An Introduction to p-adic Analytic Groups

Frieder Selisko

Bachelor's thesis
2023:K14

Lund University

Faculty of Science
Centre for Mathematical Sciences
Mathematics

CENTRUM SCIENTIARUM MATHEMATICARUM

Popular Abstract

There are few concepts that are as integral to our culture, thinking and to the nature of the universe as the idea of symmetry. From the most fundamental principles of physics to the simple reflection symmetry of a human face, symmetry can be found in the smallest of particles and the biggest astronomical objects. When thinking about symmetry the concepts of reflection symmetry or rotational symmetry immediately come to mind and they suggest that objects are symmetric if they do not change their structure when a certain action is carried out. We usually think of this action as a rotation or reflection but in a mathematical sense this action is less restricted. If we consider four identical objects that are placed in a line we can certainly perform a reflection and thus exchange the first and the fourth as well as the second and the third object. However, would not the structure remain the same if we exchanged the first and the second object for example? Thus, we have discovered another symmetry. This is just a very simple example of a symmetry in a mathematical sense, however, symmetries can be extremely complex.

We can now define, in a very intuitive way, what a group is. Let us say that we are given a structure with a certain symmetry. This can be something as simple as the four objects from above. Now we consider all actions that leave the structure the same, in other words all actions related to a certain symmetry, let us call these actions symmetry actions. Then this collection of symmetry actions is a group. Not only that but every group can be seen as such a collection of symmetry actions for some structure (Frucht's theorem).

Let us now have a closer look at the structure of four identical objects. A very important thing to notice is that we can perform two such symmetry actions successively. Let us consider the action of exchanging the first and second object and let us denote this symmetry action as $(1\,2)$. So what happens if we first carry out this action and afterwards exchange the second and third object, $(2\,3)$? Well, the first object gets moved to the second position and then to the third position. The second objects is moved to the first position and the third object is moved to the second position. Now, what happens if we exchange the order of the two symmetry actions that we have performed? Firstly, we exchange the second and the third object and secondly, we exchange the first and the second object. Then the third object ends up in the first position, while the first object moves to the second position and the second object moves to the third position. In other words, the outcome is not the same; indeed, $(1\,2)(2\,3)$ is not equal to $(2\,3)(1\,2)$! Thus, for some groups we can not change the order of the symmetry actions. However, for many other groups it does not matter in which order we perform

the symmetry actions. These groups are called abelian groups. In a certain sense, abelian groups are easier to understand and to work with. For this reason there is a lot of research about them.

Another property that many groups have is that if we take a symmetry action and apply it several times we end up where we started. If we exchange the first and the second object in the example above and then do the exact same symmetry action again we end up at the starting position. In this case we needed to apply the symmetry action $(1\,2)$ only twice to arrive at the starting position, we say that $(1\,2)$ has order 2. If we consider the symmetry action of rotating a square 90 degrees, we need to carry out this action four times to end up where we started. In other words, the symmetry action of rotating a square 90 degrees has order 4. Let us now consider a certain prime p. A group where every element, i.e. every symmetry action has order of a power of p is called a p-group. Those groups are very well understood and are very important tools when it comes to understanding groups in general.

In this thesis I will introduce different types of groups. In general we want to study groups that have a useful structure for example to classify certain types of groups. We also want to achieve a high level of understanding of the types of groups that we are looking at. For those two reason it is essential to look at groups with a relatively simple structure and then generalize the findings to more complex groups. I will do this on two separate occasions in this thesis.

Firstly, the easiest method to separate "easy" groups from "hard" groups is by dividing them into finite and infinite groups. Looking at a finite amount of symmetry actions is in most cases an easier job than looking at an infinite amount of such actions. Having that in mind I will first introduce the concept of a "profinite group". These groups are more or less a combination of finite groups and a logical generalization of the concept of finiteness.

In a similar manner I will introduce "powerful" p-groups. These are a generalization of the well-understood abelian p-groups.

Finally this will lead me to groups that are both profinite and powerful p-groups. These are called powerful pro-p groups. The p-adic analytic pro-p groups are a special case of such powerful pro-p groups and of particular interest to group theoretic research since they have been useful when proving or disproving certain conjectures.

Abstract

In this thesis we introduce the concept of a p-adic analytic pro-p group. To do so we discuss important theorems and concepts connected to more general types of groups, these include profinite groups, pro-p groups, powerful p-groups, powerful pro-p groups and uniform groups.

Acknowledgement

I would like to thank my supervisor Anitha Thillaisundaram for the invaluable and concise feedback I have received and for answering my e-mails almost immediately. I would also like to thank my family for taking me in for this short amount of time and giving me as good of a working environment as possible.

Contents

Chapter 1

Introduction

The research interest of my thesis, p-adic analytic groups, are topological groups which means they combine two different fields of mathematics, group theory and topology. Before group theory became an independent research topic it was introduced separately within two different branches of mathematics.

The great mathematicians Leonhard Euler and Carl Friedrich Gauss encountered group theory in their research of number theory, for example in Euler's proof of Fermat's little theorem [7]. In a very different branch of mathematics, when trying to determine the solvability of polynomials, Joseph Louis Lagrange [19] and Évariste Galois [9] introduced the permutation groups and their connection to the solvability of polynomials. Furthermore, Galois linked the topics of group and field theory, thereby creating Galois theory. The breakthrough of group theory as a stand-alone subject, however, came towards the end of the 19th century as Camille Jordan published the first book treating group theory [15]. Around the same time, symmetry groups, and slightly later Lie groups, were studied systematically [21].

The importance of group theory in modern-day research cannot be understated. Most branches of mathematics such as algebraic geometry, harmonic analysis and combinatorics, give rise to group theoretic applications. The applications of group theory has had a big impact on cryptography and physics as well. Symmetry groups for example have been used to describe many physical systems such as lattices or atoms. Furthermore, the two most important models in physics, the standard model and the theory of general relativity are heavily based on group theory.

The branch of topology on the other hand can be traced back to the book Analysis Situs (1895) by Henri Poincaré [23], where he corrected and vastly extended previous works connected to topology by, among others, Augustin-Louis Cauchy and Bernhard Riemann. The foundation for modern day topology was laid by introducing the concepts of a metric space (Fréchet, 1906 [8]) and a topological space (Hausdorff, 1914 [14]). Nowadays, topology is relatively closely connected to set theory. Topology, especially algebraic and geometric topology has been applied to many different subjects in order to understand the structure of certain objects, these objects can be sets in data analysis or proteins in biology.

This leads us finally to the topic of topological groups which has been studied extensively since 1925. This subject studies groups that are simultaneously topological spaces, thus combining group theory and topology. Notable applications of topological groups are their connections to integrals and Fourier series that were established by Alfréd Haar [13] and André Weil [18] respectively.

Within group theory I want to highlight three types of groups that are very well understood. Finite groups, abelian groups, where all elements commute and p-groups where p is a prime and the order of every element is a power of p. This thesis introduces generalizations to the mentioned groups.

- Profinite groups and pro-p groups which are a generalization of finite groups respectively finite p-groups.

- Powerful p-groups which are a generalization of abelian p-groups.

- Powerful pro-p groups which combine both generalization above.

The subject of profinite groups builds on the work of Jean-Pierre Serre [25] and John Tate [27] from the 1960s. Profinite groups are inverse limits of finite groups and thus closely related to finite groups. For this reason it is possible to generalize many theorems for finite groups to profinite groups. The most notable example of profinite groups are (infinite) Galois groups.

In the same sense that our understanding of finite groups carries over to profinite group we can apply many characteristics of abelian p-groups to powerful p-groups. Powerful p-groups have been integral to the solution of the restricted Burnside problem [28] and the classification of finite p-groups using the coclass conjectures [20]. Finally, powerful pro-p groups and especially p-adic analytic pro-p groups have been useful to solve long-standing conjectures and to classify pro-p groups [6].

After introducing basic group theoretic and topological concepts I will dedicate one chapter of this thesis to profinite and pro-p groups and prove that they are the inverse limit of an inverse system of finite groups. Then I will state and prove important theorems connected to powerful finite p-groups, the lower p-series and the Frattini subgroup. In the last chapter I will introduce powerful pro-p groups, uniformly powerful pro-p groups and

p-adic analytic pro-p groups. Here the focus will be on the introduction of several different (hypothesized) characterizations of p-adic analytic pro-p groups using for example the concept of manifolds or the Hausdorff spectrum. In the end I will briefly introduce a conjecture that was disproved using p-adic analytic pro-p groups.

Chapter 2

Topological concepts and group theoretic concepts

The definitions and theorems in this chapter can be found in most introductory books (see [3] and [22] for further reference).

2.1 Basic concepts

In this section we prepare for the definition of a topological group and introduce important topological and group theoretic concepts.

2.1.1 Group theoretic concepts

We start by introducing basic group theoretic concepts. Examples of those will be collected below.

Definition 2.1.1. A *group* $(G, \cdot)$ (usually just G) is a set G together with a binary operation $\cdot : G \times G \mapsto G$ such that the following conditions are fulfilled.

(i) For any three elements $a, b, c \in G$ one has $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

(ii) There exists an identity element $e \in G$ (sometimes written as 1) such that $a \cdot e = e \cdot a = a$ for any $a \in G$.

(iii) For each element $a \in G$ there exists $a^{-1} \in G$ such that $a \cdot a^{-1} = a^{-1} \cdot a = e$.

Similarly to other contexts it is possible to omit the $\cdot$, i.e. $a \cdot b$ can be written as ab.

Definition 2.1.2. A *group homomorphism* is a map $f : A \to B$ from a group $(A, \cdot)$ to a group $(B, *)$ such that for all $a_1, a_2 \in A$ we have that

$$f(a_1 \cdot a_2) = f(a_1) * f(a_2).$$

Definition 2.1.3. A *subgroup* H of a group G (written $H \leq G$) is a subset of G that forms a group itself with respect to the same operation as in G. Thus it needs to be closed under products and inverses.

Definition 2.1.4. A *normal subgroup* N of G (written $N \trianglelefteq G$) is a subgroup, where $gng^{-1} \in N$ for all n in N and all g in G. The homomorphism $\phi_x : G \to G$ given by $\phi_x(g) = xgx^{-1}$ is called *conjugation.*

Definition 2.1.5. A subgroup $\langle S \rangle$ *generated by a subset* S of a group G is the smallest subgroup that contains S. Any element in $\langle S \rangle$ can be expressed as a finite product of elements in S and their inverses.

Definition 2.1.6. A *coset* of a subgroup H of G is the set $gH := \{gh \mid h \in H\}$ for an element g of G. If $g \in H$ we naturally have $gH = H$.

Definition 2.1.7. A *quotient group* of a normal subgroup N in G (written G/N) is the set of all cosets of N in G, i.e. $G/N = \{gH \mid g \in G\}$. The group operation is defined as $(aN)(bN) = (ab)N$.

Definition 2.1.8. The *centre* $Z(G)$ of a group G is the set of elements $c \in G$ that commute with all g in G, i.e. $cg = gc$ for all $g \in G$.

Definition 2.1.9. A group G is *abelian* if the group operation is commutative, i.e. for all $a, b \in G$ we have $a \cdot b = b \cdot a$.

Lemma 2.1.10. *Every cyclic group, i.e a group that is generated by a single element, is abelian.*

Proof. Let $G = \langle g \rangle$ be cyclic and let g^m and g^n be elements in G for natural numbers n and m. Then $g^m g^n = g^{mn} = g^{nm} = g^n g^m$. □

Groups can be found in many areas of mathematics and physics. Very simple examples include the symmetric group S_n of permutations of a set $M = \{1, 2, \ldots, n\}$, the whole numbers together with the addition operation, and the rational numbers without zero with multiplication. While the symmetric group is not abelian (for $n > 2$), the other two groups are examples of abelian groups.

The two trivial subgroups of any group G are the group itself and the trivial subgroup $\{e\}$. These two are naturally normal subgroups. The even integers form a subgroup denoted $2\mathbb{Z}$ of the integers $\mathbb{Z}$; indeed the sum of two even integers is even, and the negative of an even integer is even. This subgroup is normal as well, as any subgroup of an abelian group will be, simply because $gng^{-1} = gg^{-1}n = n$.

Let us consider the symmetric group S_n. The element that maps a to b and b to a, we write in the cyclic notation as $(a\,b)$. Similarly, the element $(a\,b\,c)$ maps a to b, b to c and c to a. The group S_3 consists of the elements $(1\,2), (2\,3), (1\,3), (1\,2\,3), (1\,3\,2)$ and the identity element e that leaves everything unchanged. This group has exactly four proper subgroups (that are neither S_3 nor e). Those are $\{e, (1\,2)\}$, $\{e, (1\,3)\}$, $\{e, (2\,3)\}$ and $\{e, (1\,2\,3), (1\,3\,2)\}$. It can be easily checked that the first three are in fact not normal as, for example $(1\,2\,3)(1\,2)(1\,3\,2) = (1\,3)$ is not in $\{e, (12)\}$. The last one, however, is a normal subgroup; here we can simply check for all elements, for example $(1\,2)(1\,2\,3)(1\,2) = (1\,3\,2)$ is indeed in $\{e, (1\,2\,3), (1\,3\,2)\}$, and so on. Let us call this group N. We can see that the subgroup $N = \langle(1\,2\,3)\rangle$ is generated by the element $(1\,2\,3)$ since $(1\,2\,3)(1\,2\,3) = (1\,3\,2)$ and $(1\,2\,3)(1\,3\,2) = e$. The quotient group S_3/N consists of all the cosets of N. In this case we have only two cosets as $(1\,2)N = (1\,3)N = (2\,3)N = \{(1\,2), (1\,3), (2\,3)\}$. Thus, the group S_3/N has only two elements, the identity element $e = eN = N$ and the element $a = (1\,2)N$ with the property $a^2 = e$.

