Università di Pisa

Dipartimento di Matematica

Corso di Laurea in Matematica

Embedding Problems and Iwasawa's Theorem

Relatore
Prof. Tamás Szamuely

Candidato
Cristofer Villani

Anno Accademico
2020/2021

Introduction

One of the major open problems in field theory is the inverse Galois problem, concerning whether or not finite groups can be realized as Galois groups of suitable extensions of a given field.

The main focus of this thesis is given by *embedding problems*, that generalize the inverse Galois problem as follows. Given a tower of Galois extensions $E \supset F \supset k$, with G, B the Galois groups of E, F over k respectively, we may consider an epimorphism $\alpha : A \twoheadrightarrow B$ where A is a profinite group and discuss the existence of an intermediate field $E \supset M \supset K$ such that $G(M\,|\,k) = A$ and the restriction homomorphism $G(M\,|\,k) \twoheadrightarrow G(F\,|\,k)$ is exactly α. Via Galois correspondence, this translates to the problem of finding, for a diagram

$$\begin{tikzcd}
 & & & G \arrow[d, "\varphi"] & \\
1 \arrow[r] & K \arrow[r] & A \arrow[r, "\alpha"] & B \arrow[r] & 1
\end{tikzcd}$$

of profinite groups where the row is exact, a surjective homomorphism $\psi : G \twoheadrightarrow A$ that makes the diagram commute. We study the above problem (*strong* embedding problem) for diagrams of pro-$\mathfrak{c}$-groups, i.e. inverse limits of finite groups belonging to a fixed class $\mathfrak{c}$. We also deal with a relaxed version (*weak* embedding problem) in which we do not require surjectivity for the map ψ. Furthermore, we apply the results of our discussion to proving a theorem by K. Iwasawa about the arithmetic of global fields.

The thesis is structured as follows. The first two chapters constitute an introduction to the theory of profinite groups.

In chapter 1, we discuss the topology of these groups and show how many algebraic properties of finite groups, such as the existence of p-Sylows or the structure of the Frattini quotient for p-groups, have their profinite analogues. Moreover, we introduce special sets of generators for a profinite group G, and link their cardinality to the topological structure of G and the existence of specific chains of suhgroups of G. In our exposition, we follow Chapters 1-2 of [RZ10].

In chapter 2, we introduce cohomology groups $H^n(G, A)$, for a profinite group G and a discrete G-module A, and highlight their main functorial features; we also examine how cohomology behaves with respect to subgroups and quotients, and study a fundamental invariant associated to a profinite group, namely its *cohomological dimension*. Our presentation is mainly based on [NSW15], Chapters I-II and [RZ10], Chapters 6-7.

We then employ the tools introduced in the above chapters to the study of embedding problems of pro-$\mathfrak{c}$-groups. Specifically, chapter 3 focuses on strong embedding problems: following [RZ10], Chapter 3, we introduce the concept of *free* pro-$\mathfrak{c}$-groups, and prove that the existence of strong solutions for a fixed group G in all reasonable cases is equivalent to G being, in fact, free.

In chapter 4, we instead link the existence of weak solutions for G to its *projectivity*, and derive a characterization of projective pro-$\mathfrak{c}$-groups in terms of cohomological dimension. We also discuss more closely the case of pro-p-groups, and prove that a pro-p-group is projective if and only if it is free.

Finally, we use the results on embedding problems to prove Iwasawa's theorem about the maximal prosolvable extension $\tilde{K}$ of the maximal abelian extension K of a global field: more specifically, we show that the Galois group $G(\tilde{K}|K)$ is the free prosolvable group of countable rank, so that the inverse Galois problem has a positive answer for K in the case of solvable groups.

Our discussion of projective pro-$\mathfrak{c}$-groups combines the approaches found in [NSW15], Chapter III and [RZ10], Chapter 7, while our proof of Iwasawa's theorem is based on Chapter IX of [NSW15].

Contents

Chapter 1

Pro-$\mathfrak{c}$-groups

Profinite groups are topological inverse limits of discrete finite groups, and if such finite groups belong to a given class $\mathfrak{c}$, we say their inverse limit is a pro-$\mathfrak{c}$-group.

Historically, attention to these classes of topological groups stems from infinite Galois theory: given a Galois extension $L\,|\,k$ of infinite degree, with Galois group $G = G(L\,|\,k)$, one naturally has the identification $G(L\,|\,k) = \varprojlim G(K\,|\,k)$, where K ranges through the finite Galois intermediate extensions $k \subset K \subset L$, and the transition maps $G(K\,|\,k) \to G(K'\,|\,k)$ for $K' \subset K$ are restrictions.

Moreover, the Galois correspondence theorem extends to the infinite case compatibly with the topological structure on G induced by endowing the finite groups $G(K\,|\,k)$ with the discrete topology, in the sense that intermediate extensions $k \subset L' \subset L$ correspond precisely to closed subgroups of G.

Nowadays, the theory of profinite groups has also applications to algebraic geometry (the étale fundamental group of a scheme is profinite) and finite group theory.

In this chapter, we introduce profinite and pro-$\mathfrak{c}$-groups and highlight their main properties, starting with their topological structure.

1.1 Topology of profinite groups

Characterization of profinite groups

We begin by recalling that, for an inverse system of topological spaces X_i (on a directed set of indexes), the inverse limit $X = \varprojlim X_i$ always exists and is given by the set

$$\left\{ (x_i) \in \prod_i X_i \mid f_{ji}(x_j) = x_i \text{ for } j \geqslant i \right\} \subset \prod_i X_i$$

where the $f_{ji} : X_j \to X_i$ are the transition maps. The subset topology coincides with the initial topology induced by the canonical maps $f_i : X \to X_i$ such that $f_i(x) = x_i$ for

$x = (x_i \mid i) \in X$.

The inverse limit G of an inverse system of topological groups G_i is just their topological inverse limit with the operation induced by the inclusion $G \subset \prod_i G_i$.

Lemma 1.1.1. *Suppose* $X = \varprojlim X_i$ *is an inverse limit of nonempty topological spaces, with transition maps* f_{ji}.

i) If the X_i *are Hausdorff,* X *is closed in* $\prod_i X_i$.

ii) If the X_i *are also compact,* X *is nonempty.*

Proof. To prove (i), let $(x_i) \in \prod_{i\in I} X_i \setminus \varprojlim_I X_i$. We can find $i \leqslant j$ in I such that $f_{ji}(x_j) \neq x_i$ and disjoint open neighborhoods $U_i, U_j \subset X_i$ of $x_i, f_{ji}(x_j)$ respectively. By the continuity of f_{ji} there exists an open neighborhood V of x_j such that $f_{ji}(V) \subset U_j$; thus, the set

$$V \times U_i \times \prod_{k\neq i,j} X_k$$

is an open subset of $\prod_{i\in I} X_i \setminus \varprojlim_I X_i$ containing (x_i), and the conclusion follows.

Now assume the X_i are compact Hausdorff. Their product is also compact, and to prove (ii) it is enough to write X as an intersection of closed subsets of $\prod_{i\in I} X_i$ with the finite intersection property.

For all $j \in I$, let

$$Y_j = \left\{ (x_i) \in \prod_{i\in I} X_i \mid \varphi_{jk}(x_j) = (x_k) \text{ for all } k \leqslant j \right\}.$$

Then Y_j is non-empty and, arguing as in (i), we find it is a closed subspace of $\prod_i X_i$. For every choice of indexes $j_1, \dots, j_n$, there exists an index k which is greater than all j_t: therefore

$$\bigcap_{t=1}^{n} Y_{j_t} \supset Y_k \neq \emptyset,$$

which completes the proof of (ii). □

We now proceed to describe inverse limits of *finite discrete* topological groups. We need a preliminary lemma from topology.

Lemma 1.1.2. *If* X *is a compact Hausdorff space, the connected component of a point* $x \in X$ *is the intersection* $I(x)$ *of all clopen (i.e., both closed and open) subspaces of* X *containing* x.

Proof. It is enough to prove that $I = I(x)$ is connected. Consider two disjoint closed subspaces $A, B \subset X$ such that $A \cup B = I$: we must prove that either A or B is empty. Since X is compact Hausdorff, there exist two open subsets $U, V \subset X$ containing A, B respectively such that $U \cap V = \emptyset$.

Then, $X \setminus U \cup V$ is closed and the intersection $I \cap (X \setminus U \cup V)$ is empty: by the finite intersection property of X, there exist finitely many clopen sets $U_1, \dots, U_n$ containing x such that the intersection of $C = U_1 \cap \cdots \cap U_n$ with $X \setminus U \cup V$ is already empty, i.e. $C \subset U \cup V$.

Consider the intersections $C \cap U, C \cap V$: they are both open, and each other's complement in C, so they are also closed. Suppose, without loss of generality, that $C \cap U \ni x$. Then $I \subset C \cap U \subset U$, so that $I(x) \cap B = B = \emptyset$. □

Let us also remark a general fact about compact groups (the proof is straightforward).

Lemma 1.1.3. *If G is a compact topological group, a subgroup $H < G$ is open if and only if it is closed and of finite index.*

For a closed subgroup H of a profinite group G, the *core* of H is the intersection $H_G = \bigcap_{x \in G} H^x$ of its conjugates (we let $H^x = x^{-1}Hx$). Note that H_G is the maximal closed subgroup of H which is normal in G.

Proposition 1.1.4. *For a topological group G, the following are equivalent.*

i) *G is an inverse limit of finite discrete groups.*

ii) *G is compact Hausdorff and totally disconnected.*

iii) *G is compact Hausdorff, and $1 \in G$ has a fundamental system of neighborhoods made of open normal subgroups.*

Proof. Condition (i) implies that G is compact Hausdorff by Lemma 1.1.1. To see that $G = \varprojlim G_i$ is totally disconnected, let x, y be distinct elements of G; by Lemma 1.1.2, it is enough to find a clopen subset of G that separates x from y. Since $x \neq y$, we can find an index i such that $\varphi_i(x) \neq \varphi_i(y)$, with $\varphi_i : G \to G_i$ the canonical map: then $\varphi_i^{-1}(x_i)$ is the wanted clopen.

Now, assume (ii), and consider an open neighborhood $U \neq G$ of $x \in G$. By Lemma 1.1.2, $\{x\}$ equals the intersection $I(x)$ of clopen sets containing x: since $G \setminus U$ is closed and disjoint from $I(x)$, and G is compact, there exist clopen sets $U_1, \dots, U_n$ containing x such that $\bigcap_{i=1}^n U_i \subset U$. Hence, every $x \in G$ has a fundamental system of neighborhoods made of clopens; to prove (iii) we are then left with showing that any of them contains an open normal subgroup, which is done by a standard argument.

Namely, fix a clopen set $U \ni 1$ and let $V = \{v \in U \mid Uv \subset U\}$: we claim that V is open in G. To see this, fix $v \in V$: for all $u \in U$ the product uv belongs to U and, since U is open, we can find open sets U_u, V_u in U, V respectively such that $U_u V_u \subset U$. Because U is also compact, a finite number of the sets U_u, say $U_1, \dots, U_n$, covers U: the intersection V_v of the corresponding $V_1, \dots, V_n$ is an open neighborhood of v in V.

Since the inversion map $x \mapsto x^{-1}$ is a homeomorphism, the set $H = V \cap V^{-1}$ is also open, and we prove that H is in fact a subgroup of G. The only nontrivial check is that, if $x, y \in H$, also $xy \in H$: by definition we have $Uxy \subset Ux \subset U$, so that $xy \in V$, and the same argument shows that $(xy)^{-1} \in V$. Since H is open, it has finite index in G; its core H_G has also finite index, and is therefore an open normal subgroup of G contained in U.

Finally, if G is as in (iii), let $\mathcal{U}$ be the collection of its open normal subgroups. For any $U \in \mathcal{U}$, G/U is a finite discrete group (the cosets xU are open in G for all $x \in G$, multiplication by x being a homeomorphism of G), and we have a continuous homomorphism

$$\varphi : G \to \varprojlim_{\mathcal{U}} G/U$$

induced by the projections $\varphi_U : G \to G/U$. Then φ is injective because G is Hausdorff. In order to prove surjectivity, fix $(x_U) \in \varprojlim_{\mathcal{U}} G/U$: the sets $\varphi_U^{-1}(x_U)$ are nonempty compact Hausdorff subsets of G. Therefore, by Lemma 1.1.1, their inverse limit is nonempty, and any of its elements maps to (x_U) through φ. Consequently, since G is compact and $\varprojlim_{\mathcal{U}} G/U$ is Hausdorff, φ is an isomorphism. □

Definition 1.1.5. *A topological group* G *satisfying the conditions in Proposition 1.1.4 is called a* profinite *group.*

Remark 1.1.6. One has an analogue of Proposition 1.1.4 for topological spaces: namely, a space X is an inverse limit of finite discrete topological spaces if and only if it is compact Hausdorff and is moreover totally disconnected, or equivalently has a basis made of clopen subsets (for a proof, see [RZ10], Theorem 1.1.12). In any of these cases, we say X is a *profinite* space.

Remark 1.1.7. Let $G = \varprojlim_{i \in I} G_i$, where the G_i are compact Hausdorff groups.

i) Suppose $I' \subset I$ is cofinal, i.e. for all $i \in I$ there exists $i' \in I'$ such that $i' \geqslant i$. Then clearly the canonical map $\varprojlim_{i \in I} G_i \to \varprojlim_{i' \in I'} G'_i$ is bijective and hence an isomorphism. Therefore, if necessary, we can pass to a cofinal subset of I without changing the limit.

ii) If $\varphi_i : G \to G_i$ are the projections, we have $\varprojlim G_i = \varprojlim \varphi_i(G)$ via the restrictions of the transition maps. Also, the inverse system formed by the $\varphi_i(G)$ is *surjective*, i.e. the transition maps are epimorphisms: therefore, we may always assume that a profinite group is the limit of a surjective inverse system.

Let us isolate a useful lemma for future reference.

Lemma 1.1.8. *Let* $G = \varprojlim G_i$ *be a profinite group, where the* G_i *are discrete finite groups, and let* $\varphi_i : G \to G_i$ *the canonical maps. The kernels* $\ker(\varphi_i)$ *constitute a fundamental system of neighborhoods of* 1.

Proof. By definition of the topology on G, it is enough to show that any open set of the form

$$G \cap \left(\prod_{j=1}^{s} 1_{i_j} \times \prod_{i \neq i_1, \ldots, i_s} G_i \right),$$

where $1_{i_j} < G_{i_j}$ is the trivial subgroup, contains some $\ker(\varphi_i)$. To do so, pick some $k \geqslant i_1, \ldots, i_n$ and notice that

$$G \cap \left(\prod_{j=1}^{s} 1_{i_j} \times \prod_{i \neq i_1, \ldots, i_s} G_i \right) = G \cap \left(1_k \times \prod_{i \neq k} G_i \right),$$

with the right hand side being precisely $\ker(\varphi_k)$. □

Basic properties of profinite groups

We now proceed to highlight some useful consequences of the above characterization of profinite groups.

The first concerns more generally compact Hausdorff groups. Recall that, as a functor from the category of inverse systems of topological groups to the category of topological groups, $\varprojlim$ is left exact. Namely, suppose

$$1 \to \{A_i, \varphi_{ji}\} \to \{B_i, \psi_{ji}\} \to \{C_i, \chi_{ji}\} \to 1$$

is an exact sequence of inverse systems of topological groups (on the same directed set), i.e for all i there are exact sequences

$$1 \to A_i \to B_i \to C_i \to 1$$

compatible with the transition maps (in the obvious sense) for all $j \geqslant i$; then, the sequence

$$1 \to \varprojlim A_i \to \varprojlim B_i \to \varprojlim C_i$$

is exact. In general, though, $\varprojlim$ is not right exact, as one sees by considering, for example, the epimorphisms $\mathbf{Z} \twoheadrightarrow \mathbf{Z}/p^n\mathbf{Z}$ for all $n \geqslant 0$ and observing that the induced map

$$\mathbf{Z} \to \mathbf{Z}_p = \varprojlim_n \mathbf{Z}/p^n\mathbf{Z}$$

is not surjective (in fact, $\mathbf{Z}_p$ is uncountable, see Remark 1.2.5).

Fortunately, this example gets annihilated if we restrict to the subcategory of (inverse systems of) compact Hausdorff groups.

Proposition 1.1.9. *Suppose* $A = \varprojlim A_i$ *and* $B = \varprojlim B_i$ *are inverse limits of compact Hausdorff groups, and let* $\vartheta_i : A_i \to B_i$ *be compatible epimorphisms. Then the induced map*

$$\varprojlim \vartheta_i : A \to B$$

is again an epimorphism.

Proof. This is again an application of Lemma 1.1.1: consider a sequence $(b_i) \in B$, and note $\vartheta_i^{-1}(b_i) \subset A_i$ is compact for all i. Then, $\varprojlim \vartheta_i^{-1}(b_i) \subset A$ is nonempty, and any of its elements maps to (b_i). □

Corollary 1.1.10. *The functor* $\varprojlim$ *is exact from the category of inverse systems of compact Hausdorff groups to the category of compact Hausdorff groups.*

Corollary 1.1.11. *Let* $G = \varprojlim G_i$ *be a profinite group, where the* G_i *are discrete finite groups, and call* $\varphi_i : G \to G_i$ *the projections. If* $H < G$ *is a closed subgroup,*

$$H = \varprojlim \varphi_i(H).$$

Proof. The map $H \to \varprojlim \varphi_i(H)$ induced by the φ_i is clearly injective, and is surjective by Proposition 1.1.9. Since H is compact, it is a homeomorphism. □

Next, we deal with the existence of factorizations and sections for some suitable maps.

Proposition 1.1.12. *Let* $\{G_i, \varphi_{ji}\}$ *be an inverse system of profinite groups over a directed set* I*, with inverse limit* G*, and suppose* $\rho : G \to H$ *is a continuous homomorphism to a finite discrete group* H*. Then, there exists* $k \in I$ *such that* φ *factors through the projection* $\varphi_k : G \to G_k$*, i.e. the diagram*

$$\begin{tikzcd} G \arrow[r, "\rho"] \arrow[d, "\varphi_k"'] & H \\ G_k \arrow[ur, "\overline{\rho}"'] & \end{tikzcd}$$

commutes, for some suitable continuous homomorphism $\overline{\rho} : G_k \to H$.

Proof. For each index i, write $G_i = \varprojlim_{\mathfrak{U}_i} G_i/U$ where $\mathfrak{U}_i$ is the set of open normal subgroups of G_i and $U \in \mathfrak{U}_i$. Then, if U varies in $\mathfrak{U} = \bigcup_i \mathfrak{U}_i$, the quotients G_i/U can be made into an inverse system of finite groups, with transition maps $G_j/V \to G_i/U$ induced by φ_{ji} any time that $V < \ker(G_j \to G_i \twoheadrightarrow G_i/U)$, and it is apparent that $G = \varprojlim_{\mathfrak{U}} G_i/U$.

According to Proposition 1.1.8, the kernels of the compositions $\varphi_U^{(k)} : G \to G_k \to G_k/U$, with $U \in \mathfrak{U}$, constitute a fundamental system of open neighborhoods of $1 \in G$. Consequently, since $\ker(\rho)$ is open (H being finite), there is some $U \in \mathfrak{U}$ such that $\ker(\varphi_U^{(k)}) < \ker(\rho)$: in particular, $\ker(\varphi_k) < \ker(\rho)$, and the conclusion follows. □

For a map $f : X \to Y$ of topological spaces, we say that $g : Y \to X$ is a *section* for f if it is continuous and $f \circ g$ is the identity map on Y.

Proposition 1.1.13. *Let $H < G$ be a closed normal subgroup of a profinite group G. The projection $\pi : G \to G/H$ admits a section σ (as a map of topological spaces). Moreover, we may assume $\sigma(H) = 1$.*

Proof. We prove the case when H is finite directly, and then use Zorn's lemma for the general case.

Suppose H is a finite normal subgroup of G, and pick an open normal subgroup U intersecting H trivially (consider the intersection of finitely many open normal subgroups $U_h < G$ such that $U_h \not\ni h$, for $h \in H \setminus \{1\}$). The restriction of π to U gives a continuous isomorphism $U \to \pi(U)$, and its inverse $\sigma : \pi(U) \to U$ extends to a continuous map $G/H \to G$ by translation to cosets of $\pi(U)$.

