (2020) 1–17.

[2] E. Detomi, M. Morigi and P. Shumyatsky, 'On conciseness of words in profinite groups'. J. Pure Appl. Algebra 220 (2016) 3010–3015.

[3] E. Detomi, M. Morigi and P. Shumyatsky, 'On profinite groups with commutators covered by countably many cosets'. J. Algebra 508 (2018) 431–444.

[4] M. D. Fried Moshe Jarden, Field Arithmetic. Pitman, Springer-Verlag Berlin Heidelberg (2005)

[5] S. V. Ivanov, 'P. Hall's conjecture on the finiteness of verbal subgroups', Soviet Math. (Iz. VUZ) 33 (1989) 59–70.

[6] T. Jech, Set Theory. Springer-Verlag Berlin Heidelberg (2003)

[7] A. Levy, Basic Set Theory. Springer-Verlag Berlin Heidelberg (1979)

[8] H. Neumann, Varieties of Groups, Springer-Verlag, Berlin Heidelberg New York (1967).

[9] L. Ribes, P. Zalesskii, Profinite Groups. Springer-Verlag, Berlin Heidelberg (2010)

[10] D. J.S. Robinson, A Course on the Theory of Groups. Springer, New York (1996)

[11] D. J. S. Robinson, Finiteness Conditions and Generalized Soluble Groups. Parts 1 and 2. Springer, Berlin (1972)

[12] M.J. Tomkinson, FC-groups. Pitman, Boston/London/Melbourne, (1984)

[13] R. F. Turner-Smith, 'Marginal subgroup properties for outer commutator words', Proc. Lond. Math. Soc. 14 (1964) 321–341.

[14] J. C. Wilson, 'On outer-commutator words'. Canad. J. Math. 26 (1974) 608–620.

[15] J. S. Wilson, Profinite Groups. Clarendon Press, Oxford (1998)