Definition 2.1.11. The *exponent* of a group G is the smallest natural number n such that for all g in G we have that $g^n = e$.

Lemma 2.1.12. *A group of exponent 2 is abelian.*

Proof. We have that

$$ab = ba \qquad \Longleftrightarrow \qquad baba = b^2a^2 = e.$$

The last equation is true since $baba = (ba)^2 = e$. □

Definition 2.1.13. The *order* $|G|$ of a group G is the number of its elements. The order of an element g of G however, is the smallest integer n such that $g^n = \underbrace{g \cdot g \cdots g}_{n \text{ times}} = e$.

Definition 2.1.14. A *p-group* is a group G, such that the order of any element of G is a power of p, where p denotes a prime number. The order of a finite p-group is necessarily a power of p as well.

The simplest example of a p-group is the cyclic group C_p of order p, a group that is generated by a single element, i.e. $C_p = \{e, a, a^2, \ldots, a^{p-1}\}$.

Such a cyclic group is often represented as the quotient group $\mathbb{Z}/p\mathbb{Z}$. Infinite p-groups are relatively meaningful in group theory, apart from the pro-p-groups that will be discussed in this thesis, the Tarski monster groups are counterexamples to the well-known Burnside problem and the von Neumann conjecture. However, relatively simple infinite p-groups do exist as well, for example the infinite-dimensional vector space of the field $\{0, 1\}$.

Lemma 2.1.15. *Let G be a p-group and M a maximal subgroup of G. Then M is normal in G.*

Proof. It is clear that a subgroup M is maximal if and only if $|G : M| = p$. Indeed, let M be maximal. Then G/M has no proper normal subgroup. In a p-group this implies that $|G : M| = p$. Conversely, let $|G/M| = p$. Then G/M has no proper subgroups. Let us assume that there exists a proper subgroup N containing M. Then N/M is a proper subgroup of G/M contradicting that G/M has no proper subgroups, thus the claim follows. Now, we will use the fact that the centre of a p-group is non-trivial, which follows directly from the class equation. Let G be a group of order p^n. We proceed by induction on n, where $n = 1$ is clear, since the only maximal proper subgroup is the trivial group. Let M be a maximal subgroup and let $c \neq 1$ be an element of the centre of G. If $c \in M$ it follows by the induction hypothesis that $M/\langle c\rangle$ is normal in $G/\langle c\rangle$ and by the correspondence theorem it follows that M is normal in G. If $c \notin M$, then $M\langle c\rangle = G$ and thus M is normal. □

Lemma 2.1.16. *Let G be a finite p-group. Then every cyclic normal subgroup of order p is contained in the centre.*

Proof. Let c be an element of such a cyclic normal subgroup N and $g \in G$. Then $gcg^{-1} = c^k$ for $0 < k < p$, however, since conjugation is a homomorphism it is also true that $gc^\ell g^{-1} = c^{\ell k}$. Now $g^\ell c g^{-\ell} = c^{k^\ell}$. Since G is a finite group there exists an n such that $g^{p^n} = 1$. Hence $c = g^{p^n} c g^{-p^n} = c^{kp^n}$. This requires that $k^{p^n} = \left(k^{p^{n-1}}\right)^p \equiv 1 \pmod{p}$. Fermat's little theorem states that $a^p \equiv a \pmod{p}$ and thus $k^{p^n} \equiv k \equiv 1 \pmod{p}$. However, since $0 < k < p$ we have that $k = 1$ and $gc = cg$ for all g in G. □

Lemma 2.1.17. *Let G be a p-group of order p^n. Then G has a normal subgroup of order p^m for $m \leq n$.*

Proof. We use induction on n. For $n = 1$ all subgroups are normal. Let G be of the order p^n and let $Z(G)$ be the nontrivial centre of G. Let us consider a cyclic subgroup C of order p of $Z(G)$. Then G/C has a normal subgroup of the order p^m which we call N/C. However since $N/C \triangleleft G/C$ it follows that N is a normal subgroup of G of order p^m. □

Definition 2.1.18. The *commutator* of two elements a and b of a group G is the element $[a, b] = a^{-1}b^{-1}ab$. The commutator of two subgroups A and B of G is the subgroup $[A, B]$ generated by the set $\{[a, b] \mid a \in A, b \in B\}$. The commutator subgroup $G' := [G, G]$ of G is the subgroup generated by all the commutators $[a, b]$ where a and b are elements of G. We also define $[a_1, a_2, \ldots, a_{n-1}, a_n] = [[a_1, a_2, \ldots, a_{n-1}], a_n]$ for elements $a_i \in G$ and $[H_1, H_2, \ldots, H_{n-1}, H_n] = [[H_1, H_2, \ldots, H_{n-1}], H_n]$ for subgroups H_i of G.

Lemma 2.1.19. *The commutator subgroup G' of a group G is a normal subgroup and the smallest normal subgroup such that the quotient of* G *by it is abelian.*

Proof. Every element of the commutator subgroup is a finite product of commutators and their inverses. However $[a, b]^{-1} = [b, a]$. Let $h = h_1 \cdots h_n$, where $h_1, \ldots, h_n$ are commutators, then

$$ghg^{-1} = gh_1g^{-1} \cdots gh_ng^{-1}$$

is in G' if gh_ig^{-1} is in G' for all i. This is in fact the case, as for elements a, b, g of G we have

$$g[a, b]g^{-1} = ga^{-1}b^{-1}abg^{-1} = ga^{-1}g^{-1}gb^{-1}g^{-1}gag^{-1}gbg^{-1}.$$

Now let $b_1 = gbg^{-1}$ and $a_1 = gag^{-1}$, then

$$g[a, b]g^{-1} = a_1^{-1}b_1^{-1}a_1b_1.$$

Thus $G' \trianglelefteq G$.

Let H be a normal subgroup. The quotient group G/H is abelian if and only if for all a, b in G we have that $(aH)(bH) = (bH)(aH)$. We have

$$(aH)(bH) = (bH)(aH) \iff (ab)H = (ba)H \iff a^{-1}b^{-1}ab \in H.$$

Thus G/H is abelian if and only if $G' \subseteq H$. □

Lemma 2.1.20. *For any group G, we have that $[G, G] \leq G^2$.*

Proof. The group G/G^2 is either the trivial group if $G = G^2$, in which case the statement above is true, or G/G^2 has exponent 2 since for all elements in G/G^2 we have $(gG^2)(gG^2) = g^2G^2 = G^2$. Thus G/G^2 is abelian which implies that $[G, G] \leq G^2$ by the previous lemma. □

2.1.2 Topological concepts

Definition 2.1.21. A *topology* $\mathcal{T}$ on a set X is a collection of subsets of X such that

(i) the empty set $\emptyset$ and the entire set of X are elements of $\mathcal{T}$,

(ii) any arbitrary union of members of $\mathcal{T}$ is in $\mathcal{T}$,

(iii) any intersection of a finite number of members of $\mathcal{T}$ is in $\mathcal{T}$.

Definition 2.1.22. The ordered pair $(X, \mathcal{T})$ of a set X and a topology $\mathcal{T}$ on X is called a *topological space*.

In most literature the topology is omitted in the notation and we would write a topological space X.

A member U of $\mathcal{T}$ is called an *open set*, whereas the complement $X \setminus U$ is called a *closed set*. This means that $\emptyset$ and X are both open and closed. We might recognize the term of an open set from its standard use within the real numbers, where the usual open sets, i.e. unions of open intervals, are the elements of the standard topology on $\mathbb{R}$. Two simple examples of topologies are the trivial topology, also called the indiscrete topology, which only consists of the empty set and X itself, and the discrete topology which is the collection of all subsets of X. To determine whether a collection of subsets is a topology we just need to check the three conditions above. (For the trivial topology it is very clear that all three conditions are fulfilled as the only possible intersection and union are the empty set and X itself.)

Definition 2.1.23. The *interior* of a subset A of a topological space is defined as the union of all open sets contained in A, and the *closure* of A is defined as the intersection of all closed sets containing A. It follows that the interior $\operatorname{int} A$ is open and the closure $\overline{A}$ is closed.

If we once again consider the real numbers together with the standard topology, two simple examples come to mind. Firstly, the interior of the rational numbers is empty since no open set is contained within the rationals. However, every open set contains a rational number. This means that every closed set that contains all rational numbers contains the whole space, in other words $\overline{\mathbb{Q}} = \mathbb{R}$. We would say that $\mathbb{Q}$ is *dense* in $\mathbb{R}$. Secondly, the interior of any interval is the corresponding open interval, while the closure is the corresponding closed interval.

$$\operatorname{int}([a, b]) = \operatorname{int}((a, b]) = (a, b)$$

Furthermore, the trivial and discrete topology let us make more general statements about the interior and closure of a set. In the discrete topology, the interior and the closure are the set itself, since any set is both open and closed. In the trivial topology, the interior of any set apart from the entire space X is the empty set, whereas the closure except for the empty set is always X.

Definition 2.1.24. Let $(X, \mathcal{T})$ be a topological space and Y a subset of X. Together with the *subspace topology*

$$\mathcal{T}_Y = \{Y \cap U \mid U \in \mathcal{T}\},$$

the subset Y is called a *subspace* of X.

We should remember that the subspace itself is both open and closed, which means that the interval $[a, b]$ as a subspace of the real numbers together with the standard topology is in fact open and closed, as a set however it is naturally closed. Continuing with the real numbers and the standard topology we can clearly see that the subspace of the whole numbers has the trivial topology as its subspace topology. This is true since any whole number a is contained in the open set $(a + 1, a - 1)$ which does not contain any other whole number. One might assume that this also applies to the rational numbers, however, in this case single-point sets are not open, as any open interval around a point contains an infinite amount of rational numbers. The open sets are in fact intervals (a, b), where a and b can be rational or irrational. One has to keep in mind, that if a and b are irrational the boundary points are not within the subspace and therefore

$$\mathbb{Q} \cap (a, b) = \mathbb{Q} \cap [a, b],$$

and thus (a, b) is both open and closed in the subspace topology.

Definition 2.1.25. A *basis* $\mathcal{B}$ for a topology on a set X is a collection of subsets of X such that

(i) for each $x \in X$ there exists a basis element $B \in \mathcal{B}$ such that $x \in B$,

(ii) if x is in the intersection of two basis elements B_1 and B_2 then there exists a basis element B_3 containing x such that $B_3 \subset B_1 \cap B_2$.

The *topology $\mathcal{T}$ generated by a basis $\mathcal{B}$* consist of all unions of basis elements. The usual basis for the standard topology on $\mathbb{R}$ consists of all open intervals. The introduction of a basis is necessary to define the product topology on a Cartesian product $X \times Y$.

Definition 2.1.26. Let X and Y be topological spaces. The sets $U \times V$, where U is open in X and V is open in Y form a basis for the *product topology* of $X \times Y$.

To extend this definition to infinite Cartesian products we need to introduce the notion of a subbasis.

Definition 2.1.27. A *subbasis* $\mathcal{S}$ for a topology on X is a collection of subsets of X whose union equals X. The topology generated by $\mathcal{S}$ consist of all unions of finite intersections of elements of $\mathcal{S}$.

It is clear that the finite intersections of subbasis elements form a basis. The semi-finite intervals $(-\infty, a)$ and (b, ∞) generate the standard topology on $\mathbb{R}$ since the basis elements can be created using the simple intersection $(a, b) = (-\infty, a) \cap (b, \infty)$. It is a bit harder to see that all rational open intervals generate the standard topology as well. This is true since any open interval (a, b), where b is irrational, is the infinite union of all open intervals (a, b_i), where b_i is rational. This is again due to the fact that the rationals are dense in the real numbers.

Definition 2.1.28. Let ψ_i be the projection mapping assigning each element its ith component. The *product topology* of the product space $\prod_{i \in J} X_i$ is the topology generated by the subbasis consisting of all sets $S_i = \{\psi_i^{-1}(U_i) \mid U_i \text{ open in } X_i\}$.

The resulting basis elements of the product topology on $\prod X_i$ are therefore all sets of the form $\prod U_i$, where U_i is open in X_i for all i and $U_i = X_i$ for all but finitely many i.

Definition 2.1.29. A map $f : X \to Y$ between sets X and Y with their respective topologies $\mathcal{T}_X$ and $\mathcal{T}_Y$ is *continuous* if for any open set $U \in \mathcal{T}_Y$ the set $f^{-1}(U)$ is in $\mathcal{T}_X$ (and thus open as well).

We can once more examine the standard topology on the real numbers and compare the above definition with the usual $\epsilon - \delta$ definition for continuity. We say that a function is continuous at a point x_0, if for a given $\epsilon > 0$ there exists a $\delta > 0$ such that $|x - x_0| < \delta$ implies that $|f(x) - f(x_0)| < \epsilon$. Naturally the two definitions should be the same. We observe that the interval $U = (f(x_0) - \epsilon, f(x_0) + \epsilon)$ is an open set which implies that $f^{-1}(U)$ is open as well, thus it is a union of open intervals. Let $(x_0 - a_1, x_0 + a_2)$ be the interval that contains x_0. Then $|x - x_0| < \delta := \min\{a_1, a_2\}$ implies that $|f(x) - f(x_0)| < \epsilon$. To show the other direction we want to derive from the $\epsilon - \delta$ definition that for each open set U the inverse image $f^{-1}(U)$ is open as well. Since U is a union of open intervals each $x_0 \in U$ is contained in an interval $(f(x_0) - \epsilon, f(x_0) + \epsilon)$. We know that there exists a δ such that $|x - x_0| < \delta$ implies that $|f(x) - f(x_0)| < \epsilon$. In other words the interval $V = (x_0 - \delta, x_0 + \delta)$ is in $f^{-1}(U)$. Thus x is contained in an open interval. This is true for any point $x \in f^{-1}(U)$ and consequentially $f^{-1}(U)$ is open.