Now, let $H < G$ be a closed normal subgroup, and order the pairs (K, τ) of closed normal subgroups of H and sections of $G/K \to G/H$ by defining $(K, \tau) \leqslant (K', \tau')$ if and only if $K \supset K'$ and τ' is the composition of τ with the projection $G/K' \to G/K$. Then the set of such pairs is non-empty and an ascending chain (K_i, τ_i) is bounded from above by $(\bigcap_i K_i, \bigcup_i \tau_i)$. We may therefore find a maximal pair (M, ξ) and must show $M = 1$.

Suppose this is not the case and pick an open normal subgroup U such that $M \cap U \lneq M$ (choose an element $m \in M$ different from 1 and pick $U \not\ni m$): the projection $G/M \cap U \to G/M$ admits a continuous section by the finite case, since $M/M \cap U$ is a finite subgroup of $G/M \cap U$, and therefore so does $G \to G/M \cap U$ by composition with ξ, a contradiction. □

The last basic property of profinite groups we need concerns closed subgroups.

Proposition 1.1.14. *Let $H < G$ be a closed subgroup of a profinite group G. Then H is the intersection of all open sugroups of G containing H; if H is normal, it is the intersection of all open normal subgroups of G containing it.*

This is an easy consequence of the following technical lemma.

Lemma 1.1.15. *Suppose $\{U_i \mid i \in I\}$ is a set of open subgroups of G filtered from below, i.e. such that for all $i, j \in I$, $U_i \cap U_j \supset U_k$ for some $k \in I$. Then*

$$H\left(\bigcap_i U_i\right) = \bigcap_i HU_i.$$

Proof. It is clear that the result holds if I is finite, and that in general the inclusion

$$H\left(\bigcap_i U_i\right) \subset \bigcap_i HU_i$$

holds. For the reverse inclusion, pick $x \in \bigcup_i HU_i$, and note

$$Hx \cap \bigcap_{j \in J} U_j \neq \emptyset$$

for all finite $J \subset I$ such that $\{U_j \mid j \in J\}$ is filtered from below. Because G is compact, this implies that

$$Hx \cap \bigcap_{i \in I} U_i \neq \emptyset,$$

and the result follows. □

Proof (of Proposition 1.1.14). Suppose $H < G$ is closed: by Lemma 1.1.15, $H = \bigcap_U HU$, if U runs through open normal subgroups of G. If moreover H is normal, and an open subgroup $U < G$ contains H, then its core U_G is open normal in G and $HU_G < U$. □

1.2 Algebraic properties of pro-$\mathfrak{c}$-groups

From now on, subgroups of a profinite groups are always assumed to be closed, and homomorphisms are always assumed to be continuous.

Pro-$\mathfrak{c}$-groups

In what follows, the symbol $\mathfrak{c}$ will always stand for a nonempty class of finite groups, i.e. a collection of finite groups such that any isomorphic image of a group in $\mathfrak{c}$ is still in $\mathfrak{c}$: we say a group contained in $\mathfrak{c}$ is a $\mathfrak{c}$-*group*.

We shall also implicitly assume that $\mathfrak{c}$ be closed under taking subgroups, quotients and finite direct products. If moreover $\mathfrak{c}$ is extension-closed, i.e. for any exact sequence

$$1 \to K \to G \to \overline{G} \to 1$$

such that K and $\overline{G}$ are $\mathfrak{c}$-groups, so is G, we shall call it *full class* of finite groups.

Examples of full classes include all finite, solvable or π-groups for a set of primes $\pi \subset \mathbf{Z}$, while the classes of abelian and nilpotent groups are closed under taking subgroups, quotients and finite products, but are not full classes.

Definition 1.2.1. *A topological group* G *is called a* pro-$\mathfrak{c}$-group *if it can be expressed as*

$$G = \varprojlim G_i,$$

where the G_i *are* $\mathfrak{c}$*-groups.*

When $\mathfrak{c}$ is the full class of finite groups, we get precisely profinite groups; similarly, we shall say a group is *prosolvable, pro-π, proabelian, pronilpotent* when it is a pro-$\mathfrak{c}$-group with $\mathfrak{c}$ being the class of solvable, π-, abelian, nilpotent groups respectively.

Remark 1.2.2. i) If G is a pro-$\mathfrak{c}$-group, so is any subgroup $H < G$ by Corollary 1.1.11. Also, if $U < G$ is an open normal subgroup, then G/U is a $\mathfrak{c}$-group by Lemma 1.1.8, and therefore any quotient of a pro-$\mathfrak{c}$-group is itself pro-$\mathfrak{c}$. By Corollary 1.1.9, if $\mathfrak{c}$ is a full class, any extension of pro-$\mathfrak{c}$-groups is a pro-$\mathfrak{c}$-group.

ii) For an abstract group G, consider the set $\mathcal{N}_\mathfrak{c} = \mathcal{N}_\mathfrak{c}(G)$ of normal finite index subgroups N of G such that the quotient G/N is a $\mathfrak{c}$-group. Then $\{G/N \mid N \in \mathcal{N}_\mathfrak{c}\}$ is made into an inverse system via the projections $\varphi_{MN} : G/M \to G/N$ for $M < N$. Its inverse limit

$$G_{\hat{\mathfrak{c}}} = \varprojlim_{\mathcal{N}_\mathfrak{c}} G/N$$

is a pro-$\mathfrak{c}$-group, called the *pro-$\mathfrak{c}$-completion* of G, and the map

$$G \to G_{\hat{\mathfrak{c}}}$$

induced by the projections $G \to G/H$ is injective if and only if $\bigcap \mathcal{N}_\mathfrak{c} = 1$. The profinite and pro-$\pi$-completions of G are denoted by $\widehat{G}$ and $G_{\hat{\pi}}$ respectively.

iii) For a profinite group G, we instead let

$$G(\mathfrak{c}) = \varprojlim_{\mathcal{U}_\mathfrak{c}} G/U$$

where $\mathcal{U}_\mathfrak{c}$ is the set of *open* normal subgroups U of G such that the quotient G/U is a $\mathfrak{c}$-group. It is plain that $G(\mathfrak{c}) = G/\bigcap \mathcal{U}_\mathfrak{c}$ is the *maximal pro-$\mathfrak{c}$-quotient* of G, that is if $K < G$ is normal and G/K is a pro-$\mathfrak{c}$-group, then $K > \bigcap \mathcal{U}_\mathfrak{c}$.

iv) As a basic example of (ii), note that

$$\mathbf{Z}_{\hat{p}} = \varprojlim_{n} \mathbf{Z}/p^n\mathbf{Z} = \mathbf{Z}_p,$$

and, if $\pi(\mathbb{N})$ is the subset of natural numbers with prime factors in π,

$$\mathbf{Z}_{\hat{\pi}} = \varprojlim_{\pi(\mathbb{N})} \mathbf{Z}/n\mathbf{Z}.$$

Note that, if $n \in \pi(\mathbb{N})$ has prime decomposition $\prod_{p\in\pi} p^{n(p)}$, we have natural epimorphisms $\prod_{p\in\pi} \mathbf{Z}_p \twoheadrightarrow \prod_{p\in\pi} \mathbf{Z}/p^{n(p)}\mathbf{Z} = \mathbf{Z}/n\mathbf{Z}$ giving rise to a homomorphism $\prod_{p\in\pi} \mathbf{Z}_p \to \varprojlim_{n\in\pi(\mathbb{N})} \mathbf{Z}/n\mathbf{Z}$. This map is easily seen to be injective, and is surjective by Proposition 1.1.9; therefore, we have the identification

$$\mathbf{Z}_{\hat{\pi}} = \prod_{p\in\pi} \mathbf{Z}_p.$$

More generally, if $\pi(\mathfrak{c})$ is the set of primes such that $\mathbf{Z}/p\mathbf{Z}$ is a $\mathfrak{c}$-group, the pro-$\mathfrak{c}$-completion of $\mathbf{Z}$ is

$$\mathbf{Z}_{\hat{\mathfrak{c}}} = \prod_{p\in\pi(\mathfrak{c})} \mathbf{Z}_p.$$

Index and Sylow theorems

As a consequence of the exactness of $\varprojlim$ (see Corollary 1.1.9), we can build a profinite analogue for many structures and concepts that are central in finite group theory.

We start with order and index.

Definition 1.2.3. *A* supernatural *number is a formal product*

$$n = \prod_p p^{n(p)}$$

where p *runs through prime numbers in* $\mathbb{N}$ *and* $n(p)$ *is either a natural number or* ∞*.*

For a sequence of supernatural numbers n_i, we can define in a natural way, using prime decomposition, their product, lcm and gcd: namely, the exponent of each prime p is respectively $\sum_i n_i(p)$, $\sup_i n_i(p)$ and $\inf_i n_i(p)$, with the usual conventions about ∞. We also have an obvious notion of divisibility between two supernatural numbers: $n \mid m$ if and only if $n(p) \leqslant m(p)$ for all primes p.

Definition 1.2.4. *For a subgroup* $H < G$ *of a profinite group, the* index *of* H *in* G *is defined as*

$$[G : H] = \text{lcm}\{[G/U : HU/U] \mid U\}$$

where U *runs through the normal open subgroups of* G*. The* order *of* G *is defined as*

$$\#G = \text{lcm}\{|G/U| \mid U\} = [G : 1].$$

Remark 1.2.5. i) Extending the definition of order of a profinite group as its cardinality would be of poor use: as an immediate consequence of Baire's category theorem, an infinite profinite group is always uncountable.

ii) When computing the index $[G : H]$ of a subgroup $H < G$, we can reduce to take the lcm over a fundamental system of neighborhoods of 1 made of open normal subgroups; also, $[G : H]$ is a natural number if and only if H is open.

iii) It is easily checked that indexes are multiplicative, i.e. if $K < H$ are subgroups of G we have $[G : K] = [G : H][H : K]$.

iv) A profinite group G is a pro-π-group for some set of primes π if and only if the prime factors of $\#G$ (i.e. the primes p dividing $\#G$) are in π.

We proceed to prove the profinite version of Sylow theorems.

Definition 1.2.6. *A* p-Sylow *subgroup of a profinite group* G *is a pro-*p*-subgroup* $G_p < G$ *such that* $p \nmid [G : G_p]$.

For a profinite group G, denote by $\mathrm{Syl}_p(G)$ the set of p-Sylows of G.

Theorem 1.2.7. *Let G be a profinite group, p a prime number.*

i) There exists a p-Sylow G_p of G.

ii) Any pro-p-subgroup of G is contained in a conjugate of G_p. In particular, all p-Sylows of G are conjugate.

Proof. To prove (i), write $G = \varprojlim G_i$ as a surjective inverse system of finite discrete groups G_i, and make the sets $S_i = \mathrm{Syl}_p(G_i)$ into an inverse system by noting that the transition maps $\varphi_{ji} : G_j \to G_i$ induce maps $\sigma_{ji} : S_j \to S_i$ such that $\sigma_{ji}(P_j) = \varphi_{ji}(P_i)$. Then,

$$S = \varprojlim S_i \neq \emptyset$$

by Lemma 1.1.1. Let $G_p = \varprojlim P_i$ for some element (P_i) in S: clearly, G_p is a pro-p-group. Also, by Lemma 1.1.8 and Remark 1.2.5,

$$[G : G_p] = \mathrm{lcm}_i[G/U_i : G_pU_i/U_i] = \mathrm{lcm}_i[G_i : P_i],$$

where U_i is the kernel of the canonical map $\varphi_i : G \to G_i$. Therefore, p does not divide $[G : G_p]$, and G_p is the desired p-Sylow.

Now, let $Q = \varprojlim Q_i < G$ be a pro-p-subgroup, where $Q_i = \varphi_i(Q)$. For all i, set $C_i = \{g \in G_i \mid P_i^g \supset Q_i\}$ and again, make the C_i into an inverse system by restricting the φ_{ji} to C_j whenever they are defined, and pick an element $g = (g_i) \in \varprojlim C_i \neq \emptyset$. Then $P^g > Q$ and (ii) is proved. □

The Frattini subgroup

First, we recall some properties of the Frattini subgroup of a finite group G. It is defined as the intersection $\Phi(G)$ of all maximal subgroups of G (since G is finite, they always exist).

A *non-generator* for a finite group G is an element $x \in G$ such that the equation $\langle X, x\rangle = G$ for some subset $X \subset G$ implies $\langle X\rangle = G$.

Proposition 1.2.8. *Let G be a finite group.*

i) (Frattini's argument) *If $K < G$ is a normal subgroup and $P \in \mathrm{Syl}_p(K)$, then $G = KN_G(P)$, where $N_G(P)$ is the normalizer of P in G.*

ii) $\Phi(G)$ is the set of non-generators of G, and if $\Phi(G)K = G$ for some $K < G$, then $K = G$.

iii) $\Phi(G)$ is nilpotent.

Proof. To prove (i), note that both G and K act transitively on $\mathrm{Syl}_p(K)$ by conjugation, so that if $x \in G$ there exists $y \in K$ such that $P^x = P^y$, hence $xy^{-1} \in N_G(P)$.

For (ii), clearly a non-generator x must belong to all maximal subgroups of G, thus $x \in \Phi(G)$; conversely, if $\langle X, x\rangle = G$ but $\langle X\rangle \subsetneq G$ for some $X \subset G$, pick a maximal subgroup $M \supset \langle X\rangle$ and conclude that $x \notin M$. Consequently, if $\Phi(G) = \langle x_1, \dots, x_n\rangle$, and $\Phi(G)K = \langle x_1, \dots, x_n, K\rangle = G$, one concludes by induction on n that $K = G$, since the x_i are non-generators.

Now, take a p-Sylow P of $\Phi(G)$: by (i), $G = \Phi(G)N_G(P)$ (since $\Phi(G)$ is obviously characteristic in G) and therefore $G = N_G(P)$ by (ii). In particular, $\Phi(G)$ has a unique p-Sylow for all p, and is therefore nilpotent. □

Proposition 1.2.9. *Suppose that G is a finite p-group for some prime p.*

i) The Frattini quotient $G/\Phi(G)$ *is elementary abelian.*

ii) $\Phi(G) = 1$ *if and only if G is elementary abelian.*

iii) $\Phi(G) = [G, G]G^p$, *where $[G, G]$ is the commutator subgroup of G and G^p is the subgroup generated by p-th powers.*

Proof. To prove (i), recall that every maximal subgroup of G is normal of index p: therefore, we have a natural surjection $G \twoheadrightarrow \prod_M G/M$ where M ranges through the maximal subgrups of G, whose kernel is $\Phi(G)$. Since the right hand side is a finite product of cyclic groups of order p, (i) follows. Also, if $\Phi(G) = 1$, the above map is an isomorphism, and therefore G itself is elementary abelian; this implies (ii), since clearly the intersection of maximal subgroups in $(\mathbf{Z}/p\mathbf{Z})^n$ is trivial.

Finally, (i) implies that $\Phi(G) > Q = [G, G]G^p$. Conversely, by (ii), $\Phi(G/Q)$ is trivial: thus, if $x \notin Q$ and $\bar{x}$ is its image in G/Q through the canonical projection, there is some maximal $M < G$ such that $\bar{x} \notin M/Q$, which implies $x \notin \Phi(G)$. □

Let now G be a profinite group.

Definition 1.2.10. *The* Frattini subgroup *of G as the intersection $\Phi(G)$ of all maximal subgroups of G.*

The above definition is well posed since a profinite group always has finite index subgroups and, consequently, also maximal (closed) subgroups, that are in fact always open (see Proposition 1.1.14).

Definition 1.2.11. *A subset $X \subset G$ of a profinite group* generates G *if the abstract subgroup generated by X is dense in G, i.e. $\overline{\langle X\rangle} = G$ (where the overline denotes the closure operator).*

Remark 1.2.12. i) By arguing as in the finite case, one proves that $\Phi(G)$ is the set of *nongenerators* of G, i.e. elements $x \in G$ such that any time $X \subset G$ is such that $\overline{\langle X, x\rangle} = G$, already $\overline{\langle X\rangle} = G$.

ii) If $G = \varprojlim G_i$ is a surjective limit of finite groups, it is easily checked that $\Phi(G) = \varprojlim \Phi(G_i)$. As a consequence, $\Phi(G)$ is in fact pronilpotent for a profinite group G.

We shall need the pro-p version of Proposition 1.2.9.

Lemma 1.2.13. *Every maximal subgroup M of a pro-p-group G is normal of index p.*

Proof. Consider the core M_G of M: then M/M_G is normal of index p in G/M_G, and the result follows. □

Proposition 1.2.14. *Let G be a pro-p-group for some prime p.*

i) The Frattini quotient $G/\Phi(G)$ is a direct product of cyclic p-groups.

ii) We have the equality $\Phi(G) = \overline{[G,G]G^p}$

Proof. By Lemma 1.2.13, we may again consider the map $G \to \prod_M G/M$ induced by projections $G \twoheadrightarrow G/M$, where M runs through maximal subgroups of G. Since its kernel is $\Phi(G)$, and it is surjective by Proposition 1.1.9, we get an isomorphism $G/\Phi(G) \simeq \prod_M G/M$.

For statement (ii), we have the inclusion $\Phi(G) > Q = \overline{[G,G]G^p}$ by (i). Conversely, let $x \notin Q$ and pick an open normal subgroup $U < G$ such that $xU \cap QU = \emptyset$ (observe that $\bigcap_U (xU \cap QU) = \emptyset$ and apply the finite intersection property). The Frattini quotient $(G/U)/(QU/U)$ is finite elementary abelian, and therefore has trivial Frattini subgroup by Proposition 1.2.9: since x maps to a nontrivial element, there is some maximal subgroup in $(P/U)/(QU/U)$ missing the image of x, and the conclusion is clear. □

Pontryagin duality

We end this section by stating a fundamental duality result for LCA groups, that is, locally compact Hausdorff abelian groups (for a proof, we refer to Theorem 1.7.2 of [Rud90]). Let T be the circle group, i.e. the group $\mathbf{R}/\mathbf{Z}$ with the quotient topology.

Definition 1.2.15. *For a LCA group A, its* Pontryagin dual *is $A^\curlyvee = \mathrm{Hom}(A, T)$ endowed with the compact-open topology.*

Remark that, if A is torsion, $A^\curlyvee \simeq A^* = \mathrm{Hom}(A, \mathbf{Q}/\mathbf{Z})$ as an abelian group (and also as a topological group if A is discrete).

Theorem 1.2.16 (Pontryagin). *Let A be a LCA group.*

i) Its Pontryagin dual $A^{\curlyvee}$ is again a LCA group.

ii) The canonical map $\alpha : A \to (A^{\curlyvee})^{\curlyvee}$ such that $\alpha(x)(\gamma) = \gamma(x)$ for all $x \in A$ and $\gamma \in A^{\curlyvee}$ is a natural isomorphism of topological groups.

iii) If A is compact, $A^{\curlyvee}$ is discrete, and viceversa; if A is profinite, $A^{\curlyvee}$ is discrete torsion, and viceversa.

1.3 Generators and chains of subgroups

We now look at special systems of (topological) generators for a profinite group G, and show how their cardinality relates to the topology and the lattice of subgroups of G.

We say that a sequence $(x_i \mid i)$ of elements of a profinite group G *converges to* 1 if every open subgroup $U < G$ contains almost all, i.e. all but finitely many, elements x_i.

Definition 1.3.1. *A* set of generators converging to 1 *for G is a subset $X = \{x_i \mid i \in I\} \subset G$ such that $G = \overline{\langle X \rangle}$ and the sequence $(x_i \mid i \in I)$ converges to 1.*

Proposition 1.3.2. *A profinite group G always admits a set of generators converging to 1.*

Proof. We apply Zorn's lemma to the pairs (N, X_N) of normal subgroups $N < G$ and subsets $X_N \subset G \setminus N$ such that $G = \overline{\langle N, X_N \rangle}$ and every open subgroup $U > N$ of G contains almost every element of X_N, ordered by setting $(N, X_N) \leqslant (M, X_M)$ if and only if $N > M$, $X_N \subset X_M$ and $X_M \setminus X_N \subset N$. Then, an ascending chain (N_i, X_{N_i}) is bounded from above by $(\widetilde{N}, X_{\widetilde{N}}) = (\bigcap_i N_i, \bigcup_i X_i)$, provided we show that this is still a valid pair.

To see why this is the case, note that $G/\widetilde{N} = \varprojlim G/N_i$, hence $X_{\widetilde{N}}$ generates G modulo $\widetilde{N}$, which implies $G = \overline{\langle \widetilde{N}, X_{\widetilde{N}} \rangle}$. Also, suppose $U < G$ is open and contains $\widetilde{N} = \bigcap_i N_i$: since $G \setminus U$ is compact, the open cover $\{G \setminus N_i \mid i\}$ has a finite subcover, hence there exists some i such that $U > N_i$; therefore, $X_{\widetilde{N}} \setminus U = X_{N_i} \setminus U$ is finite.