Naturally any function $f : (X, \mathcal{T}_X) \to (Y, \mathcal{T}_Y)$ is continuous if $\mathcal{T}_X$ is the discrete topology.

A useful property of continuous functions is that a composite of two continuous functions is continuous as well. Let $f : X \to Y$ and $Y \to Z$ be continuous, if U is open in Z, then $g^{-1}(U)$ is open in Y and $f^{-1}(g^{-1}(U)) = (g \circ f)^{-1}(U)$ is open in X. Thus $g \circ f$ is continuous.

Definition 2.1.30. A *homeomorphism* is a bijective and bicontinuous function, i.e a continuous function whose inverse is continuous as well. Two topological spaces with a homeomorphism between them are called *homeomorphic.*

An easy example of a homeomorphism is the continuous function $f(x) = ax$ and thus the intervals $[0, 1]$ and $[0, a]$ are homeomorphic in the real numbers.

A slightly more advanced function is given below and we leave it to the reader to show that it is continuous on the interval (a, b). Any real interval (a, b) is homeomorphic to the real numbers through the homeomorphism

$$f(x) = \frac{1}{a - x} + \frac{1}{b - x}.$$

Definition 2.1.31. For a topological space $(X, \mathcal{T})$ and a point $x \in X$ we define a *neighbourhood* of x to be a subset of X that contains an open set U with $x \in U$.

In the standard topology $[0, 2] \cup \mathbb{Q}$ is not a neighbourhood of zero but $[-1, 1]$ is.

Definition 2.1.32. A topological space $(X, \mathcal{T})$ is *Hausdorff* if any two distinct points have disjoint neighbourhoods.

Here we can observe the importance of the topology that is chosen for a given set X. A topological space consisting of any set together with the discrete topology always has the Hausdorff property, whereas any set (that contains more then two points) together with the trivial topology does not have the Hausdorff property.

Lemma 2.1.33. *Let $f : Y \to X$ be continuous and injective. If X is Hausdorff then Y is Hausdorff as well.*

Proof. For two distinct points a and b in Y we know that $f(a)$ and $f(b)$ have disjoint neighbourhoods U and V in X. Then $f^{-1}(U)$ and $f^{-1}(V)$ are disjoint neighbourhoods of a and b. □

This theorem is particularly useful since Y can be a subspace of X. This means that any subspace of a Hausdorff space is Hausdorff as well.

Lemma 2.1.34. *Let X_i be nonempty spaces, then $\prod X_i$ is Hausdorff if and only if each X_i is Hausdorff.*

Proof. If $\prod X_i$ is Hausdorff we can construct the continuous injection $f : X_j \to \prod X_i$, where for each component $i \neq j$ we define $f_i = \psi_i f$ to be a constant map, where ψ_i is the projection mapping. For the jth component we define f_j to be the identity map. Thus by Lemma 2.1.33 each X_j is Hausdorff.

Conversely, let each X_i be Hausdorff and let a and b be distinct points in $\prod X_i$, in other words at least for one component $a_j \neq b_j$. However, since X_j is Hausdorff, there exist two disjoint neighbourhoods A and B of a_j respectively b_j. But this implies that for the projection mapping ψ_j we have that $\psi_j^{-1}(A)$ and $\psi_j^{-1}(B)$ are disjoint neighbourhoods of a and b. □

Definition 2.1.35. A collection A of open sets is called a *cover* of X if the union of the elements of A equals X, i.e.

$$X = \bigcup_{\alpha \in A} \alpha.$$

Definition 2.1.36. A topological space $(X, \mathcal{T})$ is *compact* if any cover A of X has a finite subset $\{\alpha_1, \dots, \alpha_n\}$ that is a cover as well,

$$X = \bigcup_{i=1}^{n} \alpha_i.$$

Any finite topological space is compact. For any open cover one can choose a finite subcover consisting of one open set for each point. Again, the trivial and the discrete topology yield very simple results. A topological space with the discrete topology is compact if and only if it is finite. Any set together with the trivial topology is a compact topological space.

The real numbers together with the standard topology are not compact since the open cover $A = \{(n-1, n+1) \mid n \in \mathbb{Z}\}$ has no finite subcover.

Lemma 2.1.37. *A topological space X is compact if and only if for each family $(Y_a)_{a \in A}$ of closed subsets of X with empty intersection there exists a finite subset $\{a_1, \dots, a_n\}$ of A such that $\bigcap_{i=1}^{n} Y_{a_i} = \emptyset$.*

Proof. The intersection of $(Y_a)_{a\in A}$ is empty if and only if the open sets $X \setminus Y_a$ cover X. There exists a finite subset $\{a_1, \ldots, a_n\}$ of A such that $\bigcap_{i=1}^{n} Y_{a_i} = \emptyset$ if and only if $X \setminus Y_a$ has a finite subcover. □

Since compactness is closely related to closedness and boundedness we will briefly introduce the concept of boundedness thereby taking a glance at metric spaces.

Definition 2.1.38. A *metric* on a set X is a function $d : X \times X \to \mathbb{R}$ such that

(i) $d(x, y) \geq 0$ for all $x, y \in X$, equality holds if and only if $x = y$;

(ii) $d(x, y) = d(y, x)$ for all $x, y \in X$;

(iii) $d(x, y) + d(y, z) \geq d(x, z)$ for all $x, y, z \in X$.

The usual metric of a Euclidean space is given as the square root of the squares of the difference in each component, i.e. the distance between the vectors (x_1, x_2, x_3) and (y_1, y_2, y_3) is $d = \sqrt{(x_1 - y_1)^2 + (x_2 - y_2)^2 + (x_3 - y_3)^2}$. Given a set X and a metric d on X we can always construct a topological space using the metric topology:

Definition 2.1.39. Let d be a metric on X. Then the *metric topology* induced by d has the basis $\mathcal{B} = \{B_d(x, \epsilon) \mid x \in X, \epsilon > 0\}$, where the ϵ*-balls* $B_d(x, \epsilon) = \{y \in X \mid d(x, y) < \epsilon\}$ are the basis elements. In this case the topological space X is called a *metric space* and is denoted by (X, d).

Definition 2.1.40. Let X be a metric space with metric d. A subset A of X is *bounded* if there is some real number M such that $d(a_1, a_2) < M$ for all $a_1, a_2 \in A$.

For a finite-dimensional Euclidean space, a subspace is compact if and only if it is closed and bounded. This is the famous Heine-Borel theorem which we will prove for subspaces of the real numbers below. For an infinite-dimensional Euclidean space, however, compactness implies closed- and boundedness but the other direction is not true. The standard example for this is the closed unit ball. This subspace is closed and bounded but not compact. One can check for example that the cover consisting of open balls of radius $\sqrt{2}$ around the points $(0, 0, 0, \ldots), (1, 0, 0, \ldots), (-1, 0, 0, \ldots), (0, 1, 0, \ldots), (0, -1, 0, \ldots), (0, 0, 1, \ldots), \ldots$ has no finite subcover.

Theorem 2.1.41. *Subsets of the real numbers together with the standard topology are compact if and only if they are closed and bounded.*

Proof. Any subset of the real numbers that is not bounded contains an ascending (or descending) sequence of numbers a_i that goes to infinity (or negative infinity). Let A be a covering of this subset containing the open intervals $(a_0, a_2), \ldots, (a_{n-1}, a_{n+1}), \ldots$. Furthermore, all other elements of A should be bounded, let us call the bound b. We can clearly see that any subset of A that is a cover as well needs to contain all intervals (a_{n-1}, a_{n+1}) for $n > b$. This shows that no finite subcover can exist and any unbounded subset of the real numbers is not compact. Similarly one can construct such a cover for any subset that is not closed. This space contains an interval $[a, b)$ (or $(b, a]$) but not b. Let A be such that the only elements that cover $[\frac{b-a}{2}, b)$ are of the form $(a, b - \frac{b-a}{n})$ for $n \in \mathbb{N}$. Such a cover has no finite subcover which shows that subsets of the real number line that are not closed are not compact. Thus compactness implies closed and boundedness.

We will now show that every closed and bounded subset U of the real number line is indeed compact. Such a subset is the union of closed intervals. Let us denote the lower and upper bound of U as a and b. Let us consider a cover of U and extend it by the open set $[a, b] \setminus U = (a, b) \cap \mathbb{R} \setminus U$, where (a, b) and $\mathbb{R} \setminus U$ are both open sets, then if $[a, b]$ is compact it follows that U is compact as well. Thus if we can show that $[a, b]$ is compact it follows that U is compact as well. We prove by contradiction. Let us assume that there exists a cover A that does not have a finite subcover. And let $[a, x]$ $(a \leq x)$ be the largest interval that can be covered by finitely many elements of A. However the element of A that covers x needs to be an open set. Thus it contains an element that is greater than x. This contradicts the assumption that $[a, x]$ is the largest interval. In conclusion, there does not exist a largest interval and any closed interval is compact. □

For completeness the Tychonoff theorem is stated here, even though we will not prove it, since it is a rather complex proof that can be found in most topology books.

Theorem 2.1.42 (Tychonoff theorem)**.** *The (possibly infinite) Cartesian product $\prod X_i$ of compact spaces X_i is compact.*

Definition 2.1.43. A topological space $(X, \mathcal{T})$ is *connected* if there does not exist a pair of disjoint nonempty sets U and V whose union is X. Such a pair of open sets of $(X, \mathcal{T})$ is called a *separation.* Observe that U and $X \setminus U$ is a separation if and only if U is both open and closed.

Lemma 2.1.44. *If X is connected and $f : X \to Y$ is continuous, then $f(X)$ is connected.*

Proof. Let A, B be a separation of $f(X)$ then $f^{-1}(A), f^{-1}(B)$ is a separation of X. □

Theorem 2.1.45. *Let X_i be topological spaces. Then $\prod X_i$ is connected if and only if each X_i is connected.*

Proof. ($\Rightarrow$) Let $\prod X_i$ be connected. There exists a continuous map $f : \prod X_i \to X_i$, which implies that X_i is connected as well.

($\Leftarrow$) Let each X_i be connected. Suppose that $A \subseteq X = \prod X_i$ is both open and closed and nonempty. We will show that $A = X$. Otherwise, A and $X \setminus A$ would form a separation. Let $a \in A$ with components a_i. We define the map $\psi : X_j \to X$ such that for $i \neq j$ it is the constant map $\psi_i : X_j \to X_i$, where every element $x \in X_j$ gets mapped to a_i and for the jth component it is the identity map on X_j. Since ψ is continuous and X_j is connected it follows that $\psi(X_j)$ is connected as well. We also have that $a \in \psi(X_j)$, thus $A \cap \psi(X_j)$ is nonempty. Since A is open and closed in X we can conclude that $A \cap \psi(X_j)$ is open and closed in $\psi(X_j)$. However $\psi(X_j)$ is connected which implies that $A \cap \psi(X_j) = \psi(X_j)$, hence $\psi(X_j) \subseteq A$. This means that any point b that differs from a in the jth component is in A. However since j was chosen arbitrarily we can conclude that any point that differs from a by a single component is in A. By induction it follows that any point that differs from a by a finite amount of components is in A.

Since A is open in X it needs to contain a basis element $\prod U_i$ of the product topology that contains a. Thus $U_i = X_i$ for all but finitely many i. But this means that given a point $x \in X$ we can get a point in $\prod U_i$ (and thus A) by changing only finitely many components which implies that $x \in A$ and thus $A = X$. □

Definition 2.1.46. A topological space $(X, \mathcal{T})$ is *totally disconnected* if every subspace is disconnected, except for one-point sets.

Here we can observe that the trivial topology always leads to a connected space whereas a topological space with the discrete topology is always totally disconnected. Another example of a totally disconnected topological space would be the rational numbers together with standard topology. It is possible for any subspace containing more than two numbers to find a separation. Let the numbers be called a and b with $a < b$, then there exists an irrational number r such that $a < r < b$ and (∞, r), (r, ∞) is a separation.

Lemma 2.1.47. *Any interval $[a, b]$ of the real number line is connected in the standard topology.*

Proof. First of all we need to observe that the real numbers fulfill the order property, i.e. that for any $x < y \in \mathbb{R}$ there exists a $z \in \mathbb{R}$ such that $x < z < y$. For the real numbers this is relatively easy to show, since $z = \frac{x+y}{2}$ fulfills this property. Let us assume towards a contradiction that there exists a separation of $[a, b]$ consisting of the two nonempty sets A and B and let $a \in A$ and $b \in B$ with $a < b$. Now let us consider the supremum $x = \sup A$ of A. Since A and B are a separation their union needs to be the interval $[a, b]$. For this reason x needs to belong to either A or B. However, since A itself is an open set, if $x \in A$ there exists an interval $[a, c)$ that contains x and which is open in A. However since $\mathbb{R}$ fulfills the order property we can find a number x_1 in A such that $x < x_1 < c$. But then x is not the supremum of A. Conversely, if $x \in B$ there exists an open set $(d, b]$ in B that contains x. Note that $(d, b]$ does not intersect A. Consequentially, $d < x$ would be a smaller supremum of A which is a contradiction. □

It is clear that this proof can be applied to open intervals and the entire real number line as well. One might recognize the connection to the intermediate value theorem of calculus.