Thus, consider a maximal pair (M, X_M) and suppose $M \neq 1$: if $U < G$ is an open subgroup such that $U \cap M \lneq M$, let Y be a finite subset of M such that $M = \langle U \cap M, Y \rangle$, and consider the pair $(U \cap M, X_M \cup Y)$. It is still a valid pair and it is strictly greater that (M, X_M), a contradiction. □

As a consequence, the following definition is well posed.

Definition 1.3.3. *For a profinite group G, $d(G)$ the smallest cardinality of a set of generators converging to 1 for a profinite group G.*

Note that G is *finitely generated*, i.e. there exists a finite subset $X \subset G$ such that $G = \overline{\langle X \rangle}$, if and only if $d(G)$ is finite.

We now give some useful characterizations of $d(G)$.

If G is a profinite group, define its *local weight* $w_o(G)$ as the smallest cardinality of a fundamental system of neighborhoods of 1.

For a subset $X \subset G$, let $\rho(X)$ be the cardinality of the set of clopen subsets of X.

Proposition 1.3.4. *Let G be a profinite group. If $d(G)$ is infinite, and X is a set of generators of G converging to 1, $|X| = w_o(G)$. In particular, $d(G) = w_o(G)$.*

We need two preliminary lemmas.

Lemma 1.3.5. *Suppose X is an infinite set of generators converging to 1 of a profinite group G. Then*

i) $X \setminus \{1\}$ *is discrete,*

ii) $\overline{X} = X \cup \{1\}$.

In particular, if $1 \notin X$, $\overline{X}$ is the Alexandroff compactification of X, and $\rho\left(\overline{X}\right) = |X|$.

Proof. Pick $x \in X \setminus \{1\}$ and let $U < G$ be an open subgroup of G such that $x \notin U$: then $Ux \cap X$ is finite, say equal to $\{x, x_2, \dots, x_n\}$. Choosing open subsets U_i such that $x \in U_i, x_i \notin U_i$ for $i = 2, \dots n$, and setting $V = U \cap U_2 \cap \cdots \cap U_n$, we get $X \cap V = \{x\}$.

It is plain that $1 \in \overline{X}$. If $y \neq 1$ does not belong to X, we can find an open subgroup $U < G$ not containing y, so that $G \setminus U$ is an open neighborhood of y containing at most finitely many points of X. Arguing as above, we conclude y has an open neighborhood V disjoint from X.

The last statement is clear, since the clopen subsets of X are the finite subsets of $X \setminus \{1\}$ and their complements in $\overline{X}$. □

Lemma 1.3.6. *If G is an infinite profinite group, then $w_o(G) = \rho(G)$.*

Proof. Clearly, $w_o(G) \leqslant \rho(G)$ since G is profinite. Conversely, observe that the translates of a fundamental system of neighborhoods of 1 whose cardinality is $w_o(G)$ give a basis $\mathcal{U}$ for G such that $|\mathcal{U}| = w_o(G)$. For every clopen set $V \subset G$, we can find finitely many elements U_i^V of $\mathcal{U}$ such that $\bigcup_i U_i^V = V$. This defines an injective function $V \mapsto \left\{U_i^V \mid i\right\}$ from the set of clopen sets of G to the set of finite subsets of $\mathcal{U}$, and the result follows. □

Proof (of Proposition 1.3.4). By Lemma 1.3.5, we may reduce to prove that for an infinite closed set X of generators converging to 1 of G we have $w_o(G) = \rho(X)$; since clearly

$\rho(X) \leqslant \rho(G)$ and $\rho(G) = w_o(G)$ according to Lemma 1.3.6, we only need to show that $\rho(X) \geqslant w_o(G)$.

By Propostion 1.1.4, $w_o(G)$ is the cardinality of the set of open normal subgroups $U < G$. If $U < G$ is open normal, it arises as the kernel of a homomorphism $G \to H$ into a finite group H, and such a map is uniquely determined by its values on at most $|H|$ clopens of X. Therefore, there are at most $\rho(X)$ such maps, and $w_o(G) \leqslant \rho(X)$. □

Theorem 1.3.7. *Let G be a pro-$\mathfrak{c}$-group, and μ be a cardinal. Then $w_o(G) \leqslant \mu$ if and only if there exists a chain*

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

of normal subgroups $G_\lambda < G$ for $\lambda \leqslant \mu$ with the following properties:

i) for all $\lambda < \mu$, $G_\lambda / G_{\lambda+1}$ is a $\mathfrak{c}$-group,

ii) if λ is a limit ordinal, $G_\lambda = \bigcup_{\nu<\lambda} G_\nu$.

If G is infinite, we may assume $w_o(G/G_\lambda) < w_o(G)$ for all $\lambda < \mu$.

Proof. We may assume G to be infinite. Let $\mu = w_o(G)$ and consider a fundamental system $\{U_\lambda \mid \lambda < \mu\}$ of neighborhoods of 1 made of open normal subgroups of G. For all $\lambda \leqslant \mu$, set $G_\lambda = \bigcap_{\nu<\lambda} U_\nu$. Then G_λ is a pro-$\mathfrak{c}$-group for all λ, and (i) and (ii) are clearly verified. To prove the last statement, observe that the set $\{U_\nu / G_\lambda \mid \nu < \lambda\}$ is a fundamental system of neighborhoods of 1 in G/G_λ: consequently, $w_o(G/G_\lambda) \leqslant |\lambda| < \mu$.

Conversely, suppose the existence of a chain of open normal subgroups $G_\lambda < G$ indexed by $\lambda \leqslant \mu$ and verifying (i) and (ii). It is enough to prove that $w_o(G/G_\lambda) \leqslant |\lambda|$ for all $\lambda \leqslant \mu$, and we proceed by induction on λ, the case $\lambda = 1$ being trivial.

If $\lambda = \nu + 1$, let $\mathcal{U}_\nu$ be a set of open normal subgroups of G containing G_ν such that $|\mathcal{U}_\nu| \leqslant |\nu|$; then, the set $\{U/G_\nu \mid U \in \mathcal{U}_\nu\}$ is a fundamental system of neighborhoods of 1. Since $[G_\nu : G_\lambda]$ is finite, we can find an open normal subgroup $V < G$ such that $G_\lambda = G_\nu \cap V$. Thus, $\bigcap_{U \in \mathcal{U}_\nu} (U \cap V) = G_\lambda$ and $\{(U \cap V)/G_\lambda \mid U \in \mathcal{U}_\nu\}$ is a fundamental system of neighborhoods of 1 of G/G_λ, which implies $w_o(G/G_\lambda) \leqslant |\lambda|$.

If λ is a limit, choose $\mathcal{U}_\nu$ as in the previous case for all $\nu \leqslant \lambda$, and let $\mathcal{U}_\lambda$ be the set of finite intersections of elements in $\bigcup_{\nu<\lambda} \mathcal{U}_\nu$. Then, as before, $\bigcap_{U \in \mathcal{U}_\lambda} U = G_\lambda$ and consequently the set $\{U/G_\lambda \mid U \in \mathcal{U}_\lambda\}$ is a fundamental system of neighborhoods of 1 in G/G_λ. Finally, we have

$$|\mathcal{U}_\lambda| \leqslant \sum_{\nu \leqslant \lambda} |\mathcal{U}_\nu| \leqslant \sum_{\nu \leqslant \lambda} |\nu| \leqslant |\lambda|,$$

and the conclusion follows. □

Corollary 1.3.8. *Let* $H < G$ *be a normal subgroup of a profinite group* G*. If either* G *or* H *is infinite,*

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

Proof. Letting U run through the open normal subgroups of G, the sets $\{U/H \mid U > H\}$ and $\{U \cap H \mid U \not< H\}$ are fundamental systems of neighborhoods of 1 for G/H and H respectively, so that $w_o(G) \geqslant w_o(H) + w_o(G/H)$. Conversely, if $\mu = w_o(G/H), \nu = w_o(H)$, we have a chain

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

of open normal subgroups of G satisfying the conditions of Theorem 1.3.7, whence $w_o(G) \leqslant \mu + \nu$. □

Corollary 1.3.9. *Let* G *be a pro-*$\mathfrak{c}$*-group and* $H < G$ *be a normal subgroup. There exist some cardinal* μ *and a chain*

$$H = H_0 > H_1 > \cdots > H_\lambda > \cdots > H_\mu = 1,$$

with the following properties:

i) for all $\lambda < \mu$, $H_{\lambda+1}$ *is normal in* G *and* $H_\lambda/H_{\lambda+1}$ *is a* $\mathfrak{c}$*-group,*

ii) for all $\lambda < \mu$, $H_{\lambda+1}$ *is maximal in* H_λ *with respect to these properties;*

iii) if $\lambda \leqslant \mu$ *is a limit ordinal,* $H_\lambda = \bigcap_{\nu<\lambda} H_\nu$*;*

iv) if H *is infinite, and* $M < G$ *is a normal subgroup containing* K *such that* $w_o(M/H) < w_o(G)$*, then* $w_o(M/H_\lambda) < w_o(G)$ *for all* $\lambda < \mu$.

Proof. Again, we may assume H infinite. The set $\mathcal{U}_H = \{U \cap H \mid U < G \text{ open normal}\}$ is a fundamental system of open neighborhoods of 1 in H. Let $\mu = |\mathcal{U}_H| = w_o(H)$, and choose an indexing $\mathcal{U}_H = \{U_\lambda \mid \lambda < \mu\}$. For all $\lambda \leqslant \mu$, set $H_\lambda = \bigcap_{\nu<\lambda} U_\nu$.

Then (i) and (iii) clearly hold, and we may assume (ii) holds as well by inserting finitely many subgroups between H_λ and $H_{\lambda+1}$. To verify (iv) observe that $\{U_\nu/H_\lambda \mid \nu < \lambda\}$ is a fundamental system of neighborhoods of 1 in H/H_λ, so that $w_o(H/H_\lambda) \leqslant |\lambda| < \mu$, and apply the previous Corollary to get

$$w_o(M/H_\lambda) = w_o(M/H) + w_o(H/H_\lambda) < w_o(G)$$

as wanted. □

We end this section with two results about finitely generated groups. The first one sharpens Theorem 1.3.7.

Lemma 1.3.10. *Let G be a finitely generated profinite group.*

i) For all $n > 0$, G has finitely many subgroups of index n.

ii) There is a fundamental system of neighborhoods of 1 consisting of a countable chain

$$G = V_0 > V_1 > \cdots$$

of open characteristic subgroups of G.

Proof. In order to show (i), it is enough to prove that there are finitely many *normal* subgroups of index n, since an open subgroup H of G has finitely many conjugates and its core has finite index.

An open normal subgroup $N < G$ of index n is the kernel of an epimorphism $\varphi : G \to E$ where E is a finite group of order n. Since the restriction of φ to a finite set of generators of G determines φ, we only have finitely many such maps. Combined with the fact there are only finitely many (isomorphism classes of) groups of order n, this concludes.

For (ii), let V_n be the intersection of all open normal subgroups of index n. □

An abstract group G is Hopfian if any surjective endomorphism of G onto itself is an isomorphism. Finitely generated profinite groups have the topological analogue of the Hopfian property.

Proposition 1.3.11. *A finitely generated profinite group G is* Hopfian, *i.e. every (continuous) surjective endomorphism $\varphi : G \to G$ is an isomorphism.*

Proof. It is enough to prove that φ is injective, i.e. $\ker(\varphi)$ belongs to every open normal subgroup of G. For each n, let $\mathcal{N}_n$ be the finite set of open normal subgroups of G of index n, and consider the map $\mathcal{N}_n \to \mathcal{N}_n$ sending $U \to \varphi^{-1}(U)$: by the surjectivity of φ, it is injective, and therefore bijective since $\mathcal{N}_n$ is finite by Lemma 1.3.10. Consequently, if U is an open normal subgroup of G, there exists an open normal subgroup $V < G$ such that $U = \varphi^{-1}(V)$, and thus $U > \ker(\varphi)$. □

Chapter 2

Cohomology and cohomological dimension of profinite groups

After we showed their main topological and algebraic features, we are ready to introduce cohomology for a profinite group G (together with a related invariant, cohomological dimension). Its definition is analogous to the case of abstract groups, and many of the properties of abstract cohomology are still valid in our setting. In particular, though we won't be able to describe it as an Ext functor for some module over a specific ring related to G, we shall prove that cohomology groups are still the derived functors of the functor that sends a G-module to its fixed submodule.

In order to do so, we first recall some notions from homological algebra.

Let $\mathcal{A}, \mathcal{B}$ be abelian categories. A (cohomological) δ-*functor* $H^\bullet = (H^n)_{n\geqslant 0}$ is a sequence of additive functors $H^n : \mathcal{A} \to \mathcal{B}$ together with morphisms $\delta : H^n(C) \to H^{n+1}(A)$ defined for any short exact sequence $0 \to A \to B \to C \to 0$ in $\mathcal{A}$ in a way that

i) δ is functorial, i.e. for every $n \geqslant 0$ and every exact diagram

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r] \arrow[d] & B \arrow[r] \arrow[d] & C \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & A' \arrow[r] & B' \arrow[r] & C' \arrow[r] & 0
\end{tikzcd}$$

in $\mathcal{A}$, the square

$$\begin{tikzcd}
H^n(C) \arrow[r, "\delta"] \arrow[d] & H^{n+1}(A) \arrow[d] \\
H^n(C) \arrow[r, "\delta"] & H^{n+1}(A)
\end{tikzcd}$$

is commutative;

ii) for any short exact sequence $0 \to A \to B \to C \to 0$ in $\mathcal{A}$, the sequence

$$\cdots \longrightarrow H^{n-1}(C) \xrightarrow{\delta} H^n(A) \longrightarrow H^n(B) \longrightarrow H^n(C) \xrightarrow{\delta} \cdots$$

is exact.

A morphism of δ-functors $H^\bullet \to K^\bullet$ is a sequence of morphisms $H^n \to K^n$ such that the diagram

$$\begin{tikzcd} H^n(C) \arrow[r, "\delta"] \arrow[d] & H^{n+1}(A) \arrow[d] \\ K^n(C) \arrow[r, "\delta"] & K^{n+1}(A) \end{tikzcd}$$

commutes for every short exact sequence $0 \to A \to B \to C \to 0$.

We say a δ-functor $H^\bullet : \mathcal{A} \to \mathcal{B}$ is *universal* if, for every δ-functor $K^\bullet : \mathcal{A} \to \mathcal{B}$, a morphism of functors $H^0 \to K^0$ admits an extension to a morphism of δ-functors $H^\bullet \to K^\bullet$.

By definition, there exists at most one universal δ-functor $H^\bullet$ such that H^0 equals a fixed functor F; in particular, two universal δ-functors $H^\bullet, K^\bullet$ such that $H^0 = K^0$ are in fact equal.

An additive functor $F : \mathcal{A} \to \mathcal{B}$ is *effaceable* if any object A of $\mathcal{A}$ admits a monomorphism $u : A \to A'$ such that $F(u) = 0$; a δ-functor $H^\bullet : \mathcal{A} \to \mathcal{B}$ is called effaceable if every H^n is effaceable for $n > 0$. We have the following result (see [Gro57], Proposition 2.2.1).

Theorem . *An effaceable δ-functor $H^\bullet : \mathcal{A} \to \mathcal{B}$ is universal.*

The concept of δ-functor generalizes that of derived functor. If $F : \mathcal{A} \to \mathcal{B}$ is an additive functor, we call *right derived functor* for F, if it exists, the unique universal cohomological δ-functor $R^\bullet F$ such that $R^0 F = F$.

2.1 Cohomology of profinite groups

Discrete G-modules

Let G be a profinite group. A G-*module* A is a topological abelian group endowed with a continuous G-action, i.e. a continuous map $G \times A \to A$, say $(x, a) \mapsto xa$, such that $1a = a$ and $x(ya) = (xy)a$ for all $x, y \in G$ and $a \in A$. If A, B are G-modules, a continuous homomorphism $\varphi : A \to B$ is a G-*homomorphism* if $\varphi(xa) = x\varphi(a)$ for all $x \in G$ and $a \in A$.

For our purposes, we shall need G-modules to be discrete. We denote by $\mathsf{DMod}(G)$ the category of discrete G-modules with G-maps.

Definition 2.1.1. *For a subgroup $H < G$, we call $A^H = \{a \in A \mid ha = a \, \text{for all} \, h \in H\}$ the* H-fixed submodule *of* A.

Remark 2.1.2. i) One sees immediately that G-maps preserve fixed submodules. Therefore the assignment $A \to A^G$ induces a functor $\mathsf{DMod}(G) \to \mathsf{Ab}$ to the category of abelian groups, which is easily seen to be left exact.

ii) If $H < G$, A^H is by definition a trivial H-module (i.e. H acts trivially on its elements). If moreover H is normal in G, A^H becomes a G/H-module in a natural way, by setting $(Hx)a = xa$ for all $x \in G$ and $a \in A$.

Discrete G-modules are characterized as follows.

Lemma 2.1.3. *For a G-module A, the following are equivalent.*

i) A is a discrete G-module.

ii) The stabilizers G_a are open in G for all $a \in A$.

iii) $A = \bigcup_U A^U$, where U runs through the open subgroups of G.

Proof. Since G_a equals the preimage of the continuous map $G \to A$ sending $x \mapsto xa$, (i) implies (ii). Also, (ii) implies (iii) since $A^{G_a} \ni a$ for all $a \in A$.

Finally, to prove that (iii) implies (i) we have to find an open subset of $G \times A$ mapping to a through the action of G for any fixed $a \in A$: pick $U < G$ open such that $a \in A^U$, and observe that $U \times \{a\}$ is open in $G \times A$ and $xa = a$ for all $x \in U$ by the definition of A^U. □

From now on, all G-modules are assumed to be discrete.

Definition of the cohomology groups

We turn to the definition of cohomology groups for a fixed G-module A.

For $n \geqslant 0$, consider the abelian group $X^n = \mathscr{C}(G^{n+1}, A)$ of all continuous functions $f : G^{n+1} \to A$: since A is discrete, so is X^n with the open-compact topology, and it is easily checked that the G-action defined by

$$(xf)(x_0, \dots, x_n) = xf(x^{-1}x_0, \dots, x^{-1}x_n)$$

is continuous.

We make the sequence $(X^n)_{n \geqslant 0}$ of G-modules into a complex by defining differentials $d^{n+1} : X^n \to X^{n+1}$ so that

$$d^{n+1}f(x_0, \dots, x_{n+1}) = (-1)^i \sum_{i=0}^{n+1} f(x_0, \dots, \hat{x_i}, \dots, x_{n+1}),$$

where the hat means that x_i is omitted from the sequence. Also, let $d^0 : A \to X^0$ be the map $a \to (x \mapsto a)$.

Then, $A \to X^\bullet$ is a resolution of A in G-modules, as the following lemma proves.

Lemma 2.1.4. *The sequence*

$$A \xrightarrow{d^0} X^0 \xrightarrow{d^1} X^1 \xrightarrow{d^2} \cdots$$

is exact.

Proof. A straightforward computation shows that the above sequence is a complex. To prove exactness, it is enough to find a contracting homotopy, i.e. maps $k^{-1} : X^0 \to A$ and $k^n : X^{n+1} \to X^n$ such that, for for $n \geqslant 0$,

$$k^n d^{n+1} + d^n k^{n-1} = 0.$$

By defining $k^{-1}f = f(1)$ and $(k^n f)(x_0, \dots, x_n) = f(1, x_0, \dots, x_n)$, the above equation is easily verified. □

Applying the fixed functor $\bullet^G$ (see Remark 2.1.2) to the exact complex $X^\bullet$, we get a complex of abelian groups, whose n-th term is the group $C^n(G, A) = \mathscr{C}(G^{n+1}, A)^G$, consisting of all continuous functions $f : G^{n+1} \to A$ such that $xf(x_0, \dots, x_n) = f(xx_0, \dots, xx_n)$. Its cohomology is

$$H^n(C^\bullet(G, A)) = \ker(d^{n+1}) / \operatorname{im}(d^n)$$

and we call the elements of $Z^n(G, A) = \ker(d^{n+1})$ and $B^n(G, A) = \operatorname{im}(d^n)$ *homogeneous* n-cocycles and n-coboundaries, respectively, of G with respect to A.

Definition 2.1.5. *For* $n \geqslant 0$, *the* n-th cohomology group $H^n(G, A)$ *of* G *with coefficients in* A *is defined as*

$$H^n(G, A) = H^n(C^\bullet(G, A)).$$

We can give a useful alternative definition of $H^n(G, A)$ by constructing a complex $\mathscr{C}^\bullet(G, A)$ as follows. Let $\mathscr{C}^0(G, A) = A$ and, for $n > 0$, set $\mathscr{C}^n(G, A) = \mathscr{C}(G^n, A)$, the abelian group of *all* continuous functions $G^n \to A$; the differentials $\partial^{n+1} : \mathscr{C}^n(G, A) \to \mathscr{C}^{n+1}(G, A)$ are defined as

$$\begin{aligned} \partial^{n+1} f(x_1, \dots, x_{n+1}) = x_1 f(x_2, \dots, x_{n+1}) &+ \sum_{i=1}^{n} (-1)^i f(x_1, \dots, x_i x_{i+1}, \dots, x_{n+1}) \\ &+ (-1)^{n+1} f(x_2, \dots, x_{n+1}). \end{aligned}$$

We call *inhomogenous* n-cocycles and n-coboundaries the elements of $\ker(\partial^{n+1})$ and $\operatorname{im}(\partial^n)$ respectively.

Lemma 2.1.6. *The complexes* $\mathscr{C}^\bullet(G, A)$ *and* $C^\bullet(G, A)$ *are isomorphic. Consequently,* $H^n(G, A) = H^n(\mathscr{C}^\bullet(G, A))$ *for all* $n \geqslant 0$.

Proof. In degree 0, the map $C^0(G,A) \to A$ given by $f \mapsto f(1)$ is an isomorphism; for $n > 0$, an isomorphism $\varphi_n : C^n(G,A) \to \mathscr{C}^n(G,A)$ is given by

$$\varphi_n(f)(x_1,\dots,x_n) = f(1,x_1,x_1x_2,\dots,x_1\cdots x_n),$$

with inverse $\psi_n : \mathscr{C}^n(G,A) \to C^n(G,A)$ given by

$$\psi_n(g)(x_0,\dots,x_n) = x_0 g(x_0^{-1}x_1,\dots,x_{n-1}^{-1}x_n),$$

An one may readily check, the above maps commute with differentials d and ∂, and the conclusion follows. □

In particular, for $a \in A$ and $f \in \mathscr{C}(G,A)$,

$$\partial^1(a)(x) = xa - a,$$
$$\partial^2(f)(x,y) = xf(y) - f(xy) + f(x).$$

Therefore, $\ker(\partial^0) = A^G$ and, if the G-action on A is trivial, $\operatorname{im}(\partial^1) = 0$ and $\ker(\partial^2) = \operatorname{Hom}(G,A)$. By Lemma 2.1.6, this implies

Corollary 2.1.7. *For a G-module A, $H^0(G,A) = A^G$. If A is a trivial G-module, $H^1(G,A) = \operatorname{Hom}(G,A)$.*

Finally, we have an explicit description of $H^2(G,A)$ by the topological version of Schreier's theorem on group extensions with abelian kernel. Consider an extension X of A by G, i.e. an exact sequence

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r] & E \arrow[r, "\varphi"] & G \arrow[r] & 1 \end{tikzcd}$$

where A is finite abelian and E is profinite, and choose a continuous section $\sigma : G \to E$ of φ with $\sigma(1) = 1$. Then, writing operations in E additively, A is a G-module via the action $xa = {}^{\sigma(x)}a = \sigma(x) + a - \sigma(x)$, which does not depend on σ since A is abelian.

Call two extensions X, X' of A by G *equivalent* if there is a homomorphism $E \to E'$ such that the diagram

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r] \arrow[d, equal] & E \arrow[r, "\varphi"] \arrow[d] & G \arrow[r] \arrow[d, equal] & 1 \\ 0 \arrow[r] & A \arrow[r] & E' \arrow[r, "\varphi'"] & G \arrow[r] & 1 \end{tikzcd} \tag{2.1}$$

commutes (note in particular that $E \to E'$ is an isomorphism). Let $\mathcal{X}(G,A)$ be the set of extensions of A by G up to equivalence.

Theorem 2.1.8. *There is a bijection of pointed sets*

$$H^2(G,A) \simeq \mathcal{X}(G,A)$$

with a distinguished point in $\mathcal{X}(G,A)$ being the equivalence class of a semidirect product $A \rtimes G$.

Proof. We only sketch the proof, showing how the maps are constructed. Consider an extension

$$0 \longrightarrow A \longrightarrow E \xrightarrow{\varphi} G \longrightarrow 1$$

of A by G, and choose a continuous section $\sigma : G \to E$. For $x, y \in G$, the difference of $\sigma(x) + \sigma(y)$ and $\sigma(xy)$ maps to 0 through φ, hence we may find some element $f(x, y) \in A$ such that $\sigma(x) + \sigma(y) = f(x, y) + \sigma(xy)$.

One easily checks that the assignment $(x, y) \mapsto f(x, y)$ defines an inhomogenous 2-cocycle, and that changing σ with another section induces a cocycle that differs from f by a 2-coboundary: then X is associated to a well defined class $f(X) \in H^2(G, A)$. Since the choice of a section for φ induces a section for φ' in diagram (2.1), by the same argument one also proves that if X and X' are equivalent extensions they have the same class in $H^2(G, A)$. We therefore get a well defined map $\mathcal{X}(G, A) \to H^2(G, A)$.

To find an inverse, consider an inhomogenous 2-cocycle $f : G^2 \to A$ representing an element $c \in H^2(G, A)$. We may assume that f is *normalized*, that is $f(x, 1) = f(1, x) = 0$ for all $x \in G$. To see this, observe that $f(x, 1) = xf(x, 1)$ and $f(1, x) = f(1, 1)$ and consider the 2-coboundary $g = \partial^2(\overline{g})$, where the 1-cochain $\overline{g}$ is defined as $\overline{g}(x) = f(1, 1)$. Then $g(x, y) = xf(1, 1)$ and $f - g$ is a 2-cochain which still represents c and has the desidered property.

Such a normalized cocycle induces on the set $E = A \times G$ a group structure by setting

$$(a, x)(b, y) = (a + xb + f(x, y), xy)$$

for $a, b \in A$ and $x, y \in G$. This way, E is in fact a profinite group, and

$$X(f) : 0 \longrightarrow A \longrightarrow E \xrightarrow{\varphi} G \longrightarrow 1\ ,$$

with the canonical embedding and projection $A \to E$ and $E \to G$, is an extension of A by G we may then associate to f. If g is another cocycle representing c, the extension $X(g)$ is seen to be equivalent to $X(f)$, so that we get a well defined assignment $[f] \mapsto X(f)$ for $[f] \in H^2(G, A)$. Since the two maps we defined are in fact mutually inverse, the result follows. □

Remark 2.1.9. In principle, one can define the complex $C^\bullet(G, A)$ for *any* topological G-module A and consider its cohomology. Though in this generality one does not get the nice functorial properties we are now going to explain for the discrete case, this allows for example to remove the finiteness assumption on A in Theorem 2.1.8.

Cohomology as a δ-functor

We now aim to prove that the cohomology groups we have just constructed give rise to a universal δ-functor $\mathsf{DMod}(G) \to \mathsf{Ab}$, starting with their functorial properties.

Consider two profinite groups G, G' and let A, A' be a G-module and a G'-module, respectively.

Definition 2.1.10. *A map* $\varphi : G \to G'$ *of profinite groups and a homomorphism* $f : A' \to A$ *of abelian groups are* compatible *if* $f(\varphi(x)a) = xf(a)$ *for all* $a \in A, x \in G,$

In particular, if $G = G'$ and φ is the identity map, this is the same as saying that f is a G-map.

A pair (φ, f) of compatible morphisms induces maps $C^n(G', A') \to C^n(G, A)$, by which an element $g \in C^n(G', A')$ maps to the function

$$(x_0, \dots, x_n) \mapsto f \circ g(\varphi(x_0), \dots, \varphi(x_n)).$$

The compatibility assumption implies the sequence of such maps is a morphism of complexes $C^\bullet(G', A') \to C^\bullet(G, A)$. Thus, we get induced homomorphisms

$$H^n(G', A') \to H^n(G, B)$$

for all $n \geqslant 0$. As an immediate consequence, we may see $C^n(G, \bullet)$ and $H^n(G, \bullet)$ as functors $\mathsf{DMod}(G) \to \mathsf{Ab}$ for all $n \geqslant 0$.

Suppose now we have limits $G = \varprojlim G_i$ and $A = \varinjlim A_i$ of profinite groups G_i and G_i-modules respectively, and the limits are compatible in the sense that, for all $i \leqslant j$, the transition maps $\varphi_{ji} : G_j \to G_i$ and $f_{ij} : A_i \to A_j$ are compatible. Then A is naturally a G-module by setting, for $x = (x_i) \in G$ and $a = (a_i) \in A$, $xa = f_i(x_i a_i)$, where $f_i : A_i \to A$ is the canonical map and the index i is such that $f_i(a_i) = a$.

Lemma 2.1.11. *i) If* $G = \varprojlim G_i$ *and* $A = \varinjlim A_i$ *are compatible,*

$$C^n(G, A) = \varinjlim C^n(G_i, A_i).$$

ii) As a functor $\mathsf{DMod}(G) \to \mathsf{Ab}$, $C^n(G, \bullet)$ *is exact for all* $n \geqslant 0$.

Proof. To prove (i), we may easily reduce to the case where the G_i are finite: for the general case, write $G = \varprojlim G_i/U$ as in Proposition 1.1.12 and apply the finite case to find

$$C^n(G, A) = \varinjlim_{\mathcal{U}} C^n(G_i/U, A_i^U) = \varinjlim_{i} \left(\varinjlim_{\mathcal{U}_i} C^n(G_i/U, A_i^U) \right) = \varinjlim C^n(G_i, A_i).$$

Suppose the G_i are finite: for all i, the canonical maps $G \to G_i$ and $A_i \to A$ induce morphisms

$$\psi_k : C^n(G_i, A_i) \to C^n(G, A)$$

that give rise to a map

$$\psi : \varinjlim C^n(G_i, A_i) \to C^n(G, A).$$

To prove that it is an isomorphism, it is enough to show that it is a bijection.

Suppose first that $f \in \varinjlim C^n(G_i, A_i)$ maps to the zero function in $C^n(G, A)$. Pick an index k and a map $f_k \in C^n(G_k, A_k)$ such that $\psi_k(f_k) = f$, and call f_i the composition $G_i \to G_k \xrightarrow{f_i} A_i \to A_k$ for all $i \geqslant k$. Also, let $X_i = G_i^{n+1} \setminus f_i^{-1}(0)$, which is closed since A is discrete. Then X_i can be naturally made into a (cofinal) inverse system, and its inverse limit must be empty, since an element $(x_0, \dots, x_n) \in \varprojlim X_i \subset G^{n+1}$ would verify $f(x_0, \dots, x_n) \neq 0$, contradicting $f = 0$. Hence, $\varprojlim X_i = \emptyset$ and therefore, by Lemma 1.1.1, already $f_i = 0$ for some i, which proves that ψ is injective.

To see surjectivity, fix $f \in C^n(G, A)$ and observe that $\mathrm{im}(f) = \{a_1, \dots, a_t\}$ is finite since G is compact and A is discrete; also, since $f(xx_0, \dots, xx_n) = xf(x_0, \dots, x_n)$, f is constant on the cosets of $H = \bigcap_{i=1}^t G_{a_i} < G$, which is an open subgroup of G. By Lemma 1.1.8, there is an index k such that $H > \ker(\varphi_k)$, where $\varphi_k : G \to G_k$ is the canonical projection: therefore f is constant on the cosets of $\ker(\varphi_k)$ and factors to a continuous function $G_i \to A$ for all $i \geqslant k$. Also, since $\mathrm{im}(f)$ is finite, there is some $h \geqslant k$ such that the image of A_i in A via the canonical map contains $\mathrm{im}(f)$ for $i \geqslant h$: thus, we have a map $f_h : G_h \to A_h$ in $\varinjlim C^n(G_i, A_i)$ such that $\varphi(f_h) = f$, and ψ is surjective.

For assertion (ii), the case when G is finite follows by observing that

$$C^n(G, \bullet) = \mathrm{Hom}_{\mathbb{Z}[G]}(F, \bullet),$$

where $\mathbb{Z}[G]$ is the group ring on G and F is the free $\mathbb{Z}[G]$-module on the set G^{n+1} (this is clear, for the continuity assumption on elements of $C^n(G, A)$ is vacuous if G is finite).

For the general case, (i) implies that

$$C^n(G, A) = \varinjlim_{U} C^n(G/U, A^U),$$

U running through the open normal subgroups of G, and the result follows from the exactness of $\varinjlim$. □

The identification in Lemma 2.1.11(i) is really an isomorphism of complexes

$$C^\bullet(G, A) = \varinjlim C^\bullet(G_i, A_i),$$

since the isomorphisms $\varinjlim C^n(G_i, A_i) \to C^n(G, A)$ clearly commute with d. As an immediate consequence, group cohomology commutes with limits and direct sums, as follows.

Corollary 2.1.12. *i) If $G = \varprojlim G_i$ and $A = \varinjlim A_i$ are compatible,*

$$H^n(G, A) = \varinjlim H^n(G_i, A_i).$$

ii) If $A = \bigoplus_i A_i$ *is a direct sum of* G*-submodules of* A*,*

$$H^n(G,A) = \bigoplus_i H^n(G,A_i).$$

We are now able to make $(H^n(G,\bullet))_{n\geqslant 0}$ into a δ-functor. Pick a short exact sequence $0 \to A \to B \to C \to 0$ of G-modules, and consider the commutative diagram

$$\begin{tikzcd}
& C^n(G,A)/B^n(G,A) \arrow[r] \arrow[d] & C^n(G,B)/B^n(G,B) \arrow[r] \arrow[d] & C^n(G,C)/B^n(G,C) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & Z^{n+1}(G,A) \arrow[r] & Z^{n+1}(G,B) \arrow[r] & Z^{n+1}(G,C) &
\end{tikzcd}.$$

By Lemma 2.1.11(ii), its rows are exact. We may therefore apply the Snake lemma to it, and get an exact sequence

$$\begin{tikzcd}
H^n(G,A) \arrow[r] & H^n(G,B) \arrow[r] & H^n(G,C) \arrow[r, "\delta"] & H^{n+1}(G,A) \arrow[r] & {} \\
& & {} \arrow[r] & H^{n+1}(G,B) \arrow[r] & H^{n+1}(G,C)
\end{tikzcd}$$

where the connecting morphism δ is functorial by its construction. Arguing by induction on n, we get the wanted long exact sequence in order to obtain a δ-functor.

We are left with proving that $(H^n(G,\bullet))_{n\geqslant 0}$ is universal. We need the notion of coinduced modules.

Definition 2.1.13. *Let* $H < G$ *a subgroup, and* A *an* H*-module. The* H-coinduced module *of* A *is the* G*-module*

$$\mathrm{Coind}_H^G(A) = \{f \in \mathscr{C}(G,A) \mid f(hx) = hf(x) \text{ for all } h \in H, x \in G\},$$

where the action of G *is given by* $(xf)(y) = xf(x^{-1}y)$.

One esily checks that the above G-action is continuous. For $H = 1$, we let $\mathrm{Coind}^G(G,A) = \mathrm{Coind}_1^G(G,A)$; note that it coincides with $\mathscr{C}(G,A)$.

Proposition 2.1.14. *For a* G*-module* A, $H^n(G,\mathrm{Coind}^G(A)) = 0$ *for all* $n > 0$.

Proof. We claim that there is an isomorphism of complexes $X^\bullet(G,A) \xrightarrow{\sim} C^\bullet(G,\mathrm{Coind}^G(A))$: since the former is exact, the result will follow.

Such isomorphism is found by considering the maps $\varphi_n : X^n(G,A) \to C^n(G,\mathrm{Coind}^G(A))$ defined as

$$\varphi_n(f)(x_0,\dots,x_n)(x) = xf(x^{-1}x_0,\dots,x^{-1}x_n);$$

in fact, they commute with d, and are inverted by $\psi_n : C^n(G,\mathrm{Coind}^G(A)) \to X^n(G,A)$ such that $\psi_n(g)(x_0,\dots,x_n) = g(x_0,\dots,x_n)(1)$. □

We have a natural embedding $\iota : A \to \mathrm{Coind}^G(A)$, that sends $a \in A$ to the constant map $x \to a$: ι is therefore a monorphism such that $H^n(G, \bullet)(\iota) = 0$ for all $n > 0$.

This shows that $H^n(G, \bullet)$ is effaceable for all $n > 0$, and therefore $(H^n(G, \bullet))_{n \geqslant 0}$ is a universal δ-functor. We summarise the above discussion in the following result; note that, by Corollary 2.1.7, $H^0(G, \bullet) = \bullet^G$.

Proposition 2.1.15. *For a profinite group* G, $(H^n(G, \bullet))_{n \geqslant 0}$ *is the sequence of right derived functors of the fixed functor* $\bullet^G$. *In particular,* $H^\bullet(G, \bullet)$ *is a universal* δ*-functor.*

Remark 2.1.16. It is easy to prove that $\mathsf{DMod}(G)$ has enough injectives, using the corresponding result for abstract G-modules. As a consequence of Remark 2.1.2 and a general theorem from homological algebra, one then knows *a priori* that the functor $\bullet^G$ has a right derived functor. Therefore, one could define $H^n(G, \bullet) = R^n \bullet^G$, and then prove that $A \to X^\bullet(G, A)$ is a suitable resolution for the computation of such right derived functors, getting back our definition.

2.2 Cohomology of subgroups and quotients

We now look at some special homomorphisms of cohomology groups induced by specific pairs of compatible maps, that allow us to relate the cohomology of a profinite group G to that of its subgroups and quotients.

Restriction and Corestriction

For a subgroup $H < G$ and a G-module A, the inclusion $H \to G$ and the identity map $A \to A$ induce the *restriction* maps

$$\mathrm{res}^G_H : H^n(G, A) \to H^n(H, A).$$

At the level of cochains, $\mathrm{res}^G_H(f)$ is the restriction of $f \in C^n(G, A)$ to H^{n+1}; in particular, in degree 0, res^G_H is the inclusion $A^G \subset A^H$. Remark that the sequence of restrictions maps in degree n for $n \geqslant 0$ induces a morphism of δ-functors $(H^n(G, \bullet))_n \to (H^n(H, A))_n$.

For *open* subgroups of G, we get a map in the opposite direction as follows. Let $H < G$ be open and fix a transversal T of H in G. Define the *norm* $N_{G/H} : A^H \to A^G$ as

$$N_{G/H}(a) = \sum_{x \in T} xa;$$

note that T is finite by assumption, and the definition does not depend on the choice of T since a is fixed by H. We define the *corestriction* cor^H_G as the unique morphism of δ-functors $(H^n(H, \bullet))_n \to (H^n(G, \bullet))_n$ that coincides with $N_{G/H}$ in degree 0.

Lemma 2.2.1. *Let* $K < H < G$.

i) $\operatorname{res}^H_K \operatorname{res}^G_H = \operatorname{res}^G_K$.

ii) If K, H *are open,* $\operatorname{cor}^H_G \operatorname{cor}^K_H = \operatorname{cor}^K_G$.

Proof. The equalities are clear in degree 0, and this suffices, since both left and right hand sides are morphisms of universal δ-functors. □

Proposition 2.2.2. *Suppose* $H < G$ *is open. Then*

$$\operatorname{cor}^H_G \operatorname{res}^G_H = [G : H].$$

Proof. Again, we can reduce to check this in degree 0, where the composite map $A^G \to A^H \to A^G$ is $N_{G/H}(a)$ for $a \in A^G$. Since G acts trivially on A, $N_{G/H}(a) = [G : H]a$. □

We may now prove that cohomology groups are always torsion groups, and look at some consequences.

Proposition 2.2.3. *For all* $n > 0$, $H^n(G, A)$ *is a torsion group and the order of an element* $c \in H^n(G, A)$ *divides* $\#G$.