Corollary 2.1.48 (Intermediate value theorem)**.** *Let X be a connected space and let $f : X \to Y$ be a continuous map, where Y is a subspace of the real number line together with the standard topology. If a and b are two points in X and r is a point in Y such that $f(a) < r < f(b)$ then there exists a point c in X such that $f(c) = r$.*

Proof. We recognize that the sets

$$A = f(X) \cap (-\infty, r) \text{ and } B = f(X) \cap (r, \infty)$$

are open in $f(X)$. If there does not exist a number c such that $f(c) = r$ then the sets A and B form a separation of $f(X)$. However, since X is connected and f is continuous $f(X)$ is connected as well, a contradiction. □

Corollary 2.1.49. *Let X_i be nonempty topological spaces, then $\prod X_i$ is totally disconnected if and only if each X_i is totally disconnected.*

Proof. If a single X_j contains a connected subspace $U \neq X_j$ that contains more than one point, then $\prod_{i \neq j} x_i \times U$ contains more than one point, for single points x_i. Thus, if $\prod X_i$ is totally disconnected, so is each X_i. Conversely, let A be a connected subspace of $\prod X_i$ and let ψ_i be the projection mapping assigning each element its ith component. Then $\psi_i(A)$ is connected as well. If each X_i is totally disconnected $\psi_i(A)$ is a single point and thus A as well. □

2.2 Topological groups

Definition 2.2.1. A *topological group* is a group which is also a topological space such that the maps

$$\begin{aligned} f_1 &: G \to G, & g &\mapsto g^{-1} & &\text{for } g \in G \\ f_2 &: G \times G \to G, & (g,h) &\mapsto g \cdot h & &\text{for } g, h \in G \end{aligned}$$

are continuous.

First of all, every group together with the discrete topology but also with the trivial topology forms a topological group. The latter is clear since $f_1^{-1}(G) = G$ and $f_2^{-1}(G) = G \times G$. The real numbers with the standard topology form a topological group under addition. The real numbers without zero, $\mathbb{R} \setminus \{0\}$, also form a topological group under multiplication.

We will now look at some properties of topological groups.

Theorem 2.2.2. *Let G be a topological group.*

(i) *Then for each $g \in G$ the maps $x \mapsto gx$, $x \mapsto xg$ and $x \mapsto x^{-1}$ are homeomorphisms.*

(ii) *If H is a subgroup of G and H is open (respectively closed), then every coset of H is open (respectively closed).*

(iii) *Every open subgroup of G is closed.*

(iv) *The group G is Hausdorff if and only if $\{1\}$ is a closed subset of G.*

(v) *If H is a subgroup of G and H contains a nonempty open subset U of G then H is open in G.*

Proof. (i) The given maps are all bijective. They are also bicontinuous since their inverse functions $x \mapsto g^{-1}x$, $x \mapsto xg^{-1}$ and $x \mapsto x^{-1}$ are continuous.

(ii) This follows from the fact that any coset of H can be written as gH and $x \mapsto gx$ is a bicontinuous function

(iii) Let H be an open subgroup, then gH is open as well. Furthermore

$$\bigcup_{e \neq g \in G} gH$$

is open too. Thus H is closed.

(iv) In a Hausdorff space every point distinct from $\{1\}$ is contained in an open set that does not contain $\{1\}$. The union $X \setminus \{1\}$ of those sets is therefore open as well. This is true for any single point and thus in a Hausdorff space one-point sets are always closed.

Conversely, if $\{1\}$ is closed, so are all other one-point sets as they are cosets of $\{1\}$. Consequentially, let $x \neq y$, then $U = X \setminus \{xy^{-1}\}$ is open. Let us now consider the map $f : (a, b) \mapsto a^{-1}b$. This map is continuous, which can be easily seen if one considers it as a composition of the maps $(a, b) \mapsto ab$ and $x \mapsto a^{-1}a^{-1}x$. We know that $\{1\} \in U$ and since U is open the set $f^{-1}(U)$ is open as well. Furthermore the point $(1, 1) \in f^{-1}(U)$. Now this point needs to be in a basis element of the product topology, in other words, there exist two open sets V_1 and V_2 such that $\{1\} \in V_1, \{1\} \in V_2$ and $V_1^{-1} \cdot V_2 \subseteq U$. Then V_1x and V_2y are two disjoint neighbourhoods of x respectively y. This can be easily checked; indeed, let us assume that the neighbourhoods are not disjoint, i.e. there exist $a \in V_1$ and $b \in V_2$ such that $ax = by$, then $xy^{-1} = a^{-1}b$ and thus $xy^{-1} \in U$, a contradiction. Hence the neighbourhoods are disjoint and X is Hausdorff.

(v) Let $h \in H$ and let $g : x \mapsto xh^{-1}$, then $g^{-1}(U) = Uh$ is open. However

$$\bigcup_{h \in H} Uh = H.$$

Thus H is open. □

Chapter 3

Profinite groups and pro-p groups

The proofs and definitions of this chapter are based on Chapter 1 and Appendix B of [5].

3.1 Profinite groups

3.1.1 Inverse system and inverse limits

In preparation for the different definitions of profinite groups we need to introduce some concepts from category theory.

Definition 3.1.1. A *directed set* is a nonempty partially ordered set $(I, \leq)$ such that for $i, j \in I$ there exists some $k \in I$ such that $i, j \leq k$.

It is important to notice, that two elements of a directed set do not need to be related. Let us consider the subsets of the set $\{a, b, c\}$ ordered by inclusion, for example $\{a\} \leq \{a, b\}$. Then $\{a, b\} \nleq \{a, c\}$ but also $\{a, c\} \nleq \{a, b\}$.

Definition 3.1.2. An *inverse system* of sets over a directed set I is a family of sets $(G_i)_{i \in I}$ together with maps $\phi_{ij} : G_i \to G_j$ for $i \geq j$ such that ϕ_{ii} is the identity map and $\phi_{ij}\phi_{jk} = \phi_{ik}$, whenever $i \geq j \geq k$. We will denote such a system by $\{G_i, \phi_{ij}, I\}$.

This definition usually varies for different types of sets. If the sets G_i are topological spaces the maps ϕ_{ij} are defined to be continuous, for groups they need to be homomorphisms. Hence, an *inverse limit of topological groups* over a directed set I is a family of sets $(G_i)_{i \in I}$ together with continuous homomorphisms $\phi_{ij} : G_i \to G_j$ for $i \geq j$ such that ϕ_{ii} is the identity map and $\phi_{ij}\phi_{jk} = \phi_{ik}$, whenever $i \geq j \geq k$.

Let $\mathcal{A}$ be a family of normal subgroups A_i of a given group G, such that for $i \geq j$ we have that $A_i \subseteq A_j$. We can obtain the inverse system G/A_i, where the maps are the natural epimorphisms, i.e. surjective homomorphisms $G/N \to G/M$ for $N < M$.

Definition 3.1.3. An *inverse limit* or *projective limit* of the inverse system $\{G_i, \phi_{ij}, I\}$ is a subgroup of the Cartesian product of the G_i's defined as

$$G = \varprojlim_{i \in I} G_i = \left\{ \vec{g} \in \prod_{i \in I} G_i \mid g_j = \phi_{ij}(g_i) \text{ for all } i \geq j \in I \right\}.$$

The inverse limit provides maps $\phi_i : G \to G_i$, which are called *projections.*

Lemma 3.1.4. *Let G be the inverse limit $\varprojlim G_i$ of topological groups G_i. Then if all the G_i are*

(i) *compact, so is G;*

(ii) *Hausdorff, so is G;*

(iii) *totally disconnected, so is G.*

Proof. Since G is a subgroup of $\prod G_i$ and each G_i is (i) compact, (ii) Hausdorff, respectively (iii) totally disconnected it follows that G is (i) compact, (ii) Hausdorff respectively (iii) totally disconnected by the Tychonoff theorem as well as Lemmas 2.1.34 and 2.1.49. □

3.1.2 Definitions

There are many equivalent definitions for profinite groups, the simplest is given below.

Definition 3.1.5. A *profinite group* is a compact Hausdorff topological group that is totally disconnected.

However, in the literature, there are two prevalent definitions. A formal definition using neighbourhoods of the identity and a more applied definition using the inverse limit of an inverse system of finite groups.

Definition 3.1.6. A *profinite group* is a compact Hausdorff topological group whose open subgroups form a base for the neighbourhoods of the identity, i.e. every set containing $\{1\}$ contains an open subgroup.

Definition 3.1.7. A *profinite group* is the inverse limit

$$G = \varprojlim_{i \in I} G_i$$

of an inverse system $\{G_i, \phi_{ij}, I\}$ of finite groups G_i, where each group G_i has the discrete topology.

3.1.3 Equivalence of the definitions

In this section we will show that the definitions given above are indeed equivalent. We will do this by showing that 3.1.5 implies 3.1.6, 3.1.6 implies 3.1.7 and 3.1.7 implies 3.1.5. We start by proving the following lemma.

Lemma 3.1.8. *If G is a profinite group then G is topologically isomorphic to $\varprojlim(G/N)_{N \triangleleft_o G}$.*

Proof. Let us consider the homomorphism $\tau : G \to \prod G/N$ given by $g \mapsto (gN)_{N \triangleleft_o G}$ for all N being open and normal subgroups of G. We will show that τ is a bijective continuous homomorphism, i.e. a homeomorphism and thus G and $\varprojlim(G/N)_{N \triangleleft_o G}$ are topologically isomorphic. It is important to notice that in the construction of τ the element g is fixed. Elements of $\varprojlim(G/N)_{N \triangleleft_o G}$, however can have different coset representatives for each normal subgroup, thus $\tau(G) \leq \varprojlim(G/N)_{N \triangleleft_o G}$. Since $\cap_{N \triangleleft_o G} N = 1$ the map τ is injective. Let $(g_N N) \in \varprojlim(G/N)_{N \triangleleft_o G}$. Then every finite collection of cosets $g_N N$ has a nonempty intersection. This is true since the normal subgroups form a directed set. Thus for a finite set of cosets $g_N N$ there exists a coset $g_M M$ that is contained in all $g_N N$ because all G/N map surjectively onto G/M. The translation map $x \mapsto g_N x$ from N to $g_N N$ is a homeomorphism. This implies that since N is open all cosets gN are open as well. Since the cosets are equivalence classes we conclude that they are closed as well. Since the group G is compact it follows from Lemma 2.1.37 that $\cap_{N \triangleleft_o G} g_N N$ is nonempty as well. Let $g \in \cap_{N \triangleleft_o G} g_N N$. Then $\tau(g) = (g_N N)$ and thus the map τ is bijective.

We will now show that it is also continuous. For an open subgroup M of G and open subgroups N of G we define the subgroup

$$U(M) = \prod_{N < M} G/N \prod_{N \geq M} \{1\} \leq \prod_{N \triangleleft_o G} G/N.$$

We observe that $\tau^{-1}(U(M)) = M$ and that every set containing 1 contains a subgroup $U(M)$ for a given open subgroup M. The subgroups $U(M) \cap \varprojlim(G/N)_{N \triangleleft_o G}$ form therefore a base for the neighbourhoods of 1. Here we use the property that through translation we can transfer the properties of the base for the neighbourhoods of 1 to any other element which implies that $\tau^{-1}(B)$ is open for any basis element B and thus for of any open set as well. □

Theorem 3.1.9. *Definitions 3.1.5(1), 3.1.6(2) and 3.1.7(3) are equivalent.*

Proof. (3 ⇒ 1) As each G_i gets assigned the discrete topology all of them are totally disconnected and Hausdorff. Since they are finite it follows that they are compact as well. Thus $\varprojlim G_i$ is a totally disconnected, compact Hausdorff topological group.

(1 ⇒ 2) Suppose that V is a neighbourhood of $\{1\}$. Since G is compact the closure $\overline{V}$ is compact as well. Let U be an open set contained in V. Since G (and also $\overline{V}$) is Hausdorff we can find for any point x in $\overline{V}\setminus U$ an open set $K(x) \subset \overline{V}$ such that $x \in K(x)$ and $1 \notin K(x)$. Furthermore, we can choose the $K(x)$ to be closed as well. Let D be the intersection of all closed sets $K \subseteq \overline{V}$ containing x. D is nonempty since $\overline{V} \subseteq D$. We claim that D is connected. Indeed, suppose that X, Y is a separation of D and $x \in X$. Then X is a closed set that contains x. And hence $Y \subseteq D \subseteq X$ which implies that Y is empty. Hence D is connected and thus the one-point set $\{x\}$, i.e. there exists an open and closed set $K(x)$ that contains x but not 1. Since $\overline{V}$ is compact we can find finitely many x_i such that

$$\overline{V} = U \cup K(x_1) \cup \cdots \cup K(x_n)$$

for some $x_i \in \overline{V} \setminus U$. Thus

$$W := U \setminus \bigcup_{i=1}^{n} K(x_i) = \overline{V} \setminus \bigcup_{i=1}^{n} K(x_i)$$

is both open (intersection between the open sets U and $G \setminus \bigcup_{i=1}^{n} K(x_i)$) and closed (intersection between the closed sets $\overline{V}$ and $G\setminus \bigcup_{i=1}^{n} K(x_i)$) and hence W is a compact open neighbourhood of 1.

It remains to be shown that every compact open neighbourhood K of 1 contains an open subgroup. In other words, we want to find a subset H of K such that $H = H^{-1} = H^2$, where $H^{-1} = \{h^{-1} \mid h \in H\}$ and $H^2 = \{h_1h_2 \mid h_1, h_2 \in H\}$. Let $X = K^2 \setminus K$, as K and hence K^2 are compact we can conclude that X is compact as well. It is clear that $K \subseteq G\setminus X$, where $G \setminus X$ is open.

The next step is to show that there is an open neighbourhood U of 1 such that $KU \subseteq G \setminus X$. Let $\mu : G \times G \to G$ be the continuous map $(a, b) \mapsto ab$. This implies that $\mu^{-1}(G \setminus X)$ is open and thus

$$\mu^{-1}(G \setminus X) = \bigcup A_\alpha \times B_\alpha,$$

where A_α and B_α are open sets. Now $K \times \{1\} \subseteq \mu^{-1}(G \setminus X)$ is compact, so we can find a finite subcover

$$K \times \{1\} \subseteq \bigcup_{i=1}^{n} A_i \times B_i,$$

where for all i we have that $1 \in B_i$. If we now take the set $U = \cap_{i=1}^{n} B_i$ we have

$$K \times U = K \times \cap_{i=1}^{n} B_i \subseteq \bigcup_{i=1}^{n} A_i \times B_i \subseteq \mu^{-1}(G \setminus X).$$

This gives $KU \subseteq G \backslash X$. Furthermore, $K(K \cap U) \subseteq (G \backslash X) \cap K^2 \subseteq K$. This is true since $G \backslash X = G \backslash (K^2 \backslash K) = (G \backslash K^2) \cup K$. Now let $V = K \cap U \cap (K \cap U)^{-1}$, which is constructed in such a way to fulfill the condition $V = V^{-1}$. Also $KV \subseteq (G \setminus X) \cap K^2 \subseteq K$. Hence $KV^n \subseteq K$ for all $n \geq 1$. Now let $H = \cup_{i=1}^{\infty} V^i$. Then $H \subseteq K$, $H^{-1} = H = H^2$. Thus H is the wanted open subgroup contained in the set containing 1.

($2 \Rightarrow 3$) This step follows from the above lemma. □

3.2 Pro-p groups

Definition 3.2.1. A *pro-p group* is a profinite group in which every open normal subgroup N has index equal to some power of p.

Similarly to profinite groups it is possible to define pro-p groups using an inverse limit.

Proposition 3.2.2. *A topological group G is a pro-p group if and only if G is isomorphic to the inverse limit of finite p-groups.*

Proof. Every pro-p group G is per definition profinite which means that

$$G \cong \varprojlim (G/N)_{N \triangleleft_o G}.$$

However, since $|G : N| = p^n$ it follows that G/N is a p-group. For the converse, suppose that $G = \varprojlim (G_i)_{i \in I}$, where every G_i is a finite p-group. Then G is profinite and every open subgroup contains a subgroup

$$H(S) = G \cap \left(\prod_{i \notin S} G_i \times \prod_{i \in S} \{1\} \right)$$

for some finite subset S of I. Now the index of $H(S)$ in G divides $\prod_{i \in S} |G_i|$. But since the order of each G_i is a power of p this implies that $|G : H(S)|$ is a power of p as well. Thus, every open subgroup of G has index p. □

3.3 Examples

Profinite groups can be viewed as an extension of finite topological groups and many theorems that apply for finite groups can be generalized to profinite groups. For this reason it is logical that finite groups equipped with the discrete topology are profinite groups as well.

When talking about profinite groups two prominent examples have to be highlighted. Firstly, the group of p-adic integers and secondly the Galois groups. We will briefly introduce both concepts but omit some details. For a more complete picture see [12] and [26] respectively.

Within the usual decimal system we describe a real number r using integer coefficients $0 \leq a_i < 10$ in the power series

$$r = \pm \sum_{i=-\infty}^{n} a_i 10^i,$$

where the series extends from minus infinity to a finite integer n. This is certainly not restricted to using powers of 10. The familiar binary number system and the hexadecimal system come to mind. In general we can write a real number using the equation

$$r = \pm \sum_{i=-\infty}^{n} a_i k^i,$$

where k can be any positive integer and $0 \leq a_i < k$. However, it is also possible to define a power series in such a way that it extends from a certain integer $m \geq 0$ to positive infinity. Those are the p-adic integers $\mathbb{Z}_p$, given that k in this case is a prime. Let s be a p-adic integer then

$$s = \sum_{i=m}^{\infty} a_i p^i,$$

where once again the $0 \leq a_i < p$ are integer coefficients. This series is a formal series which means that we are not interested in the actual value that this series converges to (which in most cases would be infinity). We define a different norm which depends on the divisibility by p. Let s be a p-adic integer and let r be the highest exponent such that p^r divides s. This is equivalent to saying that $s = \sum_{i=r}^{\infty} a_i p^i$. Then the norm equals $|s|_p = p^{-a}$. To conclude this definition we have to define $|0|_p = 0$. Note that a norm immediately defines the metric $d(x, y) = |x - y|_p$.

We can observe that a minus sign is not necessary when using the p-adic numbers. Let us for example say $p = 7$ then in the usual notation we have $1_7 + \ldots 6666_7 = 0_7$, where the numbers extend towards the left, thus, $-1_7 = \ldots 6666_7$. Similarly, we can find for any (positive) p-adic integer a another positive p-adic integer b such that $a + b = 0$.

Let us have look at the finite cyclic groups $\mathbb{Z}/p^n\mathbb{Z}$ together with the homomorphisms $f_{ij} : \mathbb{Z}/p^i\mathbb{Z} \to \mathbb{Z}/p^j\mathbb{Z}$ for $i \geq j$ given by the reduction modulo p^{i-j}. Thus the family of groups $\mathbb{Z}/p^n\mathbb{Z}$ is an inverse system. Taking the inverse limit we get the profinite group

$$G = \varprojlim \mathbb{Z}/p^n\mathbb{Z} = \left\{ \vec{g} \in \prod \mathbb{Z}/p^n\mathbb{Z} \mid g_j = f(g_i) \right\}.$$

Since the groups $\mathbb{Z}/p^n\mathbb{Z}$ are finite p-groups G is in fact a pro-p group. An example for an element of this group given $p = 5$ could be $\vec{g} = (1, 21, 46, \ldots,$ where $1 \equiv 21 \pmod 5$, $21 \equiv 46 \pmod{5^2}$ and so on. In general we have that $\vec{g} = (a_0, a_0 + a_1 p, a_0 + a_1 p + a_2 p^2, \ldots)$. As we can see, this is just a different notation for the p-adic integers, which is why the p-adic integers form a pro-p group. They are not only the most important example of such a group but have historically been the origin of the study of pro-p groups. In addition to forming a pro-p group the p-adic integers form a ring as well. They are an abelian group together with addition and are associative (and also commutative) when it comes to multiplication. The element $\ldots 001$ is the multiplicative identity. Finally, the p-adic integers are also distributive. However, even though many p-adic integers have multiplicative inverses the ones that end in zero obviously do not. Thus the p-adic integers $\mathbb{Z}_p$ are not a field. Below we show the multiplicative inverses of 0002_7 and 0003_5 respectively. One can see those as equivalent to the fractions $1/2$ in the 7-adic numbers and $1/3$ in the 5-adic numbers.

$$\ldots 3334_7 \cdot \ldots 0002_7 = \ldots 0001_7$$
$$\ldots 13132_5 \cdot \ldots 0003_5 = \ldots 0001_5.$$

Secondly every profinite group is a Galois group and vice versa. A Galois group $\mathrm{Gal}(L : K)$ is the group consisting of all the K-automorphisms of a field extension $L : K$. We essentially have two fields $K \subseteq L$ such that the operations of K are the same as the operations of L restricted to K. An example could be the fields $K = \mathbb{Q}$ and $L = \mathbb{R}$. A K-automorphism is an isomorphism $\phi : L \to L$ such that ϕ restricted to K is the identity map. Now let us consider the Galois group $\mathrm{Gal}(F : K)$, where F is an intermediate field, i.e $L \supseteq F \supseteq K$. It is possible that $\mathrm{Gal}(F : K)$ is infinite. However, if we consider all possible finite Galois groups $\mathrm{Gal}(F : K)$, where F is an intermediate field we get an inverse system of finite groups with $i \geq j$ for groups $\mathrm{Gal}(F_i : K)$ and $\mathrm{Gal}(F_j : K)$ if $F_i \supseteq F_j$. The mappings are constructed by restricting the automorphisms, i.e. if $F_i \supseteq F_j$ then the map $f_{ij} : \mathrm{Gal}(F_i : K) \to \mathrm{Gal}(F_j : K)$ is defined by $g \mapsto g|_{F_j}$, the automorphism g restricted to F_j. The inverse limit of such an inverse system is in fact the Galois group $\mathrm{Gal}(L : K)$ together with a certain topology which is called the Krull topology.

Chapter 4

Powerful p-groups

In the following chapters we will use the notation $G^p = \langle g^p \mid g \in G \rangle$ for the subgroup generated by the pth powers of the elements of G.

This Chapter is based on Chapter 2 of [5]. Some of the proofs regarding the Frattini subgroup have been based on Chapter 5 from [24]. In this chapter we will focus our attention on finite p-groups and introduce the concept of a powerful finite p-group. We will see in the next chapter that most of the results that we discuss in this chapter can be transferred to pro-p groups.

Definition 4.0.1. A *powerful p-group G* is a finite p-group, where G/G^p is abelian for $p \neq 2$. The case $p = 2$ is different, here a finite 2-group is powerful if G/G^4 is abelian.

One could also describe a powerful p-group using the commutator subgroup.

Definition 4.0.2. A *powerful p-group G* is a finite p-group, where the commutator subgroup $[G, G]$ is contained in G^p respectively in G^4 for $p = 2$.

We know that the commutator subgroup is the smallest subgroup H such that the quotient group G/H is abelian, it follows immediately that a quotient group G/A is abelian if and only if the subgroup A contains the commutator subgroup. And hence the definitions are equivalent.

Definition 4.0.3. A subgroup N is *powerfully embedded* in a finite p-group G if $[N, G] \leq N^p$ except for $p = 2$, where $[N, G] \leq N^4$ is required.

We can see that G is powerful if and only if G is powerfully embedded in G. Also, if N is powerfully embedded in G it follows that N is powerful as $[N, N] \leq [N, G]$. An important result is that N is normal in G as well.

Proposition 4.0.4. *Let N be powerfully embedded in G. Then N is normal in G.*

Proof. This proposition follows directly from the fact that $[N, G] \leq N^p \leq N$. Thus for elements $n_1, n_2 \in N$ and $g \in G$ we have that $n_1^{-1} g^{-1} n_1 g = n_2$ and thus $g^{-1} n_1 g = n_1 n_2 \in N$. □

It is interesting to ask, why $p = 2$ is treated differently than the odd primes. To understand why this is the case we need a better intuition for the powerful property. We can recognize that this property gives a notion of how small the commutator subgroup is. For abelian groups the commutator subgroup is the trivial subgroup, thus any abelian p-group is powerful. In this sense we can understand powerful p-groups as a generalization of abelian p-groups. In fact, powerful p-groups have many properties of abelian groups.

We can see that $[G, G] \leq G^p$ gives us control over the size of the commutator subgroup for $p \neq 2$. For $p = 2$ however, we get no further information as $[G, G] \leq G^2$ is true for any group. The logical conclusion is therefore to say that a 2-group is powerful if $[G, G] \leq G^4$, such that we still have control over the size of the commutator subgroup.

There are many examples for powerful p-groups since most simple examples of p-groups are abelian and thus powerful. We can also easily find examples of groups such as the dihedral group D_8 or the quaternion group Q_8 that are neither abelian nor powerful. A good example of a p-group for $p \neq 2$ that is neither powerful nor abelian is the Heisenberg group modulo p consisting of all the matrices

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix},$$

where a, b, c are elements of $\mathbb{Z}/p\mathbb{Z}$. For this group one can check that $G^p = 1$ which implies that it is not powerful. Apart from the Heisenberg group there exists another non-abelian group of order p^3 [4] for $p \neq 2$ which turns out to be powerful. This is the group

$$H = \left\{ \begin{pmatrix} 1 + pa & b \\ 0 & 1 \end{pmatrix} \mid a, b \in \mathbb{Z}/p^2\mathbb{Z} \right\}.$$

We leave it to the reader to check that $[H, H] = H^p$ is a cyclic group of order p consisting of the elements $\left\{ \begin{pmatrix} 1 & pb \\ 0 & 1 \end{pmatrix} \mid b \in \mathbb{Z}/p^2\mathbb{Z} \right\}$.

To exemplify the similarity between abelian p-groups and powerful p-groups we will introduce the Frattini subgroup.

Definition 4.0.5. The *Frattini subgroup* $\Phi(G)$ of a group G is the intersection of all maximal subgroups, i.e. all subgroups $H \neq G$ that are not properly contained in any other proper subgroup $K \neq G$.

An important property of the Frattini subgroup and a second definition is the fact that it consists of all the non-generators.

Lemma 4.0.6. *The Frattini subgroup $\Phi(G)$ of a group G is the set of all non-generators, where $g \in G$ is a non-generator if for all $\langle X, g\rangle = G$ it holds that $\langle X\rangle = G$.*

Proof. Let $g \in \Phi(G)$ and suppose that $\langle X, g\rangle = G$ but $\langle X\rangle \neq G$ then g is not in $\langle X\rangle$ and $\langle X\rangle$ is contained in a maximal proper subgroup M. But then $\langle X, g\rangle \subseteq M \leq G$ which is a contradiction. Conversely, let g be a non-generator. And let us assume that there exists a maximal subgroup M that does not contain g. Then $G = \langle M, g\rangle = M$ which is a contradiction. □

Lemma 4.0.7. *The Frattini subgroup of an abelian group is $\Phi(G) = \bigcap G^p$ for all p that divide the order of G.*

Proof. ($\Phi(G) \subseteq \cap G^p$) This statement follows if $\Phi(G) \subseteq G^p$ for all p. If $G^p = G$ the statement is trivial. Otherwise, the group G/G^p is an elementary abelian group which means that each of its elements has the same order p; indeed $(aG^p)^p = a^pG^p = G^p$. This implies that G/G^p is a vector space over the prime field of order p and has a basis. Each subset of this basis missing a single basis element generates a maximal subgroup. This implies that the intersection of the maximal subgroups, $\Phi(G/G^p)$, is trivial. Now let $\overline{M_i}$ be the maximal subgroups of G/G^p and M_i the corresponding maximal subgroups in G. We have $G^p \subseteq M_i \subseteq G$. Since $\cap\overline{M_i} = \{1\}$ we have $\cap M_i = G^p$. Thus $\Phi(G) \subseteq G^p$ and hence $\Phi(G) \subseteq \cap G^p$.