Proof. By Corollary 2.1.12, we may write $H^n(G, A) = \varinjlim_U H^n(G/U, A^U)$ where, as usual, the U are normal open subgroups in G; thus, since it is preserved by taking this limit, it suffices to prove the wanted property assuming that G is finite. In this case, $1 < G$ is open, and Proposition 2.2.2 implies

$$|G| H^n(G, A) = \operatorname{cor}^1_G \operatorname{res}^G_1 H^n(G, A) = \operatorname{cor}^1_G H^n(1, A) = 0,$$

hence the result. □

For a torsion abelian group A, let A_p be its p-primary part, i.e. the subgroup of p-torsion elements. An immediate consequence of Proposition 2.2.3 is

Corollary 2.2.4. *Let* A *be a* G*-module. Then*

i) $H^n(G, A) = \bigoplus\limits_p H^n(G, A)_p$;

ii) if A *is torsion,* $H^n(G, A) = \bigoplus_p H^n(G, A_p)$.

Proposition 2.2.5. *Suppose* $H < G$ *is such that* $p \nmid [G : H]$. *Then the restriction*

$$\operatorname{res}^G_H : H^n(G, A)_p \to H^n(H, A)$$

is injective. If H *is open, the corestriction*

$$\operatorname{cor}^H_G : H^n(H, A)_p \to H^n(G, A)$$

is surjective.

Proof. We prove the statement about restriction; the other one is analogous. Write $H = \bigcap U = \varprojlim U$, where U ranges the open subgroups of G containing H. Then $H^n(H, A) = \varinjlim_U H^n(U, A)$, and the transition maps $H^n(U, A) \to H^n(U', A)$ for $U' < U$ are precisely the restrictions. Suppose $\operatorname{res}^G_H(c) = 0$ for some $c \in H^n(G, A)_p$: by Proposition 1.1.12, $\operatorname{res}^G_U(c) = 0$ for some open subgroup $U > H$. Since U is open,

$$0 = \operatorname{cor}^U_G \operatorname{res}^G_U(c) = [G : H]c,$$

a which implies $c = 0$ for c is p-torsion and $p \nmid [G : H]$. □

Corollary 2.2.6. *For each prime p, let G_p be a p-Sylow of G. If $H^n(G_p, A) = 0$ for all p, then $H^n(G, A) = 0$.*

Proof. The restriction $\operatorname{res} : H^n(G, A)_p \to H^n(G_p, A)$ is the zero map. By Proposition 2.2.5, $H^n(G, A)_p = 0$, and Corollary 2.2.4 concludes. □

We are now able to prove the profinite version of Shapiro's lemma. We need a preliminary result, whose proof goes exactly like the one of Lemma 2.1.11.

Lemma 2.2.7. *i) If $H < G$ and A is an H-module,*

$$\operatorname{Coind}^G_H(A) = \varinjlim \operatorname{Coind}^{G/U}_{HU/U}(A^U).$$

ii) As a functor $\mathsf{DMod}(H) \to \mathsf{DMod}(G)$, $\operatorname{Coind}^G_H(\bullet)$ is exact.

Proposition 2.2.8 (Shapiro's lemma)**.** *Let $H < G$ a subgroup and A an H-module. We have natural isomorphisms*

$$H^n(G, \operatorname{Coind}^G_H(A)) \simeq H^n(H, A)$$

for all $n \geqslant 0$.

Proof. Consider the canonical map $\mu : \operatorname{Coind}^G_H(A) \to A$ such that $\mu(f) = f(1)$. Since $\operatorname{Coind}^G_H(\bullet)$ is exact by Lemma 2.2.7, $(H^n(G, \operatorname{Coind}^G_H(\bullet)))_{n\geqslant 0}$ is a universal δ-functor. The composition

$$H^n(G, \operatorname{Coind}^G_H(A)) \xrightarrow{\text{res}} H^n(H, \operatorname{Coind}^G_H(A)) \longrightarrow H^n(H, A),$$

where the right map is induced by μ, induces a morphism of universal δ-functors

$$(H^n(G, \operatorname{Coind}^G_H(\bullet)))_n \to (H^n(H, \bullet))_n.$$

It suffices to prove that it is an isomorphism in dimension 0: in this case, it reduces to the map sending $f \in \left(\operatorname{Coind}^G_H(A)\right)^G$ to $f(1) \in A^H$, and is inverted by the map sending $a \in A^H$ to the constant function $x \mapsto a$ in $\left(\operatorname{Coind}^G_H(A)\right)^G$. □

Inflation

The last special morphism of cohomology groups we need to look at is the *inflation* map. For a normal subgroup $K < G$ define

$$\mathrm{inf}_G^{G/K} : H^n(G/K, A^K) \to H^n(G, A)$$

as the homomorphism induced by the projection $G \to G/K$ and the inclusion $A^K \to A$ (recall that A^K is in fact a G/K-module by Remark 2.1.2). In degree zero, $\mathrm{inf} : (A^K)^{G/K} \to A^G$ is the identity map, while a cocycle $f \in C^n(G/K, A^K)$ is lifted by $\mathrm{inf}_G^{G/K}$ to $g \in C^n(G, A)$ defined by $g(x_0, \dots, x_n) = f(x_0K, \dots, x_nK)$.

Again, remark that inflation is a morphism of δ-functors $(H^n(G/K, \bullet^K))_n \to (H^n(G, A))_n$, and therefore the following multiplicativity result is obvious.

Proposition 2.2.9. *Suppose $K' < K < G$ are normal subgroups. Then $\mathrm{inf}_G^{G/K'} \mathrm{inf}_{G/K'}^{G/K} = \mathrm{inf}_G^{G/K}$.*

We shall need a different interpretation of the inflation map when $n = 2$ in terms of group extensions. Suppose we have a diagram

$$\begin{tikzcd}
 & & & G \arrow[d, two heads, "\psi"] & \\
X : 0 \arrow[r] & A \arrow[r] & E \arrow[r, "\varphi"] & \overline{G} \arrow[r] & 1
\end{tikzcd}$$

where the lower row is an extension of A by G in the sense of Theorem 2.1.8, and the map $\psi : G \to \overline{G}$ is an epimorphism. Then we may consider the *pullback* extension

$$\begin{tikzcd}
Y : 0 \arrow[r] & A \arrow[r] & A \times_{\overline{G}} G \arrow[r] & G \arrow[r] & 1
\end{tikzcd}$$

where $A \times_{\overline{G}} G = \{(a, x) \in A \times G \mid \varphi(a) = \psi(x)\}$ is the fibre product of $A \times G$ over $\overline{G}$. Note that it fits in the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r] \arrow[d, equal] & A \times_{\overline{G}} G \arrow[r] \arrow[d] & G \arrow[r] \arrow[d, two heads, "\psi"] & 1 \\
0 \arrow[r] & A \arrow[r] & E \arrow[r, "\varphi"] & \overline{G} \arrow[r] & 1
\end{tikzcd}$$

via the canonical embedding of A and projections on $A \subset E$ and G. The choice of a continuous section σ for φ induces a section $G \to A \times_{\overline{G}} G$ of the projection defined by $x \mapsto (\sigma(\varphi(x)), x)$. Observe that the G-module structure that A inherits via this section is the same as the one induced by ψ, namely $xa = \psi(x)a$ for $x \in G$.

Now we look at the cohomology classes associated to X and Y via the described sections (see the proof of Theorem 2.1.8): the class $c_X \in H^2(\overline{G}, A)$ of X is represented by the inhomogenous cocycle

$$f(\overline{x}, \overline{y}) = \sigma(\overline{x}) + \sigma(\overline{y}) - \sigma(\overline{xy})$$

for $\overline{x}, \overline{y} \in \overline{G}$, while the class $c_Y \in H^2(G, A)$ of Y is represented by

$$g(x, y) = (\sigma(\varphi(x)) + \sigma(\varphi(y)) - \sigma(\varphi(xy)), 1)$$

for $x, y \in G$, which corresponds to

$$\sigma(\varphi(x)) + \sigma(\varphi(y)) - \sigma(\varphi(xy)) = f(\varphi(x), \varphi(y))$$

via the projection $A \times_{\overline{G}} G \to E$. But $f(\varphi(x), \varphi(y))$ is precisely the cocycle representing the class of $\inf(c_X)$ through the inflation map $H^2(\overline{G}, A) \to H^2(\overline{G}, A)$, whence $c_Y = \inf(c_X)$. Summarising,

Proposition 2.2.10. *For an epimorphism* $\psi : G \to \overline{G}$ *of profinite groups, and an extension*

$$X : 0 \to A \to E \xrightarrow{\varphi} \overline{G} \to 1$$

of a finite abelian group A *by* $\overline{G}$ *whose corresponding cohomology class is* $c \in H^2(\overline{G}, A)$, $\inf(c) \in H^2(G, A)$ *corresponds to the pullback extension*

$$0 \to A \to A \times_{\overline{G}} G \to G \to 1.$$

2.3 Cohomological dimension

As the last cohomological ingredient we need, we look at a fundamental invariant for profinite groups.

Definition 2.3.1. *For a prime* p, *the* p-cohomological dimension $\mathrm{cd}_p(G)$ *of a profinite group* G *is the smallest integer* $n \geqslant 0$, *if it exists, such that* $H^k(G, A)_p = 0$ *for all* $k > n$ *and all torsion* G-*modules* A. *Otherwise, we set* $\mathrm{cd}_p(G) = \infty$ *if such an integer does not exist.*

We let $\mathrm{cd}(G) = \sup_p \mathrm{cd}_p(G)$ *and call it the* cohomological dimension *of* G.

Remark 2.3.2. i) By Corollary 2.2.4, $\mathrm{cd}(G)$ is either ∞ or the minimum integer $n \geqslant 0$ such that $H^k(G, A) = 0$ for all $k > n$ and all torsion G-module A.

ii) If we remove the hypothesis that A be torsion, we get the definition of p-*strict* cohomological dimension $\mathrm{scd}_p(G)$, which is related to $\mathrm{cd}_p(G)$ by the inequalities $\mathrm{cd}_p(G) \leqslant \mathrm{scd}_p(G) \leqslant \mathrm{cd}_p(G) + 1$ (see [Ser97], Proposition 13 for a proof).

First of all, we want to minimize the set of G-modules that we have to check in order to compute cohomological dimension. A G-module A is called *simple* if it has no nontrivial G-submodule.

Remark 2.3.3. Since the orbit of an element $a \in A$ under the action of G is finite, a simple G-module is always a finitely generated abelian group. Consequently, there exists a prime p such that the p-multiplication $A \xrightarrow{p} A$ is not surjective. Then $pA = 0$ by simplicity of A, so that A is in fact finite and such a p is unique.

Proposition 2.3.4. *For a profinite group G, $\mathrm{cd}_p(G) \leqslant n$ if and only if $H^{n+1}(G, A) = 0$ for all* simple p-primary G-*modules A.*

Proof. One implication is clear. For the nontrivial one, assume $H^{n+1}(G, A) = 0$ whenever A is simple p-primary and consider first a nontrivial simple submodule A' of a (non simple) finite p-primary G-module A. The short exact sequence

$$0 \to A' \to A \to A/A' \to 0$$

induces the long exact sequence

$$\cdots \to H^{n+1}(G, A') \to H^{n+1}(G, A) \to H^{n+1}(G, A/A') \to \cdots$$

Assuming inductively that $H^{n+1}(G, B) = 0$ if $|B| < |A|$, we get that both $H^{n+1}(G, A')$ and $H^{n+1}(G, A/A')$ are zero, hence also $H^{n+1}(G, A) = 0$.

For a general torsion module A, we can write A_p as the direct limit of its finite G-submodules B, and therefore we have

$$H^{n+1}(G, A)_p = H^{n+1}(G, A_p) = \varinjlim_{B} H^{n+1}(G, B) = 0$$

by Corollaries 2.1.12 and 2.2.4.

To extend the result to arbitrary degrees $k > n$, we argue by dimension shifting: namely, consider the short exact sequence

$$0 \to A \xrightarrow{\iota} \mathrm{Coind}^G(A) \to \mathrm{coker}(\iota) \to 0;$$

applying Proposition 2.1.14 to the induced long exact sequence in cohomology and arguing by induction, we get $H^{k+1}(G, A) \simeq H^k(G, \mathrm{coker}(\iota)) = 0$. □

The situation is particularly easy when G is a pro-p-group.

Proposition 2.3.5. *If G is a pro-p-group, the only simple p-primary G-module is $\mathbf{Z}/p\mathbf{Z}$ (with the trivial action of G).*

Proof. Let A be a simple p-primary G module. Then A must be finite and in fact elementary abelian by Remark 2.3.3. Thus, the intersection of stabilizers $U = \bigcap_{a \in A} G_a$ is an open subgroup of G, and so is its core U_G. Therefore, viewing A as a simple G/U_G-module, we may assume G to be finite.

We then claim that the action of G must be trivial. Otherwise, $A^G = 0$ because A is simple and $A^G \neq A$, so that all nonzero elements of A lie in an orbit of the G-action whose cardinality is divisible by p: this gives $|A| \equiv 1 \pmod p$, a contradiction since A is a finite p-group. Consequently, A must be a simple finite p-group, and thus isomorphic to $\mathbf{Z}/p\mathbf{Z}$. □

Corollary 2.3.6. *For a pro-p-group G, $\mathrm{cd}(G) \leqslant n$ if and only if $H^{n+1}(G, \mathbf{Z}/p\mathbf{Z}) = 0$.*

We have the following result about cohomological dimension of subgroups.

Theorem 2.3.7. *For a subgroup $H < G$, $\mathrm{cd}_p(H) \leqslant \mathrm{cd}_p(G)$. Equality holds in the following cases:*

i) if $p \nmid [G : H]$;

ii) if $\mathrm{cd}_p(G) < \infty$ and $p^\infty \nmid [G : H]$.

Proof. The inequality follows from Shapiro's lemma (see Proposition 2.2.8): if $k > \mathrm{cd}_p(G)$, and A is a torsion G-module, so is $\mathrm{Coind}_H^G(A)$, whence

$$H^k(H, A)_p = H^k(G, \mathrm{Coind}_H^G(A))_p = 0.$$

Now, if (i) holds, the restriction $\mathrm{res}_H^G : H^k(G, A)_p \to H^k(H, A)_p$ is injective by Proposition 2.2.5. Thus, if $H^k(H, A)_p = 0$, so is $H^k(G, A)_p$.

Assuming (ii), we first suppose $H < G$ is open. Let $n = \mathrm{cd}_p(G)$ and choose a torsion G-module A such that $H^n(G, A)_p \neq 0$. If T is a (finite) transversal of H in G, the map $\pi : \mathrm{Coind}_H^G(A) \to A$ defined by $\pi(f) = \sum_{t \in T} t^{-1} f(t)$ is a G-homomorphic section of the canonical embedding $\iota : A \to \mathrm{Coind}_H^G(A)$, and is therefore surjective.

The short exact sequence

$$0 \to \ker(\pi) \to \mathrm{Coind}_H^G(A) \xrightarrow{\pi} A \to 0$$

induces the exact sequence

$$H^n(G, \mathrm{Coind}_H^G(A))_p \to H^n(G, A)_p \to H^{n+1}(G, \ker(\pi)) = 0,$$

so that the first map is surjective and $H^n(G, \mathrm{Coind}_H^G(A))_p = H^n(H, A)_p \neq 0$.

For the general case, suppose p^t divides exactly $[G : H]$, where t is finite by hypothesis, and choose p-Sylows H_p, G_p of H, G respectively in such a way that $H_p < G_p$. Since

$$[G_pU/U : H_pU/U] \leqslant p^t$$

for all open normal subgroups $U < G$, $[G_p : H_p] = p^s < \infty$ for some finite s. Then, by the previous case, $\mathrm{cd}_p(G_p) = \mathrm{cd}_p(H_p)$, and by (i) they are equal to $\mathrm{cd}_p(G)$ and $\mathrm{cd}_p(H)$ respectively. □

Corollary 2.3.8. *Let* G_p *be a* p*-Sylow of a profinite group* G*. Then* $\mathrm{cd}_p(G) = \mathrm{cd}_p(G_p)$.

Corollary 2.3.9. *For a profinite group* G*,*

i) $\mathrm{cd}_p(G) = 0$ *if and only if* $p \nmid \#G$*;*

ii) if $\mathrm{cd}_p(G) \neq 0, \infty$*, then* $p^\infty \mid \#G$.

Proof. For (i), we may suppose that G is a pro-p-group; then obviously $\mathrm{cd}_p(G) = \mathrm{cd}_p(1) = 0$ if $p \nmid \#G$. Conversely, suppose $\mathrm{cd}_p(G) = 0$: considering $\mathbf{Z}/p\mathbf{Z}$ as a trivial G-module, we get

$$H^1(G, \mathbf{Z}/p\mathbf{Z}) = \mathrm{Hom}(G, \mathbf{Z}/p\mathbf{Z}) = 0,$$

which necessarily implies $G = 1$.

Statement (ii) follows from Theorem 2.3.7: if $p^\infty \nmid \#G$ and $\mathrm{cd}_p(G)$ is finite, we have $0 = \mathrm{cd}_p(1) = \mathrm{cd}_p(G)$. □

As a consequence, p-cohomological dimension is a rather sloppy invariant for finite groups G, since it is either ∞ or 0 according to whether p does or does not divide $|G|$. We shall see in a while that, for infinite G, this is not the case.

Chapter 3

Strong Embedding Problems

We shall now begin the study of our main topic of interest: embedding problems.

Definition 3.0.1. *Let* G *be a profinite group. An embedding problem for* G *is a diagram of profinite groups*

$$\begin{tikzcd} & & & G \arrow[d, two heads, "\varphi"] & \\ 1 \arrow[r] & K \arrow[r] & A \arrow[r, "\alpha"] & B \arrow[r] & 1 \end{tikzcd} \tag{3.1}$$

where the row is exact, i.e. A *is an extension of* B *by* K*, and* φ *is a surjective map.*

A (weak) solution *to an embedding problem (3.1) is a map* $\overline{\varphi} : G \to A$ *lifting* φ*, i.e. such that* $\alpha \circ \varphi = \overline{\varphi}$*. We say that a solution is* strong *(or* proper*) if it is surjective, and an embedding problem is* solvable *(resp.* strongly solvable*) if it admits a* solution *(resp. a* strong solution*).*

Embedding problems (as well as their name) originate in Galois theory, and give a generalization of the inverse Galois problem. Let $E \supset F \supset k$ be a tower of Galois extensions of k, and let G, B be the Galois groups of E, F over k respectively. Then there is a natural projection map $\varphi : G \to B$ induced by the restriction of k-automorphisms of E to k-automorphisms of F.

If $\alpha : A \to B$ is a surjective map of profinite groups, the problem of finding an intermediate extension $E \supset M \supset F \supset k$ such that $G(M|k) = A$ and the projection map $G(M|k) \to G(F|k)$ is exactly α is solved (via Galois correspondence) precisely when the corresponding embedding problem for G has a strong solution.

As we shall see, though, embedding problems prove a useful tool already in the context of profinite group theory per se: our main result, in this chapter, will be the characterization of free pro-$\mathfrak{c}$-groups (wich we are now going to introduce) for full classes $\mathfrak{c}$ of finite groups, via the existence of strong solutions to a specific class of embedding problems.

3.1 Free pro-$\mathfrak{c}$-groups

Recall that a sequence $(x_i \mid i \in I)$ of elements a profinite group G *converges to* 1 if any open subgroup $U < G$ contains almost all (i.e. all but finitely many) elements x_i. Also, a map $\mu : X \to G$ *converges to* 1 if $(\mu(x) \mid x \in X)$ converges to 1 in G.

Throughout this section, $\mathfrak{c}$ will be a fixed class of finite groups closed under taking subgroups, quotients and finite direct products.

Definition 3.1.1. *Let* X *be a set. A* free pro-$\mathfrak{c}$-group *over* X *is a pro-*$\mathfrak{c}$*-group* F *together with a map* $\iota : X \to F$ *such that*

i) ι *converges to* 1*;*

ii) if G *is a pro-*$\mathfrak{c}$*-group, and* $\mu : X \to G$ *is a map converging to* 1*, there exists a unique map* $\varphi : F \to G$ *such that* $\varphi \circ \iota = \mu$*.*

Observe that $\iota(X)$ is a set of generators converging to 1 for the free pro-$\mathfrak{c}$-group on X. Also, one may verify that property (ii) holds by checking it in the case when G is a finite $\mathfrak{c}$-group.