($\Phi(G) \supseteq \cap G^p$) Let $g \in \cap G^p$. We want to show that g is contained in every maximal subgroup M which would prove the statement. Let us assume towards a contradiction that $g \notin M$. Since M is maximal the set $\{M \cup g\}$ generates G and there exists a prime q such that $g^q \in M$. Indeed, if that was not true and the smallest number n such that $g^n \in M$ was a composite number, i.e. $n = qm$, where $q, m > 1$, then the group $\langle\{M \cup g^q\}\rangle$ would be greater than M but would not contain g and thus M would not be maximal. Thus $g^q \in M$ for some prime q. However, since $g \in \cap G^p$ we can find an element h in G such that $g = h^q$. Since $G = \langle\{M \cup g\}\rangle$ we have $h = mg^k$ for $0 < k < q$. Then $g = h^q = m^q g^{kq}$, but $g^q \in M$ and thus $g \in M$ which is a contradiction. □

The logical conclusion is now, that the Frattini subgroup of a powerful p-group G is given by $\Phi(G) = G^p$.

Lemma 4.0.8. *A finite p-group G (with $p \neq 2$) is powerful if and only if $\Phi(G) = G^p$.*

Proof. In Lemma 4.0.15 we will show that for every powerful p-group has the property $\Phi(G) = G^p$. For the reverse direction we want to show that if $\Phi(G) = G^p$ then G is powerful. The commutator subgroup $[G, G]$ of a p-group is contained in every maximal subgroup M and thus in the Frattini subgroup. Indeed, we observe that since M is maximal G/M is cyclic of order p and thus abelian. Hence for $a, b \in G$ we have

$$(a^{-1}b^{-1}ab)M = (a^{-1})M(b^{-1})M(a)M(b)M = M.$$

Thus, every commutator $a^{-1}b^{-1}ab$ is in M and therefore $[G, G] \leq \Phi(G) = G^p$ and G is powerful. □

Lemma 4.0.9. *Let G be a finite p-group and let N, K and W be normal subgroups of G with $N < W$.*

(i) *If N is powerfully embedded in G then NK/K is powerfully embedded in G/K.*

(ii) *If $K \leq N^p$ (respectively $K \leq N^4$) then N is powerfully embedded in G if and only if N/K is powerfully embedded in G/K.*

(iii) *If N is powerfully embedded in G and $x \in G$ then $\langle N, x\rangle$ is powerful.*

(iv) *If N is not powerfully embedded in W, then there exists a normal subgroup J of G such that*

- *for p is odd $N^p[[N, W], W] \leq J < N^p[N, W]$ and $|N^p[N, W] : J| = p$,*
- *for $p = 2$ accordingly $N^4[N, W]^2[N, W, W] \leq J < N^4[N, W]$ and $|N^4[N, W] : J| = 2$.*

Proof. (i) It is helpful to recognize that the elements of NK/K are of the form nK, where $n \in N$. And since $(nK)^p = n^pK$ it follows that $(NK/K)^p = N^pK/K$. We want to show that $[NK/K, G/K] \leq (NK/K)^p$ (respectively $(NK/K)^4$). Observe that $[NK/K, G/K] = [NK, G]K/K$, thus

$$\begin{aligned}[N, G] \leq N^p \Longrightarrow [NK, G] \leq N^pK \Longrightarrow {} & [NK, G]K/K \leq (N^pK)/K \\ \Longrightarrow {} & [NK/K, G/K] \leq (NK/K)^p.\end{aligned}$$

(ii) We have that

$$[N, G] \leq N^p \Longleftrightarrow [N, G]K/K \leq N^p/K \Longleftrightarrow [N/K, G/K] \leq (N/K)^p.$$

(iii) Let us start by verifying the commutator identities $[ab, c] = b^{-1}[a, c]b[b, c]$ and $c^{-1}[a, b]c = [c^{-1}ac, c^{-1}b]$. We have that

$$[ab, c] = b^{-1}a^{-1}c^{-1}abc = b^{-1}a^{-1}c^{-1}acbb^{-1}c^{-1}bc = b[a, c]b^{-1}[b, c]$$

and

$$c^{-1}[a, b]c = c^{-1}a^{-1}b^{-1}abc = c^{-1}a^{-1}cc^{-1}b^{-1}cc^{-1}acc^{-1}bc = [c^{-1}ac, c^{-1}b].$$

Let $H = \langle N, x\rangle$. Since N is normal in G it follows that N is normal in H. Thus for $n_1 \in N$ we have that $xn_1x^{-1} = n_2 \in N$. Hence $xn_1 = n_2x$, which implies that each element h in H can be written as $h = nx^s$ for some integer s. Hence for elements $h_1 = n_1x^b$ and $h_2 = n_2x^a$ of H we can write

$$[h_1, h_2] = [n_1x^a, n_2x^b] = x^{-a}[n_1, h_2]x^a[x^a, n_2x^b].$$

Since $x^{-a}[n_1, h_2]x^a = [x^{-a}n_1x^a, x^{-a}h_2x^a]$ and N is normal in H it follows that $x^{-a}[n_1, h_2]x^a \in [H, H]$. Furthermore, $[x^a, n_2x^b] = [n_2x^b, x^a]^{-1}$ and $[n_2x^b, x^a] = x^{-b}[n_2, x^a]x^b[x^b, x^a] = [x^{-b}n_2x^b, x^a]$ which implies that due to normality $[x^a, n_2x^b]$ and therefore $[h_1, h_2]$ as well are in $[N, H]$. Thus $[N, H] = [H, H]$. Therefore $[H, H] = [N, H] \le [N, G] \le N^p \le H^p$.

(iv) Since N is not powerfully embedded in W we know that $[N, W]$ is not contained in N^p, thus $N^p < N^p[N, W]$. Let $M = N^p[N, W]$, since N and W are normal we conclude that N^p and M are normal as well. The group G/N^p has a normal subgroup J such that $|M/J| = p$ (Lemma 2.1.17) and $N^p \le J$. Thus M/J is in the centre of G/J (Lemma 2.1.16), hence

$$N^p[[N, W], W]J/J = N^p[[N, W]J/J, WJ/J] = N^pJ/J = J/J$$

since all the elements in $[N, W]J/J$ and G/J commute and N^p is contained in J. The case $p = 2$ allows a similar argument and is left to the reader. □

Proposition 4.0.10. *Let h and g be elements of a group G and n a positive integer. Then*

$$[h^n, g] = h^{-(n-1)}[h, g]h^{n-1}h^{-(n-2)}[h, g]h^{n-2} \cdots [h, g].$$

Proof. We have that

$$\begin{aligned} h^{-(n-1)}[h, g]h^{n-1}h^{-(n-2)}[h, g]h^{n-2} \cdots [h, g] &= h^{-(n-1)}[h, g]h[h, g]h^{n-2} \cdots [h, g] \\ &= h^{-n}g^{-1}hgh[h, g]h^{n-2} \cdots [h, g] \\ &= h^{-n}g^{-1}h^2gh^{n-2} \cdots [h, g] \\ &= h^{-n}g^{-1}h^ng = [h^n, g]. \end{aligned}$$ □

Theorem 4.0.11. *Let G be a finite p-group and $N < G$. If N is powerfully embedded in G then N^p is powerfully embedded in G.*

Proof. We will show this for $p \neq 2$. The case $p = 2$ can be constructed in a similar manner. Since N is powerfully embedded in G it is given that $[N, G] \leq N^p$. Furthermore, N and thus N^p are normal in G which implies that $J = (N^p)^p[N^p, G, G]$ is normal in G as well. Let us define a new G and N^p. We will now show that $N^p := N^p/J$ is powerfully embedded in $G := G/J$ and thus the result follows. In this case $(N^p)^p = [N^p, G, G] = 1$. Thus $[N^p, G]$ is in the centre and $[N, G, G] \leq [N^p, G] \leq Z(G)$. For any given $n \in N$ and $g \in G$ we can construct the homomorphism $x \mapsto [n, g, x]$ from G into $Z(G)$. We have that

$$\prod_{j=1}^{p-1}[n, g, n^j] = \prod_{j=1}^{p-1}[n, g, n]^j = [n, g, n]^{p(p-1)/2} = 1,$$

since

$$\begin{aligned}
[n, g, n]^j &= ((g^{-1}n^{-1}gn)n^{-1}(n^{-1}g^{-1}ng)n)^j \\
&= (g^{-1}n^{-1}gn)n^{-1}(n^{-1}g^{-1}ng)((g^{-1}n^{-1}gn)n^{-1}(n^{-1}g^{-1}ng)n)n \\
&\quad \cdot ((g^{-1}n^{-1}gn)n^{-1}(n^{-1}g^{-1}ng)n)^{j-2} \\
&= (g^{-1}n^{-1}gn)n^{-2}(n^{-1}g^{-1}ng)n^2((g^{-1}n^{-1}gn)n^{-1}(n^{-1}g^{-1}ng)n)^{j-2} \\
&= (g^{-1}n^{-1}gn)n^{-j}(n^{-1}g^{-1}ng)n^j = [n^{-1}g^{-1}ng, n^j] = [n, g, n^j].
\end{aligned}$$

Hence

$$\begin{aligned}
[n^p, g] &= n^{-(p-1)}[n, g]n^{p-1}n^{-(p-2)}[n, g]n^{p-2} \cdots [n, g] = \prod_{j=0}^{p-1}[n, g][n, g, n^j] \\
&= [n, g]^p \prod_{j=0}^{p-1}[n, g, n^j] \qquad \text{since } [n, g, n^j] \text{ is in the centre} \\
&= [n, g]^p[n, g, n]^{p(p-1)/2} = [n, g]^p.
\end{aligned}$$

Thus $[N^p, G] = [N, G]^p \leq (N^p)^p = 1$. Returning to the original notation and using the fact that $[N^p, G, G] \leq (N^p)^p$ we get that $[N^p, G]J/J \leq (N^p)^p/J = 1$ implies that $[N^p, G] \leq (N^p)^p$ and thus N^p is powerfully embedded in G. □

Lemma 4.0.12. *Let G be a finite p-group then $\Phi(G) = G^p[G, G]$.*

Proof. For any maximal subgroup M we know that $|G : M| = p$ and $M \lhd G$ which implies that G/M is cyclic and thus abelian. Therefore $[G, G] \leq M$.

Furthermore, since G/M is cyclic of order p we have that $G^p \leq M$. Thus $\Phi(G) \geq G^p[G,G]$. Conversely, the group $G/G^p[G,G]$ is abelian and has exponent p and thus $\Phi(G/G^p[G,G]) = 1$. Let $H \lhd G$ and $H \leq \Phi(G)$. Since H is normal in all maximal subgroups of G we can conclude that for a maximal subgroup M of G the quotient group M/H is a maximal subgroup in G/H. Thus, $\Phi(G/H) = \Phi(G)/H$. Now let $H = G^p[G,G]$ then $1 = \Phi(G/G^p[G,G]) = \Phi(G)/G^p[G,G]$ which implies that $\Phi(G) = G^p[G,G]$. □

For the next lemma we need to prove a rather technical proposition.

Proposition 4.0.13. *Let G be a group and let $[G,G] \leq Z(G)$ then*

$$(xy)^n = x^n y^n [y,x]^{n(n-1)/2}.$$

Proof. We prove this by induction on n. Since $[G,G] \leq Z(G)$ we can change the position of $[x,y]$. The case $n = 1$ is clear. We want to show that if $(xy)^n = x^n y^n [y,x]^{n(n-1)/2}$ holds $(xy)^{n+1} = x^{n+1} y^{n+1} [y,x]^{(n+1)n/2}$ is true as well. We observe that

$$(xy)^{n+1} = (xy)^n xy = x^n y^n [y,x]^{n(n-1)/2} xy = x^n y^n [y,x]^{(n+1)n/2} [x,y]^n xy.$$

In other words it suffices to show that $x^n y^n xy[x,y]^n = x^{n+1} y^{n+1}$. We now insert every $[x,y]$ between the x and y such that

$$x^n y^n xy[x,y]^n = x^n y^n x[x,y]y[x,y]^{n-1} = x^n y^n y^{-1} xy^2 [x,y]^{n-1}$$

. Continuing this process by now inserting $[x,y]$ between x and y^2 and so on we get $x^n y^n xy[x,y]^n = x^n y^n y^{-n} xy^{n+1} = x^{n+1} y^{n+1}$. □

Definition 4.0.14. Let G be a finite p-group. We define recursively $P_1(G) = G$ and $P_{i+1}(G) = P_i(G)^p[P_i(G), G]$ for positive integers i. We will shorten the notation to $G_i = P_i(G)$. The series $G \geq G_2 \geq \cdots$ is called the *lower p-series* of G.

Lemma 4.0.15. *Let G be a powerful p-group.*

(i) *Then G_i is powerfully embedded in G and $G_{i+1} = G_i^p = \Phi(G_i)$ for all i.*

(ii) *The map $x \mapsto x^p$ induced a homomorphism from G_i/G_{i+1} to G_{i+1}/G_{i+2} for all i.*

Proof. (i) We will prove this by induction. Firstly, it is clear that $G_1 = G$ is powerfully embedded in G. Suppose that G_i is powerfully embedded in G, then $[G_i, G] \leq G_i^p$. Thus $G_{i+1} = G_i^p[G_i, G] = G_i^p$. Since G_i is powerfully embedded it follows that $G_{i+1} = G_i^p$ is powerfully embedded as well (Theorem

4.0.11). Since $G_i^p[G_i, G_i] = \Phi(G_i)$ we have that $G_i^p \leq \Phi(G_i) = G_i^p[G_i, G_i] \leq G_{i+1}$, where the last inequality follows because $[G_i, G_i] \leq [G_i, G]$. However, since $G_i^p = G_{i+1}$ we can conclude that $G_{i+1} = \Phi(G_i)$.