Proposition 3.1.2. *For each set* X*, there exists a free pro-*$\mathfrak{c}$*-group* F *on* X*. Moreover,* F *is determined up to unique isomorphism.*

Proof. Take F_0 to be the abstract free group on the set X, with $\iota_0 : X \to F_0$ the immersion of X in F_0 as a basis, and let $F = \varprojlim_U F_0/U$, where U varies through the normal finite index subgroups of F_0 containing almost all elements of X and such that F_0/U is a $\mathfrak{c}$-group. Let ι be the map $X \to F$ induced by the natural projections

$$\pi_U : X \xrightarrow{\iota_0} F_0 \to F_0/U,$$

which evidently converges to 1, since for all U as above there is only a finite number of elements $x \in X$ such that $\pi_U(x) \neq 0$.

If G is a pro-$\mathfrak{c}$-group, and $\mu : X \to G$ converges to 1, it induces a homomorphism $\varphi_0 : F_0 \to G$ such that $\varphi_0 \circ \iota_0 = \mu$ by the universal property of F_0. If V varies through the open normal subgroups of G then, the subgroups $\varphi_0^{-1}(V)$ are such that $F_0/\varphi_0^{-1}(V)$ is a $\mathfrak{c}$-group, and contain almost all elements of X, and the maps

$$F_0/\varphi_0^{-1}(V) \to G/V$$

induced by φ_0 yield in turn a continuous homomorphism

$$\varphi : F \to \varprojlim_V F_0/\varphi_0^{-1}(V) \to \varprojlim_V G/V = G,$$

which verifies $\varphi \circ \iota = \mu$ by construction. Also, φ is clearly unique, since $\iota(X)$ generates F. We therefore established existence for F.

Uniqueness follows from a standard argument. Namely, given a diagram

$$\begin{tikzcd} F & & F' \\ & X \arrow[ul, "\iota"] \arrow[ur, "\iota'"'] & \end{tikzcd}$$

with F, F' free pro-$\mathfrak{c}$-groups on X, by the universal property of F, F' we get unique maps $\varphi : F \to F', \psi : F' \to F$ making the triangle commute. By the uniqueness property, it is straightforward to see that $\psi \circ \varphi, \varphi \circ \psi$ are the identities of F, F' respectively. □

We write $F_{\mathfrak{c}}(X)$ to refer to the free pro-$\mathfrak{c}$-group on the set X. The following corollary is immediate from the above construction (see Remark 1.2.2).

Corollary 3.1.3. *Let X be a finite set. Then, $F_{\mathfrak{c}}(X)$ is uniquely characterized as the pro-$\mathfrak{c}$-completion of the abstract free group on X.*

Proposition 3.1.4. *Let (F, ι) be a free pro-$\mathfrak{c}$-group on the set X.*

i) The set $\iota(X)$ does not contain 1, and ι is injective.

ii) $|X| = d(F)$.

Proof. Let $C = \langle a \rangle$ be a cyclic $\mathfrak{c}$-group, and fix $x \in X$. Then the homomorphism $F \to C$ induced by the assignment $x \mapsto a, X \setminus \{x\} \mapsto 1$ must be surjective, and therefore $\iota(x) \neq 1$. If X has more than one element, take $G = \langle a, b \rangle$ a 2-generated $\mathfrak{c}$-group, and let $x \mapsto a, y \mapsto b, X \setminus \{x, y\} \mapsto 1$: then we must have $\iota(x) \neq \iota(y)$, since the induced map is an epimorphism. This proves (i).

Statement (ii) follows from Proposition 1.3.4 if $d(F) \geqslant \aleph_0$. Otherwise, let $d(F) = n$ finite, and fix a subset $\{x_1, \dots, x_n\} \subset X$ (note $|X| \geqslant d(F)$). Let $Y = \{y_1, \dots y_n\}$ be a system of generators converging to 1 for F and define $\mu : X \to F$ by the assignment $x_i \mapsto y_i$ and $x \mapsto 1$ for $x \neq x_i$. Then μ extends to a map $\varphi : F \to F$, which is surjective since the y_i generate F. By Proposition 1.3.11, φ is then an isomorphism, and therefore $X \setminus \{x_1, \dots, x_n\}$ must be empty by (i). □

Due to the above Proposition, we may always see a set X as a subset of the free pro-$\mathfrak{c}$-group F on X, and we call it a *basis* for F. Also, the cardinality of a base for F is independent of its choice, and equals $d(F)$; we shall refer to it as the *rank* of F.

It is evident that two free pro-$\mathfrak{c}$-groups of the same rank are isomorphic, an isomorphism being induced by a bijection between two of their bases. Therefore, if κ is a cardinal, we shall use the notation $F_{\mathfrak{c}}(\kappa)$ to refer to the (isomorphism class of the) free pro-$\mathfrak{c}$-group of rank κ. In particular, the free pro-$\mathfrak{c}$-group of countable rank will be denoted by $F_{\mathfrak{c}}(\omega)$.

Examples 3.1.5. i) If $\mathfrak{f}$ is the class of all finite groups, $F_{\mathfrak{f}}(1) = \widehat{\mathbf{Z}}$. More generally, if π is a set of primes, the free pro-π-group of rank 1 is $\mathbf{Z}_\pi = \prod_{p \in \pi} \mathbf{Z}_p$. These statements both follow immediately from Corollary 3.1.3. Also, since all the quotients of $\mathbf{Z}$ are, say, abelian, or solvable, $\widehat{\mathbf{Z}}$ is the free proabelian, or prosolvable, group of rank 1 as well.

ii) The free proabelian group on a set X is the direct product $\prod_{x \in X} \widehat{\mathbf{Z}}$, with $\iota(x)$ being the sequence with 1 in the position corresponding to $x \in X$ and 0 everywhere else.

This follows from the fact that, if a map $\mu : X \to A$ to a finite abelian group converges to 1, $\mu(x) = 0$ for almost all $x \in X$ since A is discrete; if $Y = \{x \in X \mid \mu(x) \neq 0\}$, μ is then easily extended to the finite product $\widehat{\mathbf{Z}}^{\times Y}$, and may instead be defined as the zero map on $\widehat{\mathbf{Z}}^{\times X \setminus Y}$.

iii) In general, one may define a suitable concept of free pro-$\mathfrak{c}$ product, by reasonably modifying the universal property for abstract free products. It is then fairly easy to verify that, if X is a finite set, $F_{\mathfrak{c}}(X)$ is the free pro-$\mathfrak{c}$ product of $|X|$ copies of $\mathbf{Z}_{\widehat{\mathfrak{c}}}$, the pro-$\mathfrak{c}$ completion of $\mathbf{Z}$.

Remark 3.1.6. A natural way to define free pro-$\mathfrak{c}$-groups is as the free objects in the category of pro-$\mathfrak{c}$-groups, with respect to the forgetful functor taking values in the category of profinite spaces; explicitly, this gives a pro-$\mathfrak{c}$-group F with a continuous function $\iota : X \to F$ from a profinite space X such that, for any continuous function $\mu : X \to G$ to a pro-$\mathfrak{c}$-group, there exists a unique map $\varphi : F \to G$ such that the diagram

$$\begin{tikzcd}
F \arrow[r, "\varphi"] & G \\
X \arrow[u, "\iota"] \arrow[ur, "\mu"'] &
\end{tikzcd}$$

commutes. A similar definition can be given considering *pointed* profinite spaces.

Then, one may easily see that $F_{\mathfrak{c}}(X)$, where X is a set, is in fact a free pro-$\mathfrak{c}$-group on a pointed profinite space $(\widetilde{X}, \star)$: namely, $\widetilde{X}$ is the Alexandrov compactification of X seen as a discrete space, $\star$ being the adjoined point ($\widetilde{X}$ is in fact a profinite space, being compact, Hausdorff and totally disconnected).

Moreover, using the characterization of free pro-$\mathfrak{c}$-groups on a set that we shall prove in the next section, one may also show (see [RZ10], Proposition 3.5.12) that every free pro-$\mathfrak{c}$-group on a pointed space is also a free pro-$\mathfrak{c}$-group according to Definition 3.1.1.

Proposition 3.1.7. *Every pro-$\mathfrak{c}$-group is a quotient of a free pro-$\mathfrak{c}$-group.*

Proof. Let G be a pro-$\mathfrak{c}$-group, and pick a set X of generators converging to 1 for G. Let F be the free pro-$\mathfrak{c}$-group on the set X: the inclusion map $X \to G$ converges to 1, and therefore induces a surjective map $F \to G$. In particular, notice that we may choose $d(F) = d(G)$. □

3.2 Characterization of free pro-$\mathfrak{c}$-groups

In the current section, $\mathfrak{c}$ will always denote a full class of finite groups. We aim to characterise free pro-$\mathfrak{c}$-groups in terms of strong embedding problems.

We deal with the finitely generated case first.

Lemma 3.2.1. *Let $\varphi : G \to H$ be an epimorphism of profinite groups with $d(G) \leqslant n$ finite, and suppose $H = \overline{\langle h_1, \dots, h_n \rangle}$. There exist $g_1, \dots, g_n \in G$ such that $\varphi(g_i) = h_i$ and $G = \overline{\langle g_1, \dots, g_n \rangle}$.*

Proof. Assume G finite first. For a subgroup $L < G$ and a n-uple $h = (h_1, \dots, h_n) \in H^n$, let $t_L(h)$ be the number of n-uples $(g_1, \dots, g_n)$ such that $\langle g_1, \dots, g_n \rangle = L$ and $\varphi(g_i) = h_i$. Then,

$$t_G(h) = |\ker(\varphi)|^n - \sum t_L(h),$$

with L ranging through the proper subgroups of G such that $\varphi(L) = H$. Since G has a set of n generators, there exists $h \in H^n$ such that $t_G(h) > 0$. It thereby suffices to prove that $t_G(h)$ is independent of the choice of h, which can be seen by assuming inductively that $t_L(h)$ does not depend on h for every surjection $L \to H$ such that $|L| < |G|$ and using the above formula for $t_G(h)$.

For the general case, consider the epimorphisms $\varphi_U : G/U \to H/\varphi(U)$ for $U < G$ open normal and observe that $\varphi = \varprojlim_U \varphi_U$. If we let $h^U \in H/\varphi(U)$ the image of $h \in H$ via the projection $H \to H/\varphi(U)$, we then have $H/\varphi(U) = \langle h_1^U, \dots, h_n^U \rangle$ for all U. Also, the sets X_U of n-uples $(\overline{g}_1, \dots, \overline{g}_n) \in G/U$ such that $\varphi_U(\overline{g}_i) = h_i^U$ and $\langle \overline{g}_1, \dots, \overline{g}_n \rangle = G/U$ are nonempty by the finite case. Therefore, an element $(g_1, \dots, g_n) \in \varprojlim X_U \neq \emptyset$ gives the wanted n-uple. □

Theorem 3.2.2. *Let G be a pro-$\mathfrak{c}$-group with $d(G) = n$ finite. Then, G is a free pro-$\mathfrak{c}$-group if and only if any embedding problem (3.1) of pro-$\mathfrak{c}$-groups with $d(A), d(B) \leqslant n$ is strongly solvable.*

Proof. If G is free over $\{x_1, \dots, x_n\}$, and $B = \overline{\langle b_1, \dots, b_n \rangle}$, choose $a_1, \dots, a_n$ such that $A = \overline{\langle a_1, \dots, a_n \rangle}$ and $\alpha(a_i) = b_i$. The map $G \to A$ induced by the assignment $x_i \mapsto a_i$ is then a strong solution to the given embedding problem.

Conversely, let $F = F_{\mathfrak{c}}(n)$ and choose an epimorphism $F \to G$. The identity of G then lifts to an isomorphism $G \xrightarrow{\sim} F$. □

The infinitely generated case is more involved. We begin with a definition.

Definition 3.2.3. *If* G *is a pro-*$\mathfrak{c}$*-group, we say that* G *has the* strong lifting property (SLP) *if any embedding problem*

$$\begin{tikzcd} & & & G \arrow[d, two heads, "\varphi"] & \\ 1 \arrow[r] & K \arrow[r] & A \arrow[r, "\alpha"] & B \arrow[r] & 1 \end{tikzcd}$$

of pro-$\mathfrak{c}$*-groups such that* $w_0(A) \leqslant w_0(G), w_0(B) < w_0(G)$ *is strongly solvable.*

Notice that the hypoteses on the local weight of A and B are necessary to make the definition non vacuous: since we wish for an epimorphism $\overline{\varphi} : G \to A$ we surely need $w_0(A) \leqslant w_0(G)$; also, if we allowed $w_0(B) = w_0(G)$ we would get a surjective lift of the identity of G, and therefore an isomorphism, for any epimorphism $\varphi : A \to G$, which is clearly not possible. We shall therefore name *admissible* an embedding problem satisfying the above conditions.

Our goal is to prove that, if $d(G) \geqslant \aleph_0$, G has the SLP if and only if it is a free pro-$\mathfrak{c}$-group. The first step is a reduction on the class of problems to check.

Lemma 3.2.4. *Let* G *be a pro-*$\mathfrak{c}$*-group, and suppose that an admissible embedding problem for* G *is solvable whenever* K *is a finite minimal normal subgroup of* A*. Then,* G *has the SLP.*

Proof. Consider an admissible embedding problem of pro-$\mathfrak{c}$-groups

$$\begin{tikzcd} & & & G \arrow[d, two heads, "\varphi"] & \\ 1 \arrow[r] & K \arrow[r] & A \arrow[r, "\alpha"] & B \arrow[r] & 1 \end{tikzcd}$$

and take a chain

$$K = K_0 > K_1 > \cdots > K_\mu = 1$$

as in Corollary 1.3.9.

For all $\lambda \leqslant \mu$, we have an induced embedding problem

$$\begin{tikzcd} & & & G \arrow[d, two heads, "\varphi"] & \\ 1 \arrow[r] & K \arrow[r] \arrow[d] & A \arrow[r, "\alpha"] \arrow[d] & B \arrow[r] \arrow[d, equal] & 1 \\ 1 \arrow[r] & K/K_\lambda \arrow[r] & A/K_\lambda \arrow[r] & B \arrow[r] & 1 \end{tikzcd}$$

and it is enough to show, by induction, that the induced problem has a strong solution $\varphi_\lambda : G \to A/K_\lambda$ which is compatible with the already constructed solutions for $\nu < \lambda$, that is the triangle

$$\begin{tikzcd} & G \arrow[dl, "\varphi_\lambda"'] \arrow[dr, "\varphi_\nu"] & \\ A/K_\lambda \arrow[rr] & & A/K_\nu \end{tikzcd}$$

is commutative. This is clear for $\lambda = 0$.

If $\lambda = \nu + 1$, the problem

$$\begin{tikzcd} & & & G \arrow[d, two heads, "\varphi_\lambda"] & \\ 1 \arrow[r] & K_\nu/K_\lambda \arrow[r] & A/K_\lambda \arrow[r, "\alpha"] & A/K_\nu \arrow[r] & 1 \end{tikzcd}$$

is admissible: this follows by condition (iii) on the chain if K is infinite while, if K is finite, we must have $w_0(A) = w_0(B) < w_0(G)$. Since K_ν/K_λ is finite and minimal normal in A/K_λ, it has a strong solution φ_λ, satisfying the compatibility condition by construction.

Finally, if λ is a limit, then $K_\lambda = \bigcap_{\nu<\lambda} K_\nu$. Therefore, $K/K_\lambda = \varprojlim_{\nu<\lambda} K/K_\nu$, and φ_λ can be taken as the inverse limit of maps φ_ν. □

Proposition 3.2.5. *If F is a free pro-𝔠-group of infinite rank, F has the SLP.*

Proof. Consider an admissible embedding problem

$$\begin{tikzcd} & & & F \arrow[d, two heads, "\varphi"] & \\ 1 \arrow[r] & K \arrow[r] & A \arrow[r, "\alpha"] & B \arrow[r] & 1 \end{tikzcd}$$

where we may assume K finite by the previous lemma, and let X be a basis for F.

We claim that, if $H = \ker(\varphi)$, $|X \cap H|$ is infinite. In fact, let $\mathcal{U} = \{U_i \mid i \in I\}$ be a fundamental system of neighbourhoods of 1 made of open normal subgroups of B. Recall that $\bigcap_i U_i = 1$, so that

$$|X \setminus H| = \left| X \setminus \varphi^{-1}\left(\bigcap_i U_i\right)\right| = \left|\bigcup_i X \setminus \varphi^{-1}(U_i)\right|.$$

Since X converges to 1, $X \setminus \varphi^{-1}(U_i)$ is finite for all i, and therefore $|X \setminus H| = |\mathcal{U}|$, which is strictly smaller than $|X|$ since $w_0(B) < w_0(F)$. Hence, $|X \cap H| = |X|$ is infinite.

Now, to get a strong solution for the above problem, it is enough to construct a map $\mu : X \to A$ convergent to 1 such that $\mu(X)$ generates A. To do so, choose a bijection $\psi : Y \to K$, where Y is a (finite) subset of $X \cap H$, ad let $\sigma : B \to A$ be a continuous section of α. Then, the map $\mu : X \to A$, defined piecewise as ψ on Y and as the composition $\sigma \circ \varphi$ on $X \setminus Y$, converges to 1 as X does and $\sigma \circ \varphi$ is continuous; also, since φ is surjective and $A = K \cdot \sigma(B)$, $\mu(X)$ generates A. □

Theorem 3.2.6. *Let* G *be a pro-*$\mathfrak{c}$*-group with* $d(G) = \kappa \geqslant \aleph_0$*. Then* G *has the the SLP if and only if* G *is a free pro-*$\mathfrak{c}$*-group of rank* κ*.*

Proof. One implication is the above proposition. For the converse, let $F \simeq F_{\mathfrak{c}}(\kappa)$, and choose chains

$$F = F_0 > F_1 > \cdots > F_\kappa = 1$$

$$G = G_0 > G_1 > \cdots > G_\kappa = 1$$

for F, G respectively in such a way that their quotients are $\mathfrak{c}$-groups and, for all $\lambda < \kappa$, $w_o(G/G_\lambda) < w_o(G), w_o(F/F_\lambda) < w_o(F)$; also, if λ is a limit, we assume $F_\lambda = \bigcap_{\nu<\lambda} F_\nu, G_\lambda = \bigcap_{\nu<\lambda} G_\nu$.

We build inductively new chains

$$F = F'_0 > F'_1 > \cdots > F'_\kappa = 1$$

$$G = G'_0 > G'_1 > \cdots > G'_\kappa = 1$$

so that in addition, for all $\lambda \leqslant \kappa$,

i) $F'_\lambda < F_\lambda, G'_\lambda < G_\lambda$ and $w_o(F/F'_\lambda) \leqslant w_o(F/F_\lambda), w_o(G/G'_\lambda) \leqslant w_o(G/G_\lambda)$;

ii) there exist compatible isomorphisms $\varphi_\lambda : F/F_\lambda \to G/G_\lambda$, i.e. such that, for all $\nu < \lambda$, the diagram

$$\begin{tikzcd} F/F_\lambda \arrow[r, "\varphi_\lambda"] \arrow[d] & G/G_\lambda \arrow[d] \\ F/F_\nu \arrow[r, "\varphi_\nu"] & G/G_\nu \end{tikzcd}$$

commutes.

We set φ_0 the zero map.

If $\lambda = \nu + 1$, let $H = F_\lambda \cap F'_\nu, K = G_\lambda \cap G'_\nu$. The problem

$$\begin{tikzcd} & & G \arrow[d, two heads] \\ F/H \arrow[r, two heads] & F/F'_\nu \arrow[r, two heads, "\varphi_\nu"] & G/G'_\nu \end{tikzcd}$$

is admissible by (i), and since H has finite index in F'_ν: then, by the SLP of G, it has a strong solution, say $\psi : G \to F/H$.

Set $G'_\lambda = K \cap \ker(\psi)$, and let $\overline{\psi} : G/G'_\lambda \to F/H$ be the epimorphism induced by ψ. By Proposition 3.2.5, the admissible problem

$$\begin{tikzcd} & F \arrow[d, two heads] \\ G/G'_\lambda \arrow[r, two heads, "\overline{\psi}"] & F/H \end{tikzcd}$$

has a strong solution $\eta : F \to G/G'_\lambda$.

If $F'_\lambda = \ker(\eta)$, η induces an isomorphism $\varphi_\lambda : F/F'_\lambda \to G/G'_\lambda$, compatible by construction. Also, as one may easily see, F'_λ and G'_λ satisfy condition (i).

Finally, if λ is a limit ordinal, let $F'_\lambda = \bigcap_{\nu<\lambda} F'_\nu, G'_\lambda = \bigcap_{\nu<\lambda} G'_\nu$, so that $F/F'_\lambda = \varprojlim_{\nu<\lambda} F/F'_\nu$ and

$$w_0(F/F'_\lambda) \leqslant \sum_{\nu<\lambda} w_0(F/F'_\nu) \leqslant \sum_{\nu<\lambda} w_0(F/F_\nu) = w_0(F/F_\lambda),$$

with G/G'_λ behaving analogously. We may then set $\varphi_\lambda = \varprojlim_{\nu<\lambda} \varphi_\nu$, and the proof is complete. □

The above characterization of free pro-$\mathfrak{c}$-groups is a generalization to arbitrary rank of the following result of K. Iwasawa (see [Iwa53]), which covers the case where the rank of G is countable. We shall return to this theorem when we prove an application of it, again due to Iwasawa, to the arithmetic theory of global fields.

Theorem 3.2.7 (Iwasawa). *If G is a pro-$\mathfrak{c}$-group with $d(G) \leqslant \aleph_0$, every embedding problem*

$$\begin{tikzcd} & & & G \arrow[d, two heads, "\varphi"] & \\ 1 \arrow[r] & K \arrow[r] & A \arrow[r, "\alpha"] & B \arrow[r] & 1 \end{tikzcd}$$

with A finite is strongly solvable if and only if $G \simeq F_{\mathfrak{c}}(\omega)$.

Proof. By Theorem 3.2.6, $G \simeq F_{\mathfrak{c}}(\omega)$ if and only if every embedding problem with $w_0(A) \leqslant \aleph_0$ and finite $w_0(B)$ has a strong solution. Now, $w_0(B) < \aleph_0$ if and only if B is finite, and by Lemma 3.2.4 we may assume K to be finite. Therefore, we may reduce to the case when A finite as well, and the result follows. □

Chapter 4

Weak Embedding Problems and Iwasawa's Theorem

We now turn to weak embedding problems: through them, we shall obtain a characterization of pro-$\mathfrak{c}$-groups G such that $\mathrm{cd}(G) \leqslant 1$, with $\mathfrak{c}$ a full class of finite groups, and see that they are precisely *projective* pro-$\mathfrak{c}$-groups. Moreover, in the case when $\mathfrak{c}$ is the class of all finite p-groups, we shall enstablish equality between projective and free pro-p-groups.

Finally, in the last section, we shall prove an arithmetic application, due to K. Iwasawa, of the characterizations we found using both strong and weak embedding problems.

In what follows, we assume that $\mathfrak{c}$ is a full class of finite groups.

4.1 Cohomological characterization of projective pro-$\mathfrak{c}$-groups

A pro-$\mathfrak{c}$-group G is said to be $\mathfrak{c}$-*projective* if it is a projective object in the category of pro-$\mathfrak{c}$-groups, i.e. the functor $\mathrm{Hom}(G, \cdot)$ preserves epimorphisms of pro-$\mathfrak{c}$-groups. Explicitly, if A, B are pro-$\mathfrak{c}$-groups and $\alpha : A \to B$ is a surjective map, every map $\varphi : G \to B$ lifts to a continuous homomorphism $\psi : G \to A$ such that $\alpha \circ \psi = \varphi$.

To check the above condition, we may in fact restrict to verify that, for any choice of a surjection $\alpha : A \to B$ of pro-$\mathfrak{c}$-groups, any *epimorphism* $G \to B$ lifts to a map $G \to A$.

Indeed, if this is the case, the diagram

$$\begin{tikzcd}
 & G \arrow[dl, dashed, "\psi"'] \arrow[d, two heads, "\varphi"] \\
\alpha^{-1}(\mathrm{im}(\varphi)) \arrow[r] \arrow[d, hook] & \mathrm{im}(\varphi) \arrow[d, hook] \\
A \arrow[r, "\alpha"] & B
\end{tikzcd}$$

where ψ exists by hypotesis and the square is commutative, shows that any map $\varphi : G \to B$ lifts to a map $G \to A$. Therefore, we get the

Lemma 4.1.1. *A pro-$\mathfrak{c}$-group G is $\mathfrak{c}$-projective if and only if any embedding problem*

$$\begin{tikzcd}
 & & & G \arrow[d, two heads, "\varphi"] & \\
1 \arrow[r] & K \arrow[r] & A \arrow[r, "\alpha"] & B \arrow[r] & 1
\end{tikzcd}$$

of pro-$\mathfrak{c}$-groups is weakly solvable.

This motivates the following generalization of $\mathfrak{c}$-projectivity to arbitrary profinite groups.

Definition 4.1.2. *A profinite group G is $\mathfrak{c}$-projective if every embedding problem*

$$\begin{tikzcd}
 & & & G \arrow[d, two heads, "\varphi"] & \\
1 \arrow[r] & K \arrow[r] & A \arrow[r, "\alpha"] & B \arrow[r] & 1
\end{tikzcd} \tag{4.1}$$

where K is a pro-$\mathfrak{c}$-group is weakly solvable.

If $\mathfrak{c}$ is the class of all finite groups, we say that G is projective. Also, if $\mathfrak{c} = \mathfrak{c}(\pi)$ is the class of all π-groups for some set of primes π, we say that G is π-projective.

Remark 4.1.3. A first example of $\mathfrak{c}$-projective pro-$\mathfrak{c}$-groups is given by free pro-$\mathfrak{c}$-groups. This comes immediately from their definition: if F is a free pro-$\mathfrak{c}$-group on the set X, and

$$\begin{tikzcd}
 & & & F \arrow[d, two heads, "\varphi"] & \\
1 \arrow[r] & K \arrow[r] & A \arrow[r, "\alpha"] & B \arrow[r] & 1
\end{tikzcd}$$

is an embedding problem of pro-$\mathfrak{c}$-groups, choose a continuous section $\sigma : B \to A$. The composition $\sigma \circ \varphi_{|X}$ then induces a (weak) solution to the above problem.

Moreover, it is easily seen that every projective pro-$\mathfrak{c}$-group G embeds in a free pro-$\mathfrak{c}$-group: just consider an epimorphism $F \to G$ from a free pro-$\mathfrak{c}$-group and lift the identity of G to an embedding $G \to F$ using $\mathfrak{c}$-projectivity of G.

The following result is an analogous version of Lemma 3.2.4 for weak solvability.

Proposition 4.1.4. *A profinite group G is $\mathfrak{c}$-projective if and only if every embedding problem (4.1) where A is finite and K is an abelian $\mathfrak{c}$-group is weakly solvable.*

We need a preliminary basic lemma.

Lemma 4.1.5. *Let A be a profinite group, and K, U be normal subgroups of A. Then the diagram*

$$\begin{tikzcd}
A/K\cap U \arrow[r] \arrow[d] & A/K \arrow[d] \\
A/U \arrow[r] & A/UK
\end{tikzcd}$$

is cartesian, i.e. $A/K\cap U$ is isomorphic to the fibre product $A/K \times_{A/UK} A/U$.

Proof. The natural map $A/K\cap U \to A/K \times_{A/UK} A/U$ given by $aK\cap U \mapsto (aK, aU)$ is clearly well defined and injective. Also, if $(bK, cU) \in A/K \times A/U$ is such that $bUK = cUK$, then $bc^{-1} = ku$ for some $k \in K$ and $u \in U$. Therefore, the element $a = k^{-1}b = uc$ is such that $aK\cap U \mapsto (bK, cU)$, whence surjectivity. □

We now turn to the proof of the above proposition.

Proof (of Proposition 4.1.4). First, we show that we may reduce to asking that embedding problems be solvable whenever K is a $\mathfrak{c}$-group.

If that is the case, choose an embedding problem (4.1) with K a pro-$\mathfrak{c}$-group. Consider the set of pairs (N, ψ), where N is a normal subgroup of A contained in K and $\psi : G \to A/N$ is a solution to the induced embedding problem

$$\begin{tikzcd}
 & & & G \arrow[d, two heads, "\varphi"] & \\
1 \arrow[r] & K/N \arrow[r] & A/N \arrow[r, "\alpha"] & B \arrow[r] & 1
\end{tikzcd}$$

ordered by $(N, \psi) \leqslant (N', \psi')$ if $N' < N$ and ψ' lifts ψ. This set is non-empty, and an ascending chain of pairs $(N_\lambda, \psi_\lambda)$ is bounded from above by the pair $(\bigcap_\lambda N_\lambda, \psi)$, where ψ is the inverse limit of maps ψ_λ, since $A/\bigcap_\lambda N_\lambda = \varprojlim_\lambda A/N_\lambda$: by Zorn's lemma, there exists a maximal element (N, ψ); we are to show that $N = 1$.

Suppose this is not the case, and choose an open normal subgroup $U < A$ such that $N' = U \cap N \lneq N$; then N' is open in N. If $\widetilde{A}/N'$ is the preimage of $\mathrm{im}(\psi)$ in A/N', the problem

$$\begin{tikzcd}
 & & & G \arrow[d, two heads, "\psi"] & \\
1 \arrow[r] & N/N' \arrow[r] & \widetilde{A}/N' \arrow[r] & \mathrm{im}(\psi) \arrow[r] & 1
\end{tikzcd}$$

has a solution $\widetilde{\psi}$, since N/N' is a $\mathfrak{c}$-group. Consequently, the diagram

$$\begin{tikzcd}
 & & & G \arrow[dl, "\widetilde{\psi}"'] \arrow[d, two heads, "\psi"] & \\
1 \arrow[r] & N/N' \arrow[r] \arrow[d, equal] & \widetilde{A}/N' \arrow[r] \arrow[d, hook] & \mathrm{im}(\psi) \arrow[r] \arrow[d, hook] & 1 \\
1 \arrow[r] & N/N' \arrow[r] & A/N' \arrow[r] & A/N \arrow[r] & 1
\end{tikzcd}$$

shows the existence of a map $\psi' : G \to A/N'$ such that the pair (N', ψ') is strictly larger than (N, ψ), a contradiction.

Now, we show that we may also assume A to be finite. Suppose that any embedding problem with A finite and K a $\mathfrak{c}$-group is weakly solvable, and consider an embedding problem (4.1) such that K is a $\mathfrak{c}$-group. Pick an open normal subgroup $U < A$ such that $U \cap K = 1$ (U exists since K is finite), and consider the induced problem

$$\begin{tikzcd}
 & & & G \arrow[d, two heads] & \\
1 \arrow[r] & K \arrow[r] & A/U \arrow[r] & B/\alpha(U) \arrow[r] & 1
\end{tikzcd}$$

where the vertical map is the composition of φ with the natural projection. Since A/U is finite, it has a solution $\overline{\psi} : G \to A/U$, and the diagram

$$\begin{tikzcd}
 & & & G \arrow[d, two heads, "\varphi"] \arrow[ddl, "\overline{\psi}"] & \\
1 \arrow[r] & K \arrow[r] \arrow[d, equal] & A \arrow[r, "\alpha"] \arrow[d] & B \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & K \arrow[r] & A/U \arrow[r] & B/\alpha(U) \arrow[r] & 1
\end{tikzcd}$$

where the right hand square is cartesian by Lemma 4.1.5, shows the existence of a solution $\psi : G \to A$ to the original problem, induced by the maps $\varphi, \overline{\psi}$.

Finally, assume that any embedding problem (4.1) is solvable whenever A is finite and K is an abelian $\mathfrak{c}$-group: we show, by induction on the order of K, that any embedding problem (4.1) with A finite and K a non necessarily abelian $\mathfrak{c}$-group is weakly solvable. The case $K = 1$ is trivial.

If $K \neq 1$ is not a minimal normal subgroup in A, then pick $N \lneq K$ normal in A, so that the problem

$$\begin{tikzcd}
 & & & G \arrow[d, two heads, "\varphi"] & \\
1 \arrow[r] & K/N \arrow[r] & A/N \arrow[r] & B \arrow[r] & 1
\end{tikzcd}$$

has a solution $\overline{\psi} : G \to A/N$ by induction, which in turn gives a solution $\psi : G \to A$ via the diagram

$$\begin{tikzcd}
 & & & G \arrow[d, two heads, "\overline{\psi}"] & \\
1 \arrow[r] & N \arrow[r] \arrow[d, equal] & \overline{A} \arrow[r] \arrow[d, hook] & \mathrm{im}(\overline{\psi}) \arrow[r] \arrow[d, hook] & 1 \\
1 \arrow[r] & N \arrow[r] & A \arrow[r] & A/N \arrow[r] & 1
\end{tikzcd}$$

where $\overline{A} < A$ is the preimage of $\mathrm{im}(\overline{\psi}) < A/N$, and a solution $G \to \overline{A}$ exists again by induction.

If K is a minimal normal subgroup of A, instead, suppose first $K \not< \Phi(A)$: then there is a maximal subgroup $M < A$ such that $KM = A$, so that the embedding problem

$$\begin{tikzcd}
 & & & G \arrow[d, two heads, "\varphi"] & \\
1 \arrow[r] & K \cap M \arrow[r] & M \arrow[r] & B \arrow[r] & 1
\end{tikzcd}$$

is well defined and has a solution ψ' by induction, which in turn yields a solution $G \to A$ via

$$\begin{tikzcd}
 & & & G \arrow[d, two heads, "\varphi"] & \\
1 \arrow[r] & K \cap M \arrow[r] \arrow[d, hook] & M \arrow[r] \arrow[d, hook] & B \arrow[r] \arrow[d, equal] & 1 . \\
1 \arrow[r] & K \arrow[r] & A \arrow[r, "\alpha"] & B \arrow[r] & 1
\end{tikzcd}$$

Finally, if $K < \Phi(A)$, then $[K, K]$ is either 1 or K, given that K is minimal normal in A; since $\Phi(A)$ is nilpotent by Proposition 1.2.8, so is K, and subsequently we must have $[K, K] = 1$. Hence, K is abelian and the problem is solvable by assumption. □

The above proposition provides a link with cohomology: since, in order to decide whether a profinite group G is $\mathfrak{c}$-projective, we only need to check embedding problems where K is finite abelian, we are in fact dealing with extensions encoded by $H^2(B, K)$. The following result enlightens the connection.

Proposition 4.1.6. *Let G be a profinite group, and consider an embedding problem*

$$\begin{tikzcd}
 & & & G \arrow[d, two heads, "\varphi"] & \\
1 \arrow[r] & K \arrow[r] & A \arrow[r, "\alpha"] & B \arrow[r] & 1
\end{tikzcd}$$

where K is a finite abelian group. If $c \in H^2(B, K)$ is the class associated with the above extension, the problem has a solution if and only if $\inf(c) = 0 \in H^2(G, K)$.

Proof. According to Proposition 2.2.10, $\inf(\mathfrak{c})$ is precisely the class associated with the pullback

$$\begin{tikzcd}
1 \arrow[r] & K \arrow[r] \arrow[d, equal] & A \times_B G \arrow[r] \arrow[d] & G \arrow[r] \arrow[d, "\varphi"] & 1 \\
1 \arrow[r] & K \arrow[r] & A \arrow[r, "\alpha"] & B \arrow[r] & 1
\end{tikzcd},$$

and consequently it is enough to prove that there exists a solution $G \to A$ to the embedding problem if and only if the pullback extension admits a homomorphic section $G \to G \times_B A$. But this is plain: a homomorphic section induces a solution by composition with the pullback map $A \times_B G \to A$; conversely, if $\psi : G \to A$ solves the above embedding problem, the map $g \mapsto (\psi(g), g)$ is a homomorphic section for the pullback extension. □

Recall that, if $\mathfrak{c}$ is a full class of groups, by $\pi(\mathfrak{c})$ we mean the set of primes p such that $\mathfrak{c}$ contains the cyclic group of order p.

Theorem 4.1.7. *Let G be a profinite group, and let $\pi = \pi(\mathfrak{c})$. The following are equivalent.*

i) G *is* $\mathfrak{c}$*-projective.*

ii) G *is* π*-projective.*

iii) $\mathrm{cd}_p(G) \leqslant 1$ *for all* $p \in \pi$.

Proof. To show that (i) implies (iii), consider a discrete simple p-primary G-module A, with $p \in \pi$, and notice an extension

$$\begin{tikzcd}
1 \arrow[r] & A \arrow[r] & E \arrow[r] & G \arrow[r] & 1
\end{tikzcd}$$

splits, since the embedding problem

$$\begin{tikzcd}
 & & & G \arrow[d, "\mathrm{id}"] & \\
1 \arrow[r] & A \arrow[r] & E \arrow[r] & G \arrow[r] & 1
\end{tikzcd}$$

has a solution. Therefore, $H^2(G, A) = 0$ and, since A was arbitrary, we get $\mathrm{cd}_p(G) \leqslant 1$.

Now, assume $\mathrm{cd}_p(G) \leqslant 1$ for all $p \in \pi$: in order to show that G is π-projective, by Proposition 4.1.4 we may reduce to find a solution to every embedding problem

$$\begin{tikzcd}
 & & & G \arrow[d, two heads, "\varphi"] & \\
1 \arrow[r] & K \arrow[r] & A \arrow[r, "\alpha"] & B \arrow[r] & 1
\end{tikzcd},$$

with K a π-group which is a minimal normal abelian subgroup of A. Then, K contains no nontrivial characteristic subgroup, and is therefore an elementary abelian p-group for some $p \in \pi$: since $H^2(G, K) = 0$, the problem has a solution by Proposition 4.1.6.

Finally, (ii) implies (i) trivially, since $\mathfrak{c}$-groups are, in particular, π-groups. □

Finally, we obtain the following characterization of projective objects in the category of pro-$\mathfrak{c}$-groups.

Corollary 4.1.8. *If G is a pro-$\mathfrak{c}$-group, the following are equivalent.*

i) G *is* $\mathfrak{c}$*-projective.*

ii) G *is projective.*

iii) $\mathrm{cd}(G) \leqslant 1$.

iv) G *is a subgroup of a free pro-*$\mathfrak{c}$*-group.*

Proof. Assumption (i) implies (iv) by Remark 4.1.3, which also shows that a free pro-$\mathfrak{c}$-group F is $\mathfrak{c}$-projective: thus, by the above Theorem, $\mathrm{cd}_p(F) \leqslant 1$ for all $p \in \pi$, and therefore also $\mathrm{cd}(F) \leqslant 1$ by Corollary 2.3.9, since if $p \notin \pi(\mathfrak{c})$ then surely $p \nmid \#F$. Then (iii) follows by (iv) via Proposition 2.3.7. The implication of (ii) by (iii) is again contained in Theorem 4.1.7, and (ii) trivially implies (i). □

4.2 The case of pro-p-groups

We now wish to prove that a pro-p-group is projective if and only if it is a free pro-p-group.

Remark 4.2.1. i) Recall that, if G is a pro-p-group, the only discrete simple p-primary G-module is $\mathbf{Z}/p\mathbf{Z}$ (see Proposition 2.3.5), and therefore $\mathrm{cd}(G) \leqslant n$ if and only if $H^{n+1}(G, \mathbf{Z}/p\mathbf{Z}) = 0$. We shall denote $H^n(G) = H^n(G, \mathbf{Z}/p\mathbf{Z})$: it is plainly a p-torsion abelian group, and therefore an $\mathbb{F}_p$-vector space. Its dimension over $\mathbb{F}_p$ will be denoted by $\dim H^n(G)$.

ii) The Frattini subgroup of a pro-p-group G is $\Phi(G) = \overline{G'G^p}$ by proposition 1.2.14, and $G/\Phi(G)$ is Pontryagin dual to $H^1(G)$, since

$$(G/\Phi(G))^\curlyvee = \mathrm{Hom}(G/\Phi(G), \mathbf{Q}/\mathbf{Z}) = \mathrm{Hom}(G, \mathbf{Z}/p\mathbf{Z}) = H^1(G).$$

The equivalence (i)-(iii) in the following result can be interpreted as a p-group-theorethic version of Nakayama's lemma, with the Frattini subgroup playing the role of the Jacobson radical.

Proposition 4.2.2. *Let $\varphi : G \to H$ be a map of pro-p-groups. The following are equivalent:*

i) φ is an epimorphism;

ii) the induced map $H^1(\varphi) : H^1(H) \to H^1(G)$ is injective;

iii) the induced map $\Phi(\varphi) : G/\Phi(G) \to H/\Phi(H)$ *is surjective.*

Proof. Statements (ii) and (iii) are equivalent by Pontryagin duality. If φ is surjective, then $H^1(\varphi)$ is clearly injective.