(ii) From part (i) we use that $G_{i+1} = G_i^p = \Phi(G_i)$. Since every G_i is powerful and $P_k(G_i) = G_{i+k-1}$ we can just look at the group G_i and set $G_1 = G := G_i$. Furthermore, we have that G/G_3 is powerful as well and if we let $G := G/G_3$ then $G_3 = 1$. We have that $[G_2, G] \leq G_3 = 1$ which implies that G_2 is in the centre. Thus $[G, G] \leq G_2 \leq Z(G)$. Now the previous proposition shows that for $x, y \in G$ we have $(xy)^p = x^p y^p [y, x]^{p(p-1)/2}$. If $p \neq 2$ then p divides $p(p-1)/2$ and thus $[y, x]^{p(p-1)/2} \in G_2^p = G_3 = 1$. If $p = 2$ we have $[G, G] \leq G^4 \leq (G^2)^2 = G_3 = 1$. So in both cases we have that $(xy)^p = x^p y^p$. In other words the map $x \mapsto x^p$ from G/G_2 to $G_2/G_3 = G_2 = G^p$ is a homomorphism. □

Lemma 4.0.16. *Let $G = \langle a_1, \ldots, a_n \rangle$ be a powerful p-group, then $G^p = \langle a_1^p, \ldots, a_n^p \rangle$.*

Proof. Let $\theta : G/G_2 \to G_2/G_3$ be the homomorphism given by Lemma 4.0.15. We have that $G/G_2 = \langle a_1 G_2, \ldots, a_n G_2 \rangle$ and thus

$$G_2/G_3 = \langle \theta(a_1 G_2), \ldots, \theta(a_n G_2) \rangle = \langle a_1^p G_3, \ldots, a_n^p G_3 \rangle$$

which gives $G_2 = \langle a_1^p, \ldots, a_n^p \rangle G_3$. Now $G_2 = G^p$ and $G_3 = \Phi(G_2)$ and thus $G^p = \langle a_1^p, \ldots, a_n^p \rangle \Phi(G^p)$. As $\Phi(G^p)$ consists of all nongenerators of G^p the set $\{a_1^p, \ldots, a_n^p\}$ needs to generate G^p. □

Lemma 4.0.17. *Let G be a powerful p-group, then each element in G^p is a pth power in G.*

Proof. Let $g \in G^p$, as $x \mapsto x^p$ induces a homomorphism from G/G_2 to G_2/G_3 the coset xG_2 gets mapped to $x^p G_3$ which implies that g can be written as $g = x^p y$, where $x \in G$ and $y \in G_3$. Since G^p is powerfully embedded Lemma 4.0.9 shows that $H = \langle G^p, x \rangle$ is powerful. Also $g \in H^p$ as $g = x^p y$, where $y \in G_3 = (G^p)^p$. If $H = G$ then $G = H = \langle G^p, x \rangle = \langle \Phi(G), x \rangle = \langle x \rangle$ is cyclic, in this case $G^p = \langle x^p \rangle$ and every element is trivially an element of pth power. The cyclic case gives the smallest possible order of G and thus the base case for induction on $|G|$. If $H < G$ then the induction hypothesis gives that g is a pth power in H and thus also in G. □

The following theorem summarizes the results of this section.

Theorem 4.0.18. *Let $G = \langle a_1, \ldots, a_n \rangle$ be a powerful p-group and let $i, k \geq 1$ be integers. Then*

(i) $G_{i+1} = G^{p^i} = \{g^{p^i} | g \in G\} = \langle a_1^{p^i}, \ldots, a_n^{p^i} \rangle$;

(ii) *the map* $x \mapsto x^{p^k}$ *induces a homomorphism from* G_i/G_{i+1} *to* G_{i+k}/G_{i+k+1};

(iii) $G_{i+k} = P_{k+1}(G_i) = G_i^{p^k}$ *and thus* $G_{i+1} = G^{p^i}$.

Proof. (i) From Lemma 4.0.17 it follows by induction that $G_i = \{g^{p^i} \mid g \in G\}$ and similarly Lemma 4.0.16 gives $G_i = \langle a_1^{p^i} \ldots, a_n^{p^i} \rangle$. The first equality follows from (iii).

(ii) We can just repeatedly take the homomorphism from Lemma 4.0.15(ii).

(iii) This result follows from induction as Lemma 4.0.15(i) states that $G_{i+1} = G_i^p$. Also,

$$P_{k+1}(G_i) = G_i^{p^k} = \{g_i^{p^k} \mid g_i \in G_i\} = \{g^{p^{i-1+k}} \mid g \in G\} = G_{i+k}. \qquad \square$$

Corollary 4.0.19. *Let* $G = \langle a_1, \ldots, a_n \rangle$ *be a powerful* p*-group, then* G *is the product of its cyclic subgroups,* $G = \langle a_1 \rangle \cdots \langle a_n \rangle$.

Proof. Let i be maximal such that G_i is not the trivial group, i.e. $G_i > G_{i+1} = 1$. By induction on the order of G we can assume that G/G_i is the product of its cyclic subgroups and thus $G/G_i = \langle a_1 G_i \rangle \cdots \langle a_n G_i \rangle$. Hence, $G = \langle a_1 \rangle \cdots \langle a_n \rangle G_i$. Using Theorem 4.0.18(i) and induction we get $G_i = \langle a_1^{p^{i-1}} \rangle \cdots \langle a_n^{p^{i-1}} \rangle$, where G_i is in the centre of G, since $[G_i, G] \leq G_{i+1} = 1$. Thus all elements of G commute with elements of G_i. Hence

$$G = \langle a_1 \rangle \cdots \langle a_n \rangle G_i = \langle a_1 \rangle \cdots \langle a_n \rangle \langle a_1^{p^{i-1}} \rangle \cdots \langle a_n^{p^{i-1}} \rangle = \langle a_1 \rangle \cdots \langle a_n \rangle. \qquad \square$$

Definition 4.0.20. The *rank* of a group G is the minimal number of elements that can generate G is denoted by $d(G)$. For a finite p-group G we have that $G/\Phi(G)$ has the dimension $d(G)$ as a vector space over the field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \{0, 1, \ldots, p-1\}$.

Theorem 4.0.21. *Let* G *be a powerful* p*-group and* $H \leq G$ *then* $d(H) \leq d(G)$.

Proof. We prove this theorem by induction on the order $|G|$ of G. Let $K = G_2 \cap H$. Since G_2 is powerful and strictly smaller than G we assume by the induction hypothesis that $d(K) \leq d(G_2)$. The map $\theta : G/G_2 \to G_2/G_3$ given by $x \mapsto x^p$ is a surjective homomorphism. Thus the dimension of the kernel of θ as a vector space over the field $\mathbb{F}_p$ is given by $\dim(\ker \theta) = d(G) - d(G_2)$. It follows that $\dim(\ker \theta \cap HG_2/G_2) \leq d(G) - d(G_2)$. For any homomorphism $\phi : V \to W$ we know that $\dim(W) = \dim(\ker \phi) + \dim(\text{Im } \phi)$, where Im ϕ

denotes the image. Applying this to HG_2/G_2 we get that $\dim(HG_2/G_2) = \dim(\ker\theta \cap HG_2/G_2) + \dim(\theta(HG_2/G_2))$. Thus,

$$\dim(HG_2/G_2) - d(G) + d(G_2) \leq \dim(\theta(HG_2/G_2)).$$

Let $e = \dim(HG_2/G_2)$ and let $h_1, \ldots, h_e$ be elements of H such that $HG_2 = \langle h_1, \ldots, h_e \rangle G_2$.

Since $\Phi(K) \leq K^p = (H \cap G_2)^p \leq G_3$ we have that

$$\dim(\langle h_1^p, \ldots, h_e^p \rangle / \Phi(K) \geq \dim(\theta(HG_2/G_2)) \geq d(G_2) - (d(G) - e)$$

and thus

$$\dim(\langle h_1^p, \ldots, h_e^p \rangle / \Phi(K) + (d(G) - e) \geq d(G_2).$$

Since $d(K) \leq d(G_2)$ there exists $s = d(G) - e$ elements $y_1, \ldots, y_s$ of K such that

$$K = \langle h_1^p, \ldots, h_e^p, y_1, \ldots, y_s \rangle \Phi(K).$$

Since the Frattini subgroup is the group of all nongenerators it follows that $K = \langle h_1^p, \ldots, h_e^p, y_1, \ldots, y_s \rangle$. We can conclude that

$$H = H \cap HG_2 = H \cap \langle h_1, \ldots, h_e \rangle G_2 = \langle h_1, \ldots, h_e \rangle K = \langle h_1, \ldots, h_e, y_1, \ldots, y_s \rangle.$$

Thus $d(H) \leq d(G)$. □

Definition 4.0.22. The *subgroup rank* (sometimes also just referred to as the rank) of a finite group G is defined as

$$rk(G) = \sup\{d(H) \mid H \leq G\}.$$

Thus the subgroup rank is the maximum of the ranks of all the subgroups of G.

It might be confusing that there are two different definitions for the rank of a group. The reason is that the subgroup rank has the useful property that the subgroups of a group G can never have a greater subgroup rank than G itself. If we just consider the cardinality of the minimal generating set it is possible that the rank of a subgroup of G is indeed greater than the rank of G.

Let us consider the free group G generated by two elements a and b, in other words, the group containing all distinct words that can be construct using a, b, a^{-1} and b^{-1}. The identity element is the empty word, with no letters. Let us take the subgroup H generated by the set $\{a^n b^n\}$, where n is in $\mathbb{N}$. We can see that for $\ell \neq k$ the subgroup generated by $\{a^\ell b^\ell\}$ does not contain $a^k b^k$ which implies that H is infinitely generated.

Chapter 5

Powerful pro-p groups and p-adic analytic groups

5.1 Powerful pro-p groups

During the last two chapters we have introduced the concepts of a pro-p group and a powerful p-group. Powerful pro-p groups are now defined in the same manner as powerful p-groups applying a slightly altered powerful property to pro-p groups. In most cases, when we apply a result from Chapter 4 to powerful pro-p groups we take into consideration the closure of certain groups.

Definition 5.1.1. A *powerful pro-p group* is a pro-p group, where $G/\overline{G^p}$ (for $p \neq 2$), respectively $G/\overline{G^4}$ (for $p = 2$), is abelian.

Definition 5.1.2. An open subgroup N is *powerfully embedded* in a pro-p group G if $[N, G] \leq \overline{N^p}$, respectively $[N, G] \leq \overline{N^4}$ for $p = 2$.

We can observe that if N is powerfully embedded in G it follows that N is powerful as well.

Lemma 5.1.3 ([5, 3.3 Corollary]). *A topological group G is a powerful pro-p group if and only if G is the inverse limit of an inverse system of powerful finite p-groups in which all the maps are surjective.*

Proof. Let G be a powerful pro-p group. Then G is a pro-p group and thus isomorphic to $\varprojlim G/N$, where N runs over the normal subgroups of G and each G/N is finite. However G is also a powerful p-group and thus all the G/N are powerful p-groups as well since $[G, G] \leq G^p$ implies that $[G/N, G/N] = [G, G]N/N \leq G^pN/N = (G/N)^p$.

Conversely, suppose that G is the inverse limit of powerful finite p-groups G_λ. Then G is a pro-p group and since all the maps are surjective the group G/N for an open normal subgroup N is isomorphic to a quotient group G_λ/K of some G_λ and thus G/N is powerful (Lemma 4.0.9). Since all G/N are powerful we conclude that G is powerful as well. This is true since $[G,G]N/N = [G/N, G/N] \leq (G/N)^p = G^pN/N$ implies that $[G,G] \leq \cap G^pN = \overline{G^p}$. □

The above theorem explains why powerful pro-p groups are very similar to finite powerful p-groups. This similarity is especially relevant concerning the results connected to the lower p-series and the minimal generating set.

The most important results that are analogous to Chapter 4 are listed below for completeness but we will not prove them. For further detail we refer the reader to Chapter 3.1 in [5]. The following theorems are analogous to Theorem 4.0.18, to Corollary 4.0.19 and to Theorem 4.0.21.

Theorem 5.1.4. *Let $G = \overline{\langle a_1, \ldots, a_n\ \rangle}$ be a finitely generated powerful pro-p group and let $i, k \geq 1$ be integers. Then*

(i) $G_{i+1} = G^{p^i} = \{g^{p^i} | g \in G\} = \overline{\langle a_1^{p^i}, \ldots, a_n^{p^i} \rangle}$;

(ii) *the map $x \mapsto x^{p^k}$ induces a homomorphism from G_i/G_{i+1} to G_{i+k}/G_{i+k+1};*

(iii) $G_{i+k} = P_{k+1}(G_i) = G_i^{p^k}$ *and in particular* $G_{i+1} = \Phi(G_i)$.

Proposition 5.1.5. *If $G = \overline{\langle a_1, \ldots, a_n \rangle}$ is a powerful pro-p group, then $G = \overline{\langle a_1 \rangle} \ldots \overline{\langle a_n \rangle}$.*

Theorem 5.1.6. *Let G be a powerful finitely generated pro-p group and H a closed subgroup. Then $d(H) < d(G)$.*

5.2 Uniform groups

In Chapter 4 we introduced the concept of a powerful p-group and the similarities that arise between abelian p-groups and powerful p-group. For pro-p groups it is possible to define a slightly stronger condition, the "uniformly powerful" pro-p groups or simply "uniform" groups. In fact it can be shown that one can construct a homeomorphism between any uniform group and $\mathbb{Z}_p^n$, a finitely generated $\mathbb{Z}_p$ module, where $\mathbb{Z}_p$ is the group of the p-adic integers. A module is a generalization of the notion of vector space in which the underlying field is replaced by a ring. In other words it is an algebraic object that represents n copies of $\mathbb{Z}_p$.