Conversely, suppose $\mathrm{im}(\varphi) \lneq H$ and choose a maximal subgroup $U < H$ containing $\mathrm{im}(\varphi)$. Then U is normal of index p in H, so that the projection $\pi : H \to H/U \simeq \mathbf{Z}/p\mathbf{Z}$ is a nonzero element in $H^1(H) = \mathrm{Hom}(H, \mathbf{Z}/p\mathbf{Z})$. Nevertheless, $H^1(\varphi)$ sends π to zero in $H^1(G)$, so $H^1(\varphi)$ is not injective. □

Proposition 4.2.3. *Let* G, H *be projective pro-*p*-groups. If* $H^1(G)$ *and* $H^1(H)$ *are isomorphic, so are* G *and* H.

Proof. Let $\alpha : H^1(H) \xrightarrow{\sim} H^1(G)$ be an isomorphism. Then so is its dual map $\alpha^\vee : G/\Phi(G) \to G/\Phi(H)$. The conclusion follows at once by the more general lemma below. □

Lemma 4.2.4. *Let* G, H *be projective pro-*$\mathfrak{c}$*-groups, and* $\rho : G/\Phi(G) \xrightarrow{\sim} H/\Phi(H)$ *an isomorphism. There exists an isomorphism* $\psi : G \to H$ *lifting* ρ*, i.e. such that the diagram*

$$\begin{tikzcd}
G \arrow[r, "\psi"] \arrow[d] & H \arrow[d] \\
G/\Phi(G) \arrow[r, "\rho"] & H/\Phi(H)
\end{tikzcd}$$

commutes.

Proof. By projectivity of G, the embedding problem

$$\begin{tikzcd}
 & G \arrow[d, two heads] \\
 & G/\Phi(G) \arrow[d, two heads, "\rho"] \\
H \arrow[r, two heads] & H/\Phi(H)
\end{tikzcd}$$

has a solution $\psi : G \to H$, which is surjective by Proposition 4.2.2.

Consequently, the embedding problem

$$\begin{tikzcd}
 & H \arrow[d, "\mathrm{id}"] \\
G \arrow[r, two heads, "\psi"] & H
\end{tikzcd}$$

has a solution $\eta : H \to G$ since H is projective, i.e. $\psi \circ \eta = \mathrm{id}_H$, so that η is injective and $\eta(H)\ker(\psi) = G$. Now, notice $\ker(\psi) < \Phi(G)$ since ρ is injective: therefore, η is an isomorphism and so is ψ. □

Theorem 4.2.5. *Let G be a pro-p-group. The following are equivalent.*

i) *G is projective.*

ii) *G is a free pro-p-group.*

iii) $\mathrm{cd}(G) \leqslant 1$.

Proof. We only need to show that (i) implies (ii). Let $\kappa = \dim H^1(G)$, and consider $F = F_p(X)$ where $|X| = \kappa$. Then $H^1(F) = \mathrm{Hom}(F, \mathbf{Z}/p\mathbf{Z})$ identifies with the set of maps $X \to \mathbf{Z}/p\mathbf{Z}$ which are zero almost everywhere, due to the universal property of F, and is therefore isomorphic to $\mathbf{Z}/p\mathbf{Z}^{\oplus\kappa}$. Consequently, there exists an isomorphism $H^1(F) \xrightarrow{\sim} H^1(G)$, and Proposition 4.2.3 concludes. □

Corollary 4.2.6. *i) A profinite group G is projective if and only if, for all primes p, a p-Sylow of G is a free pro-p-group.*

ii) A subgroup H of a free pro-p-group G is again a free pro-p-group.

Proof. Statement (i) follows from the above theorem joint with Corollary 2.3.8, while (ii) is a consequence of Theorem 4.2.5 and Theorem 2.3.7. □

4.3 Iwasawa's theorem

As a final application of our results on embedding problems, we are now going to prove a theorem of K. Iwasawa about the Galois group of the maximal prosolvable extension $\widetilde{k^{ab}}$ of the maximal abelian extension of a global field k. Namely, we shall show that the group $G(\widetilde{k^{ab}}\,|\,k^{ab})$ is the free prosolvable group on countably many generators. Note that this implies, by Proposition 3.1.7, that the inverse Galois problem for solvable groups is solved for k^{ab}. First, we need to recall some notions from algebraic number theory.

If k is a field and $K|k$ is a Galois extension with Galois group $G = G(K|k)$, we let $H^n(K|k, A) = H^n(G, A)$ for a G-module A. In particular, for a separable closure $\bar{k}$ of k, we denote by $G_k = G(\bar{k}|k)$ the absolute Galois group of k, and set $H^n(k, A) = H^n(\bar{k}|k, A) = H^n(G_k, A)$.

Suppose now that k is a global field, and $K|k$ a separable extension. In order to avoid the explicit choice of a prime $\mathfrak{P}$ of K lying over $\mathfrak{p}$, we implicitly fix an embedding $\iota_\mathfrak{p} : k_\mathfrak{p} \hookrightarrow \overline{k_\mathfrak{p}}$, or equivalently a prime of $\overline{k_\mathfrak{p}}$ lying over $\mathfrak{p}$. Consequently, we have a distinguished prime $\mathfrak{P}$ of K over $\mathfrak{p}$, and we denote $K_\mathfrak{p} = \iota_\mathfrak{p}(K)k_\mathfrak{p}$ the localization of K at $\mathfrak{P}$ (or equivalently its completion, if $K|k$ is finite).

If moreover $K \,|\, k$ is Galois, we write $G_{\mathfrak{p}}(K \,|\, k)$ for the decomposition group $G_{\mathfrak{P}}(K \,|\, k) \subset G(K \,|\, k)$ and identify it with the local Galois group $G(K_{\mathfrak{p}} \,|\, k_{\mathfrak{p}})$: in particular, we can view $G(K_{\mathfrak{p}} \,|\, k_{\mathfrak{p}})$ as a subgroup of $G(K \,|\, k)$.

Therefore, for every $G(K \,|\, k)$-module A we have a restriction map

$$\mathrm{res}_{\mathfrak{p}} : H^n(K \mid k, A) \to H^n(K_{\mathfrak{p}} \mid k_{\mathfrak{p}}, A).$$

If we fix a set of primes T of k, the restrictions above for primes $\mathfrak{p}$ in T induce a homomorphism

$$H^n(K \,|\, k, A) \to \prod_{\mathfrak{p} \in T} H^n(K_{\mathfrak{p}} \,|\, k_{\mathfrak{p}}, A).$$

To prove Iwasawa's theorem, we need the above map to be surjective in degree 1 under a specific set of hypotheses on T and A, assuming that $K = \bar{k}$. This is a consequence of the local duality theorem joint with Čebotarev density theorem (see [NSW15], Theorem 9.2.3 for a proof).

For a G_k-module A, consider the morphism $G_k \to \mathrm{Aut}(A)$ induced by the action of G on A, and let $H < G_k$ be its kernel. The *minimal trivializing extension* $k(A)$ is the extension of k corresponding to H. Recall that, by Remark 2.3.3, a simple G-module A admits exactly one prime p such that $pA = 0$.

Theorem 4.3.1. *Let k be a global field, T a finite set of primes of k. For a G_k-module A and a prime p, suppose either one of the following is true:*

i) A is a finite simple G_k-module with $pA = 0$, $p \nmid \mathrm{char}(k)$, and $G(k(A) \mid k)$ is solvable;

ii) A is a p-primary G_k-module, and $p = \mathrm{char}(k)$.

Then, the restriction map

$$H^1(k, A) \to \prod_{\mathfrak{p} \in T} H^1(k_{\mathfrak{p}}, A)$$

is an epimorphism.

We also need the following result about the cohomological dimension of specific extensions of local and global fields, which is a consequence of the structure of their Brauer groups (we refer to Theorem 7.1.8 and Corollary 8.1.18 of [NSW15]).

Theorem 4.3.2. *Let $K \,|\, k$ be a field extension, and p a prime. If $p = 2$ and k is a number field, suppose moreover that K is totally imaginary.*

i) If k is a local field and $p^\infty \mid [K : k]$, then $\mathrm{cd}_p(G_K) \leqslant 1$.

ii) If k is a global field and $p^\infty \mid [K_{\mathfrak{p}} : k_{\mathfrak{p}}]$ for all primes $\mathfrak{p}$ of K, then $\mathrm{cd}_p(G_K) \leqslant 1$.

For a field k and some prime ℓ, consider the maximal pro-ℓ-quotient $G_k(\ell)$ of G_k (see Remark 1.2.2), and note that $G_k(\ell)$ is the Galois group of the maximal pro-ℓ-extension $k(\ell) \,|\, k$. As a consequence of the local duality theorem, the maximal pro-ℓ-quotients of G_k are well understood for a local field k. In particular, we have the following result, a proof of which can be found in [NSW15], Proposition 7.5.9.

Lemma 4.3.3. *Let k be a local field of residue characteristic p, and $\ell \neq p$ a prime. Then $G_k(\ell)^{ab} \simeq \mathbf{Z}_\ell \oplus U$, with U a (possibly trivial) finite cyclic ℓ-group, where $G^{ab} = G/\overline{[G,G]}$ is the abelianization of a profinite group G.*

We may now turn to the proof of Iwasawa's theorem, starting with a technical result. Denote the inertia group of an extension $K \,|\, k$ of valued fields by $T(K \,|\, k)$, and in particular set $T_k = T(\overline{k} \,|\, k)$ for a fixed separable closure $\overline{k}$ of k.

Lemma 4.3.4. *Let $K \,|\, k$ an infinite abelian extension of a global field k. For every choice of a finite group E and a finite separable extension $K' \,|\, K$, there exist primes $\mathfrak{P}_1, \dots, \mathfrak{P}_s$ of K and homomorphisms $\varphi_i : G_{K_{\mathfrak{P}_i}} \to E$ such that*

i) $\mathfrak{P}_1, \dots, \mathfrak{P}_s$ split completely in K';

ii) E is generated by the images of the φ_i.

Proof. It is enough to prove that, for a fixed prime ℓ, there are infinitely many primes $\mathfrak{P}$ of K that split completely in K' and admit an epimorphism $G_{K_{\mathfrak{P}}} \twoheadrightarrow \mathbf{Z}_\ell$.

By Čebotarev density theorem (see [Neu99], Theorem 13.4), we may find infinitely many primes $\mathfrak{P}$ of K which are completely decomposed in K' and such that $K_{\mathfrak{P}}$ contains a primitive ℓ-th root of unity ζ if ℓ differs from the characteristic of k: take a finite extension $K_0 \,|\, k$ inside K and a finite separable extension $K_0' \,|\, K_0$ such that $KK_0' = K'$ and consider the prolongations to K of infinitely many primes of K_0 that split completely in $K_0'(\zeta)$, or simply in K_0' if $\ell = \operatorname{char} k$.

Fix now such a $\mathfrak{P}$ and let $\mathfrak{p} = \mathfrak{P} \cap k$ be its contraction to k. Suppose first that the maximal unramified ℓ-extension L of $k_{\mathfrak{p}}$ inside $K_{\mathfrak{P}}$ is finite: if $\widetilde{k_{\mathfrak{p}}}(\ell)$ is the maximal unramified ℓ-extension of $k_{\mathfrak{p}}$ inside a fixed separable closure, $G(\widetilde{k_{\mathfrak{p}}}(\ell) \,|\, L)$ is an open subgroup of $G(\widetilde{k_{\mathfrak{p}}}(\ell) \,|\, k_{\mathfrak{p}}) \simeq \mathbf{Z}_\ell$, and is therefore isomorphic to $\mathbf{Z}_\ell$ itself. Consequently, the projection $G_{K_{\mathfrak{P}}}(\ell)/T_{K_{\mathfrak{P}}}(\ell) \twoheadrightarrow G(\widetilde{k_{\mathfrak{p}}}(\ell) \,|\, L)$ induces the wanted epimorphism.

Conversely, if L is infinite, we must have $K_{\mathfrak{P}} \supset \widetilde{k_{\mathfrak{p}}}(\ell)$. If ℓ differs from the residue characteristic p of $k_{\mathfrak{p}}$, we have $G_{K_{\mathfrak{P}}}(\ell) \simeq T_{K_{\mathfrak{P}}}(\ell)$ for $\zeta \in K_{\mathfrak{P}}$. Since $K_{\mathfrak{P}} \,|\, k_{\mathfrak{p}}$ is abelian, $T(K_{\mathfrak{P}} \,|\, k_{\mathfrak{p}})(\ell)$ is a subquotient of $G_{k_{\mathfrak{p}}}(\ell)^{ab}$, and is hence finite by Lemma 4.3.3; therefore, $G_{K_{\mathfrak{P}}}(\ell)$ is an open subgroup of $T_{k_{\mathfrak{p}}}(\ell) \simeq \mathbf{Z}_\ell$, and the conclusion follows.

Finally, if $\ell = p$ and M is the maximal pro-p extension of k in K, $G_{M_{\mathfrak{P}}}(p)$ is a free pro-p-group by Theorems 4.3.2 and 4.2.5, and so is $G_{K_{\mathfrak{P}}}(p)$ by Corollary 4.2.6, hence we have a surjection $G_{K_{\mathfrak{P}}}(p) \twoheadrightarrow \mathbf{Z}_p$ by Proposition 3.1.7. □

Theorem 4.3.5 (Iwasawa). *Let K be the maximal abelian extension of a global field. If $\widetilde{K}$ is the maximal prosolvable extension of K, its Galois group $G = G(\widetilde{K}|K)$ is the free prosolvable group of countable rank.*

Proof. Since there are at most countably many finite separable extensions of K in a fixed separable closure, $d(G) \leqslant \aleph_0$. By Theorem 3.2.7, we need to show that (in the notation of the theorem) every embedding problem for G with finite solvable A has a strong solution.

Consider the diagram

$$\begin{tikzcd}
 & & & G_K \arrow[d, two heads] & \\
 & & & G \arrow[d, two heads, "\varphi"] & \\
1 \arrow[r] & C \arrow[r] & A \arrow[r, "\alpha"] & B \arrow[r] & 1
\end{tikzcd} \tag{4.2}$$

where the map $G_K \to G$ is the canonical projection and A is a finite solvable group. If we can find a strong solution $G_K \twoheadrightarrow A$, it will factor to a map $G \twoheadrightarrow A$ since A is solvable and G is the maximal prosolvable quotient of G_K by definition.

Identifying C with a subgroup of A, and choosing a B-submodule $C' < C$ normal in A, suppose we find a strong solution ψ for the problem

$$\begin{tikzcd}
 & & & G \arrow[d, two heads, "\varphi"] & \\
1 \arrow[r] & C' \arrow[r] & A/C' \arrow[r, "\alpha'"] & B \arrow[r] & 1
\end{tikzcd} ,$$

where α' is induced by α; then we also get a solution for the above problem by considering the diagram

$$\begin{tikzcd}
 & & & G \arrow[d, two heads, "\psi"] & \\
1 \arrow[r] & C' \arrow[r] \arrow[d] & A \arrow[r] \arrow[d, equal] & A/C' \arrow[r] \arrow[d, two heads, "\alpha'"] & 1 \\
1 \arrow[r] & C \arrow[r] & A \arrow[r, "\alpha"] & B \arrow[r] & 1
\end{tikzcd} .$$

Thus, by arguing inductively, and using the fact that A is solvable, we may reduce to the case where C is an abelian simple B-module.

As a consequence of Theorem 4.3.2, we have $\mathrm{cd}(G_K) \leqslant 1$: therefore, the embedding problem (4.2) with C an abelian simple B-module has a weak solution $\psi : G_K \to A$ by Corollary 4.1.8. Let $N = \ker(G_K \twoheadrightarrow B)$ and call ψ_0 the restriction of ψ to N. Because C is simple, $\mathrm{im}(\psi_0)$ is either C or 0. In the first case, ψ is actually surjective and factors through G, so we are done. We may therefore assume $\mathrm{im}(\psi_0) = 0$.

Let $B = G(K' \mid K)$, with K' an intermediate extension of $\tilde{K} \mid K$, so that C is a trivial $G(\tilde{K} \mid K')$-module. Note we may write $G = G(\tilde{K} \mid K) = \varprojlim_k G(\tilde{K} \mid k)$, where k runs through all the finite subextensions of K: by Proposition 1.1.12 we can find a finite subextension k_0 of K such that $\varphi : G \to G(K' \mid K)$ factors to a map $\overline{\varphi} : G(\tilde{K} \mid k_0) \to G(K' \mid K)$. If we let $\ker(\overline{\varphi}) = G(\tilde{K} \mid k_0')$, we obtain a finite extension $k_0' \mid k_0$ such that $G(k_0' \mid k_0) \simeq G(K' \mid K)$ and $K' = Kk_0'$.

Then clearly, for all intermediate fields $k_0 \subset k \subset K$ finite over k_0, by letting $k' = kk_0'$ we have $G(k' \mid k) \simeq G(K' \mid K)$ and $K' = Kk'$. For all such k, we may view K as a G_k-module via the projection $G_k \twoheadrightarrow G(k' \mid k) \simeq G(K' \mid K)$.

By Lemma 4.3.4, we can find primes $\mathfrak{P}_1, \ldots, \mathfrak{P}_s$ of K and homomorphisms $\varphi_i : G_{K_{\mathfrak{P}_i}} \to C$ such that the $\mathfrak{P}_i$ split completely in K' and $C = \langle \mathrm{im}(\varphi_i) \mid i \rangle$. Up to replacing k_0 with a finite extension, we may also assume that the contractions $\mathfrak{p}_i = \mathfrak{P}_i \cap k_0$ split completely in K' (and the same is true for finite intermediate extensions $k \mid k_0$).

Fix k as above: since C is a simple G_k-module and $G(k' \mid k)$ is solvable, Theorem 4.3.1 implies that the restriction homomorphism

$$H^1(k, C) \to \prod_{i=1}^{s} H^1(k_{\mathfrak{P}_i}, C)$$

is surjective. Passing to the direct limit by Corollary 2.1.12, we obtain that

$$H^1(K, C) \to \prod_{i=1}^{s} H^1(K_{\mathfrak{P}_i}, C)$$

is again an epimorphism by exactness of $\varinjlim$.

Since the $\mathfrak{P}_i$ split completely in K', the decomposition group $G(K'_{\mathfrak{P}_i} \mid K_{\mathfrak{P}_i})$ is trivial, and so C is a trivial $G_{K_{\mathfrak{P}_i}}$-module. Thus, $H^1(K_{\mathfrak{P}_i}, C) = \mathrm{Hom}(G_{K_{\mathfrak{P}_i}}, C)$, and $(\varphi_i \mid i)$ is an element of $\prod_{i=1}^{s} H^1(K_{\mathfrak{P}_i}, C)$. We may thereby pick a preimage $c \in H^1(K, C)$ of $(\varphi_i \mid i)$.

Let f be a 1-cocycle representing c, and call $\psi' : G_K \to A$ the map defined by $\psi(\sigma) = f(\sigma)\psi(\sigma)$. Then, since $\psi_0 = 0$, the restriction ψ_0' of ψ' to N is simply f, and is therefore surjective, because $G_{K_{\mathfrak{P}_i}} < N$, f coincides with φ_i on $G_{K_{\mathfrak{P}_i}}$ and $C = \langle \mathrm{im}(\varphi_i) \mid i \rangle$.

Thus, ψ' is surjective and factors to an epimorphism $G \twoheadrightarrow A$ lifting φ. □

We conclude by noting that it is known that, at least when looking for a finite solvable extension of a global field without additional properties, the inverse Galois problem has an affirmative answer. Using methods that go beyond the scope of this dissertation, I. R. Šafarevič proved the following (see [NSW15], Theorem 9.6.1).

Theorem 4.3.6 (Šafarevič)**.** *Let* k *be a global field and let* G *be a finite solvable group. Then there exists a Galois extension* $K|k$ *with* $G(K|k) = G$.

Bibliography

[Gro57] Alexander Grothendieck. Sur quelques points d'algèbre homologique. *Tôhoku Math. J.*, 1957.

[Iwa53] Kenkichi Iwasawa. On solvable extensions of algebraic number fields. *Ann. Math.*, 1953.

[Neu99] Jürgen Neukirch. *Algebraic Number Theory*. Springer, 1999.

[NSW15] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of Number Fields*. Springer, 2nd edition, 2015.

[Rud90] Walter Rudin. *Fourier Analysis on Groups*. Wiley-Interscience, 1990.

[RZ10] Luis Ribes and Pavel Zalesskii. *Profinite groups*. Springer, 2nd edition, 2010.

[Ser97] Jean-Pierre Serre. *Cohomologie Galoisienne*. Springer, 5th edition, 1997.