Definition 5.2.1 ([5, 4.1 Definition]). A pro-p group G is *uniformly powerful* (or *uniform*) if

(i) G is finitely generated,

(ii) G is powerful,

(iii) $|P_i(G) : P_{i+1}(G)| = |G : P_2(G)|$ for all i.

The third condition could be phrased differently since we already know that there exists a surjective homomorphism $f_i : P_i(G)/P_{i+1} \to P_{i+1}(G)/P_{i+2}$ given by $x \mapsto x^p$. Thus the third condition is fulfilled if and only if all homomorphisms f_i are isomorphisms.

It turns out the group of the p-adic integers is not only a pro-p group but a uniform group as well. Let us check that this is indeed the case. Let G be the group of the p-adic integers. Then G is indeed finitely generated since, similarly to the usual integers, 1 is a generator. Furthermore, G is not only powerful but also abelian. And lastly, since G is powerful we have that $P_i(G) = G^{p^i}$. In other words, all coefficients are shifted i positions to the left and $P_i(G)$ is a copy of G. Hence $|P_i(G) : P_{i+1}(G)| = |G : P_2(G)|$ is true as well.

Similarly, finite direct products of the p-adic integers are uniform as well.

5.3 p-adic analytic pro-p groups

The study of p-adic analytic pro-p groups has been useful for proving or disproving long-standing conjectures. An integral part of the research that has been conducted towards the better understanding is the search for equivalent descriptions of p-adic analytic pro-p groups. Several equivalent definitions have been found. In this section we will introduce three such definitions, another hypothesised characterization and inspect a conjecture that has been disproved using p-adic analytic pro-p groups.

5.3.1 Definitions and examples

We will start with two standard definitions.

Definition 5.3.1 (compare [5, Interlude A]). A *p-adic analytic pro-p group* is a pro-p group of finite subgroup rank.

Definition 5.3.2 (compare [5, Corollary 8.34]). A *p-adic analytic pro-p group* is a pro-p group that contains an open normal uniform subgroup of finite index.

We may construct a p-adic analytic pro-p group considering the second definition. Let us consider a uniform group G. Now the direct product between G and a finite p-group G_f is a p-adic analytic pro-p group. The group G_f needs to be finite but it can be abelian or not abelian. If G_f is not powerful then $G \otimes G_f$ is p-adic analytic but not uniform.

5.3.2 p-adic analytic manifolds

An interesting property of p-adic analytic pro-p groups is their close relation to manifolds and analytic functions. We will just briefly mention this concept without going into detail and refer the reader to Chapter 8.1 of [5] for further reference as well as the Appendix.

Intuitively one can understand analytic functions as smooth functions, i.e. functions that have a convergent Taylor series at every point. We recall that $\mathbb{Z}_p^n$ is a module over the ring of the p-adic integers. We now define a certain structure on a topological space X for open sets U consisting of triples (U, ϕ, n), where ϕ is a homeomorphism from U onto an open subset of $\mathbb{Z}_p^n$ for some positive integer n. These triples need to cover X and the maps $\phi_1 \circ \phi_2^{-1}$ need to be analytic functions for any two ϕ_1, ϕ_2. Simplifying we can say that if we can define such structures on X then it is a p-adic manifold. Furthermore, a pro-p group that is a p-adic analytic manifold is a p-adic analytic pro-p group.

5.3.3 The Hausdorff spectrum of p-adic analytic pro-p groups

When it comes to p-adic analytic pro-p groups the concept of Hausdorff dimension has been of particular interest. This concept is usually known from fractal geometry and generalizes the idea of the dimension of geometric objects to non-integer dimensions. It is defined on a metric space X using the concept of an outer measure which might be known from the definition of the Lebesgue integral. However, it is not necessary to understand the underlying concepts of measure theory to understand the definition of the Hausdorff dimension which is why we will not introduce the concept of an outer measure.

Definition 5.3.3. Let (X, ρ) be a metric space and $S \subseteq X$. Let $\operatorname{diam} U := \sup\{\rho(x, y) \mid x, y \in U\}$ be the diameter of a set U. Let $d \geq 0$ be a real number. The *d-dimensional Hausdorff measure* of the set S is defined as

$$\mathcal{H}^d(S) = \varliminf_{\delta \to 0} \left\{ \sum_{i=1}^{\infty} \operatorname{diam} U_i \mid \cup_{i=1}^{\infty} U_i \supseteq S, \quad \operatorname{diam} U_i < \delta \right\}.$$

Thus, in a certain sense we are looking for the smallest countable cover of S, where the sizes of the elements U_i of the cover tends towards zero.

Definition 5.3.4. The *Hausdorff dimension* $\operatorname{hdim}(S)$ of S is defined as

$$\operatorname{hdim}(S) := \inf\{d \geq 0 \mid \mathcal{H}^d(S) = 0\}.$$

The next step is to apply the concept of Hausdorff dimension to profinite groups. In other word we need to find a metric such that a profinite group is a metric space. This metric is given by

$$d(x, y) = \inf\{|G : G_n|^{-1} \mid xy^{-1} \in G_n\},$$

where the G_n for n being a natural number are a filtration, i.e. a descending chain of normal finite-index subgroups with $\cap G_n = 1$. The natural choice of such a filtration for finitely generated pro-p groups is the p-power series given by $G_n = G^{p^n}$ (another possibility is the lower p-series given by Definition 4.0.14). It has been shown [1] that for a closed subgroup H of G the Hausdorff dimension can be expressed in a simpler way,

$$\operatorname{hdim}(H) = \liminf_{n \to \infty} \frac{\log |HG_n/G_n|}{\log |G/G_n|}.$$

We now present a small part of a recently published paper [17]. The hypothesis is that the order of the Hausdorff spectrum

$$\operatorname{hspec}(G) = \{\operatorname{hdim}(H) \mid H \leq G, H \text{ is closed}\} \subseteq [0, 1]$$

of a finitely generated pro-p group G is finite if and only if G is p-adic analytic. The Hausdorff spectrum of p-adic analytic pro-p groups is well understood, it consists of finitely many rational numbers [2]. Conversely, it is still an open problem if for a finitely generated pro-p group G a finite Hausdorff spectrum implies that G is p-adic analytic. In [17] it has been shown that this is the case under the condition that G is solvable, i.e. that the series $G \triangleright G^{(1)} \triangleright G^{(2)} \triangleright \cdots$ reaches the trivial subgroup. Here $G^{(i+1)} = [G^{(i)}, G^{(i)}]$ is defined recursively.

5.3.4 Automorphism conjecture

The conjecture we will briefly introduce claims that the order of a non-abelian finite p-group G divides the order of the automorphism group $\operatorname{Aut}(G)$ of G. It has been shown that this is the case for p-groups of order p^7 or smaller [10]. However, this is not true in general. In fact the conjecture mentioned above was disproved using p-adic analytic pro-p groups [11]. The key is to construct an infinite uniform group U such in a certain sense U is greater than its automorphism group. As we have seen in this thesis, U can be written as the inverse limit $U = \varprojlim U_i$ of finite p-groups. At the same time $\mathrm{Aut}(U) = \varprojlim \mathrm{Aut}(U_i)$. This suggests that for sufficiently large i the finite p-group U_i could be greater than $\mathrm{Aut}(U_i)$. In [11] it was shown that this is indeed the case an thus the conjecture was disproved.

Chapter 6

Conclusion and Outlook

The p-adic analytic pro-p groups are a useful tool in understanding pro-p groups. In this thesis we have built up to the definition of p-adic analytic pro-p groups by generalizing the concept of finiteness to profiniteness and the concept of abelian p-groups to powerful p-groups. The research into p-groups, pro-p groups and p-adic analytic pro-p groups is extensive and we have just scratched the surface. For instance, the classification of these groups is an integral step towards a better understanding of them and could be part of a more complete introduction to p-adic analytic pro-p groups. One classification of p-groups and pro-p uses the coclass conjecture [6]. Additionally, solvability and p-adic analytic groups can be used to classify just infinite pro-p groups, and furthermore there are links between pro-p groups and Lie groups [16].

Appendix A

Definitions p-adic manifold

Definition A.0.1. Let X be a topological space and U a non-empty open subset of X. A triple (U, ϕ, n) is a *chart* of dimension n on X if ϕ is a homeomorphism from U onto an open subset of $\mathbb{Z}_p^n$ for some positive integer n.

Definition A.0.2. Two charts (U, ϕ, n) and (V, ψ, m) on a topological space X are *compatible* if the maps $\psi \circ \phi^{-1}$ and $\phi \circ \psi^{-1}$ are analytic functions on $\phi(U \cap V)$ and $\psi(U \cap V)$ respectively.

Definition A.0.3. An *atlas* on a topological space X is a set of pairwise compatible charts that covers X.

Definition A.0.4. Two atlases A and B are *compatible* if every chart in A is compatible with every chart in B.

Definition A.0.5 (compare [5, Definition 8.8])**.** Let X be a topological space. A p-adic analytic manifold structure on X is an equivalence class of compatible atlases on X. If such a structure exists, X is a p-adic analytic manifold.

Now we are able give another definition of a p-adic analytic pro-p groups.

Definition A.0.6. A *p-adic analytic pro-p group* is a p-adic analytic manifold which is also a group.

Bibliography

[1] A. G. Abercrombie, "Subgroups and subrings of profinite rings," in *Mathematical Proceedings of the Cambridge Philosophical Society*, vol. 116, no. 2. Cambridge University Press, 1994, pp. 209–222.

[2] Y. Barnea and A. Shalev, "Hausdorff dimension, pro- groups, and kac-moody algebras," *Transactions of the American Mathematical Society*, vol. 349, no. 12, pp. 5073–5091, 1997.

[3] P. B. Bhattacharya, S. K. Jain, and S. Nagpaul, *Basic abstract algebra.* Cambridge University Press, 1994.

[4] K. Conrad, "Groups of order p^3," *Expository papers on group theory*, 2014.

[5] J. D. Dixon, M. P. Du Sautoy, A. Mann, and D. Segal, *Analytic pro-p groups.* Cambridge University Press, 2003, no. 61.

[6] M. Du Sautoy, D. Segal, and A. Shalev, *New horizons in pro-p groups.* Springer Science & Business Media, 2012, vol. 184.

[7] L. Euler, "Theorematum quorundam ad numeros primos spectantium demonstratio," 1736.

[8] M. Fréchet, "Sur quelques points du calcul fonctionnel," *Rendiconti del Circolo Matematico di Palermo*, vol. 22, no. 1, 1906.

[9] E. Galois, "Articles publiés par galois dans les annales de mathématiques de m. gergonne: Demonstration d'un theorème sur les fractions continues périodiques'," *J. Math. Pures App*, vol. 11, pp. 385–394, 1846.

[10] N. Gavioli, "The number of automorphisms of groups of order p^7," in *Proceedings of the Royal Irish Academy. Section A: Mathematical and Physical Sciences.* JSTOR, 1993, pp. 177–184.

[11] J. Gonzalez-Sanchez and A. Jaikin-Zapirain, "Finite groups with small automorphism group," in *Forum of Mathematics, Sigma*, vol. 3. Cambridge University Press, 2015, p. e7.

[12] F. Q. Gouvêa, *p-adic Numbers.* Springer, 1997.

[13] A. Haar, "Der Massbegriff in der Theorie der kontinuierlichen Gruppen," *Annals of mathematics*, vol. 34, no. 1, pp. 147–169, 1933.

[14] F. Hausdorff, *Gestufte Räume.* Springer, 2008.

[15] C. Jordan, *Traite des substitutions et des equations algebriques par m. Camille Jordan.* Gauthier-Villars, 1870, vol. 1.

[16] B. Klopsch, "On the lie theory of p-adic analytic groups," *Mathematische Zeitschrift*, vol. 249, pp. 713–730, 2005.

[17] B. Klopsch, A. Thillaisundaram, and A. Zugadi-Reizabal, "Hausdorff dimensions in p-adic analytic groups," *Israel Journal of Mathematics*, vol. 231, pp. 1–23, 2019.

[18] M. H. Krieger, "A 1940 letter of andré weil on analogy in mathematics," *Notices of the AMS*, vol. 52, no. 3, 2005.

[19] J. Lagrange, "Réflexions sur la résolution algébrique des équations," *Nouveaux Mémoires de l'Académie Royale des Sciences et Belles-Lettres de Berlin*, 1770.

[20] C. R. Leedham-Green and S. McKay, *The structure of groups of prime power order.* Clarendon Press, 2002, no. 27.

[21] S. Lie, *Theorie der transformationsgruppen.* BG Teubner, 1888-1893, vol. 1-3.

[22] J. R. Munkres, *Topology.* Prentice Hall, 2000.

[23] H. Poincaré, *Analysis situs.* Gauthier-Villars Paris, France, 1895.

[24] J. J. Rotman, *An introduction to the theory of groups.* Springer Science & Business Media, 2012, vol. 148.

[25] J.-P. Serre, *Cohomologie galoisienne.* Springer Science & Business Media, 1994, vol. 5.

[26] I. Stewart, *Galois theory.* CRC press, 2022.

[27] J. Tate, “Duality theorems in galois cohomology over number fields,” in *Proc. Internat. Congr. Mathematicians (Stockholm, 1962)*, 1962, pp. 288–295.

[28] M. Vaughan-Lee, *The restricted Burnside problem.* Oxford University Press, 1993.

Bachelor’s Theses in Mathematical Sciences 2023:K14
ISSN 1654-6229

LUNFMA-4144-2023

Mathematics
Centre for Mathematical Sciences
Lund University
Box 118, SE-221 00 Lund, Sweden

http://www.maths.lu.se/